Security Target for Cybertrust UniCERT 5

Common Criteria EAL4 Evaluation

Table of Contents

1. Introduction 1
1.1 Security Target Identification 1
1.2 Security Target Scope 1
1.3 Security Target Organisation 2
1.4 CC Conformance Claim 3
1.5 Glossary 4
1.6 References 12

2. TOE Description 13
2.1 Product Type 13
2.2 Methods of Use 15
2.3 Product Components 18
2.4 UniCERT Configurations 34
2.5 UniCERT Evaluated Configuration 37
2.6 CD Content Lists 41

3. TOE Security Environment 57
3.1 Introduction 57
3.2 Secure Usage Assumptions 57
3.3 Threats to Security 59
3.4 Organisational Security Policies 72

4. Security Objectives 74
4.1 Introduction 74
4.2 Security Objectives for the TOE 74
4.3 Security Objectives for the Environment 78

5. IT Security Requirements 82
5.1 Introduction 82
5.2 TOE Security Functional Requirements 82
5.3 TOE Security Assurance Requirements 108
5.4 Security Requirements for the IT Environment 119
5.5 Minimum Strength of Function Level 120

6. TOE Summary Specification 121
6.1 Introduction 121
6.2 TOE Security Functions 121
6.3 Assurance Measures 133

7. Protection Profile Claims 138

7.1 Protection Profile Reference 138
7.2 Protection Profile Refinements 138
7.3 Protection Profile Additions 138

8. Rationale 139
8.1 Introduction 139
8.2 Security Objectives Rationale 139
8.3 Security Requirements Rationale 148
8.4 TOE Summary Specification Rationale 168
8.5 PP Claims Rationale 169

9. Security Policy Model 170
9.1 Introduction 170
9.2 Definition of Users 173
9.3 Information Flow Control Policy. 178

Appendix A Documentation Contents on TOE CDs 184
A.1 UniCERT Core v5.2.1 for Windows 184
A.2 UniCERT WebRAO Client v5.2.1 for Windows 220
A.3 UniCERT Core v5.2.1 for Solaris 227

1. Introduction

1.1 Security Target Identification

1.1.1 This section provides the labelling and descriptive information necessary to control and identify the Security Target and the TOE to which it refers.

1.1.2 It is assumed that the reader of this document is familiar with the concept of PKI.

Title:	Security Target for Cybertrust UniCERT 5
Authors:	George Sarandrea, Judith Furlong, Michael Linehan, Chris Lowe
TOE Identification	Cybertrust UniCERT 5.2.1
Publication Date	January 2006
ISO 15408 (CC) Version:	2.1 Final
EAL:	4, augmented with ALC_FLR.2
ST Evaluation:	LogicaCMG's AISEF
Keywords:	PKI, Certification Authority

Table 1-1 ST Information

1.1.3 Note that the release of the product that is under evaluation is 5.2.1, including patch 5.2.1.900. Whenever "UniCERT" or "UniCERT 5" is referred to in this document or other evaluation deliverables, that is what is meant.

Also note that as a result of a recent merger, Cybertrust now holds the copyright to Betrusted products. Where the UniCERT documents or software refer to Betrusted as the legal entity, read Cybertrust.

1.2 Security Target Scope

1.2.1 Cybertrust's UniCERT is a PKI/Cryptography standards-compliant server for generating, issuing and revoking digital certificates in response to requests received from clients.

1.2.2 UniCERT provides all the functionality needed to implement a PKI system, essentially a system that provides registration, PKI management and certification authority functions. This can then be used to manage all the keys necessary for a system requiring security for end users, such as a secure messaging system, or security on Web browsers. UniCERT provides the ability to set up a centralized or a distributed PKI for organizations of any size.

1.2.3 Public Key Infrastructure (PKI) provides the core framework for a wide variety of components, applications, policies and practices to combine and achieve the four principal security functions for commercial transactions:

1.2.4 **Confidentiality** to keep information private

1.2.5 **Integrity** to prove that information has not been manipulated

1.2.6 **Authentication** to prove the identity of an individual or application

1.2.7 **Non-repudiation** to ensure that information cannot be disowned

1.2.8 Lack of security is often cited as a major barrier to the growth of e-commerce, which can only be built on the confidence that comes from knowing that all transactions are protected by these core functions.

1.3 Security Target Organization

1.3.1 The main sections of the Security Target are its TOE description, TOE Security Environment, Security Objectives, IT Security Requirements, TOE Summary Specifications, Protection Profile Claims and Rationale.

1.3.2 The *TOE Description* provides general information about the TOE, serves as an aid to understanding its security requirements, and provides context for the ST evaluation.

1.3.3 The *TOE Security Environment* describes security aspects of the environment in which the TOE is to be used and the manner in which it is to be employed. The TOE security environment includes descriptions of a) assumptions regarding the TOE intended usage and environment of use, b) threats relevant to secure TOE operation, and c) organizational security policies with which the TOE must comply.

1.3.4 The *Security Objectives* reflect the stated intent of the ST. They pertain to how the TOE will counter identified threats and it will cover identified organizational security policies and assumptions. Each security objective is categorized as being for the TOE, or for the environment.

1.3.5 The *IT Security Requirements* are subdivided as follows: (a) TOE Security Functional Requirements, including strength-of-function requirements for TOE security functions realized by a probabilistic or permutational mechanism, and (b) TOE security assurance requirements.

1.3.6 The *TOE Summary Specification* defines the instantiation of the security requirements of the TOE. This specification describes the security functions and assurance measures of the TOE that meet the TOE security requirements. The TOE Summary Specification section covers the IT security functions and specifies how these functions satisfy the TOE security functional requirements. The Functional and Assurance requirements are derived from the Common Criteria, Part 2 and 3, respectively, and the TOE must satisfy these. TOE Summary Specification includes a mapping between functions and requirements that shows which functions satisfy which requirements and that all requirements are met.

1.3.7 The *Protection Profile Claims* section contains the Protection Profile conformance claim statements. Although there are no Protection Profile conformance claims, this section is provided for completeness.

1.3.8 The *Rationale* presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment.

1.3.9 The *Rationale* is factored into two main parts. First, a Security Objectives Rationale demonstrates that the stated security objectives are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them. Then, a Security Requirements Rationale demonstrates that the security requirements (TOE and environment) are traceable to the security objectives and are suitable to meet them.

1.3.10 The Protection Profile Rationale, provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the protection profile requirements. This is not used in this ST as there is no PP dependency.

1.3.11 An acronym list is provided to define frequently used acronyms.

1.3.12 A reference section is provided to identify background material.

1.4 CC Conformance Claim

The TOE conforms to the Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408), Version 2.1, Parts 2 and 3 as follows:

a) Part 2 conformant
b) Part 3 conformant
c) EAL 4 augmented with ALC_FLR.2

1.5 Glossary

Term	Description
ARL	See *Authority revocation list*
ARM	Advanced Registration Module. A separate piece of software, which may be purchased, installed, and executed completely separately from UniCERT so as to interface to UniCERT. May not be used with the product in its evaluated configuration.
Auditor	A special class of administrator that is given permissions to perform functions on the audit logs. There are four types of auditor, as described in Section 9.2.
Audit log	Security relevant events occurring during the operation of the PKI are recorded in audit logs of either the CA and/or the RA.
Authority revocation list	A revocation list containing identification of public-key certificates issued to Certification Authorities (CA) that are no longer considered valid by the certificate issuer. This is essentially a list of authorities that have been compromised in some way and can no longer be trusted.
Authorization	The process of approving a request against criteria set forth in a registration policy.
Authorization group	An authorization group is a specific set of authorizers (human or automated processes). Membership within an authorization group may be indicated by a specify DN or DN attribute. Authorization groups are set up using the CAO, and are used to control which authorizers can process requests submitted using a particular registration policy.
Authorizer	Human or automated process, which approves a request against criteria set forth in a registration policy, whereupon a certificate is generated and issued upon affirmative approval.
Bootstrap	The process of creating a PKI, which involves creating the CA and CAO.
CA	See *Certification Authority*
CA clone	Separate instances of the CA executable, which use the same key material and the same database.
CA components	Combination of CA (Server), CA database, CAO, Publisher and Certificate Status Server (CSS) that together provide the certification part of the system.

Term	Description
CAO	See *Certification Authority Operator.*
CAO user	Person who operates the CAO.
CDP	See *CRL distribution point.*
Certificate	For the purposes of this document, Certificate refers to *X.509 Certificate* - see below.
Certificate extensions	Optional fields within an X.509 v3 formatted certificate that contain information designed to enhance the certificate verification process and to convey additional information about the subject and issuer of the certificate.
Certificate revocation list	A signed list of certificates (serial numbers) that have been revoked and can no longer be trusted (according to the standard for CRL v2 as defined in X.509).
Certification Authority	The component within the TOE which is responsible for the creation, distribution, or revocation of X.509 public key certificates
Certification Authority Operator	The interface through which the elements of a public-key infrastructure (PKI) are defined, configured and controlled. The CAO is used to configure the PKI, define registration policies, and administer certificates. It is the trusted system management component for a CA.
Certification Practices Statement	A detailed document issued by a Certification Authority that prescribes the operational procedures on the security and registration policies under which that authority issues public-key certificates.
Clone	See *CA Clone or RA clone.*
CPS	See *Certification Practices Statement.*
CRL	See *Certificate revocation list*
CRL distribution point	The location from which a CRL or partitioned CRL can be obtained. Specifically, an X.500 directory entry or other information source that is named in an X.509 v3 public-key certificate extension as a location from which to obtain a certificate revocation list.
Cross-certification	The process whereby a UniCERT CA can certify another CA. Handled using the normal processes for signing any certificate, but via a slightly different message and certificate format.

Term	Description
Crypto module	A hardware security module (HSM) or smart card, which can be used to store keys and perform some cryptographic operations. Those that can be used with the TOE are defined in 2.5.1.6.
Directory server	A directory server is typically used to store information, such as a company directory, in a central repository and to provide quick and easy access to this information. LDAP is a standard protocol for accessing directory servers.
Distinguished Name	A sequence of attributes that identifies an entity and traces its path up the directory tree. The DN provides the necessary information about the owner of a certificate. The certificate contains both the DN of the owner (subject) and the DN of the issuer of the certificate.
DN	See *Distinguished name.*
DN attribute	An element of a distinguished name, e.g., C=US or O=Cybertrust.
EE	See *End entity.*
End entity	An entity (e.g., end user) that is the subject of a public-key certificate and that is using, or is permitted and able to use, the matching private key only for some purpose other than signing a certificate.
Face-to-face registration	The process of entering end user details at the WebRAO directly, without a remote request coming in through the protocol handler.
Hardware security module	A hardware security module is a cryptographic device, which can generate, store and use cryptographic keys within a secure hardware device.
HSM	See *Hardware security module.*
Issuer DN	The distinguished name that identifies the CA that has issued a certificate.
KAS	Key Archive Server. A separate piece of software to the TOE, which may be installed with the TOE. The TOE provides an evaluated interface to the KAS.
LDAP	See *Lightweight Directory Access Protocol.*

Term	Description
Lightweight Directory Access Protocol	A set of open protocols for accessing information directories. LDAP can make the physical network topology and protocols transparent so that a network user can access any resource without knowing where or how it is physically connected.
Object identifier	A string of numbers that is unique worldwide, for example, 1.2.840.23452323.1.1. An OID represent a hierarchy of domains and objects within domains, using numbers instead of names. Each OID starts from an internationally defined root. For example, 1 at the first level represents the International Standards Organization (ISO). Each level of the hierarchy is represented by its own unique number (ID), which is appended to the OID of the level above it. For example, 1.2.840 represents the hierarchy: ISO (1) ISO member-body (2) United States (840). In a hierarchy like this, each country is responsible for defining the structure of the rest of the OID under the third level (country).
OCSP	See *Online Certificate Status Protocol.*
OID	See *Object identifier.*
Online Certificate Status Protocol	A protocol that allows applications to verify whether a certificate is valid or has been revoked. OCSP can be either a replacement or a supplement to checking against a CRL. It attempts to overcome some of the distribution limitations of the CRL. OCSP specifies a request-response message syntax between a client application that requires certificate revocation status information and a server application that has knowledge of the revocation status. The OCSP server (or OCSP responder) can also provide additional status information beyond that available through a CRL.
Operational policy	An operational policy consists of configuration information for a PKI entity. They set up operational rules, explicitly defining required tasks and how each entity performs its functions on a daily basis. For example, the CA's operational policy defines how often the CA generates a CRL and whether it generates a new CRL each time a certificate is revoked. The RA's operational policy defines the time period during which the RA processes certificate requests and how often it polls the database for new requests.

Term	Description
P11	A standard for accessing cryptographic hardware tokens for example smart cards and HSMs. The standard is defined in [PKCS11].
P12	A standard for securely storing key material in software. The standard is defined in [PKCS12].
Personal secure environment	Cybertrust supports the concept of a personal secure environment (PSE). This proprietary format holds certificate owners' private keys (or a pointer to the private keys if the keys are being kept in a smart card, token or HSM) and other sensitive data securely. They can only be accessed or altered by the authorized owner of those keys. UniCERT supports both disk- and token-based PSE.
PH	See *Protocol Handler.*
PKCS#11 device	See *Crypto module.*
PKI	See *Public key infrastructure.*
PKI entity	One of the UniCERT core components (e.g., CA, CAO, RA, WebRAO, etc.) that are within the PKI structure.
POP	See *Proof of possession.*
Proof of possession	A verification process whereby it is proven that the owner of a key pair actually possesses the private key associated with the public key.
Protocol Handler	A Protocol Handler (PH) is a UniCERT registration component though which applications can make protocol specific request for certificates and other PKI related services. A Protocol Handler converts requests from protocol specific formats to the common request format that is used internal to the UniCERT system.
PSE	See *Personal secure environment.*
Public-key certificates	A set of data that uniquely identifies an entity, contains the entity's public key and optionally other information that is digitally signed by a trusted party, thereby binding the public key to the entity. The optional information may provide more information about the user and how the key should be used.

Term	Description
Public-key infrastructure	A PKI system provides a framework by which users and entities can communicate securely. Public-key cryptography uses a combination of public and private keys, digital signatures, digital certificates, and Certification Authorities (CAs), to meet the major requirements of e-security. The X.509 standard defines a PKI as "The set of hardware, software, people and procedures needed to create, manage, store, distribute and revoke certificates based on public-key cryptography." Described in RFC3280 as published by the IETF.
RA	See *Registration Authority.*
RA clone	Separate instances of the RA executable, which use the same key material and the same database.
RA components	Combination of RA (Server), RA database, RA exchange, Protocol Handlers and WebRAO that together provide the registration portal (interface) to the system.
Registration Authority Operator	See *WebRAO*.
RAO	See *WebRAO*.
Registration	The process of collecting information required to generate and authorize (approve) a certificate request. Registration may be face-to-face, or may be via a protocol handler or programmatic interface (referred to as remote registration).
Registration Authority	The RA acts as a router, transferring information to and from the CA. It receives and verifies certificate requests from the registering entities, and sends back the CA's reply.
Registration policy	A registration policy (RP) provides a set of rules and criteria for certificate requests that must be met before the CA can issue a certificate. An RP governs what data must be collected for the certificate applicant to register, determines the content of the certificate(s) produced, and controls the life cycle of the certificate.
Registration Policy Editor	The Registration Policy Editor is a portion of the CAO, which is used to create registration policies.
Remote registration	The process of registration being initiated via a protocol handler or a programmatic interface rather than face-to-face.

Term	Description
Revocation	The process of invalidating a public key certificate. There are a number of reasons for revocation, including: unspecified, key compromise, CA compromise, affiliation changed, superseded and certificate hold. A certificate hold places a certificate on hold, referred to as suspension of a certificate in this document. With the exception of certificate hold, all other reasons for revocation are permanent, which means the certificate will no longer be or become valid.
Revocation Request	Revocation requests include requests to revoke, suspend and unsuspended a certificate.
Revoke	To invalidate a certificate.
Root CA	The Certification Authority at the top of the PKI hierarchy.
Root certificate	The self-signed public-key certificate at the top of the PKI hierarchy.
RP	See *Registration policy*.
Schema	The structure of a database system, including the layout of fields in tables, and the relationships (if any) between different tables.
Smart card	A card with an embedded integrated circuit for storing information, typically used for authenticating a computer user or banking services, providing access control, storing value applications, and/or carrying private keys in a security system.
"Social engineering" attack	An attack whereby a trusted person is either bribed or threatened to cause them to reveal or change something that they should not.
Sub CA	See *Subordinate CA*.
Subject DN	The distinguished name that identifies the entity to whom a certificate is issued, for example: cn=John Doe, ou=Sales, o=Acme, l=Northeast, c=US.
Subordinate CA	A Certification Authority that is below the level of the root CA. A subordinate CA is a special case of a CA, whereby the CA certificate is registered (certificate is signed by another CA) as part of another PKI. UniCERT may be configured either as a root CA or a subordinate CA.

Term	Description
Suspension	The temporary revocation of a certificate. Once a certificate has been suspended it can be handled in one of three ways: • It may remain on the CRL with no further action, causing users to reject transactions issued during the hold period. • It may be replaced by a (final) revocation for the same certificate, in which case the reason shall be one of the standard reasons for revocation, the revocation date shall be the date the certificate was suspended. • It may be explicitly released and the entry removed from the CRL.
System administrator	The person responsible for maintaining the systems necessary for the smooth running of UniCERT, including the operating system, the Oracle database, communications lines, etc.
Unsuspension	Removing the temporary hold (suspension) of a certificate and therefore removing it from the CRL.
UPI	UniCERT Programmatic Interface. A separate software toolkit, which provides access to the authorization and registration functionality within UniCERT. May not be used with the product in its evaluated configuration.
Web Registration Authority Operator	See *WebRAO.*
WebRAO	A Web-based application used to review and authorize (approve) certificate requests and which may also be used to submit certificates requests on behalf of an end entity.
X.509	The ISO/ITU-TX.509 standard defines what information can be included in a certificate and a certificate revocation list and describes the data format of the information.
X.509 certificate	The ISO/ITU-T X.509 Standard defines two types of certificates, the X.509 public key certificate and the X.509 attribute certificate. In this document the X.509 certificate refers to a X.509 public key certificate. (See *also Public Key Certificate.)*
X.509 public key certificate	A block of data containing your public key and basic identification details rendered unforgeable by the digital signature of the issuing CA private key, encoded in the ISO/ITU-T X.509 format.

Table 1-2 Glossary

1.6 References

1.6.1 The following documents were referenced in the preparation of this Security Target:

[3DES] FIPS 46-3 (http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf)

[CC] Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408), version 2.1, Parts 1, 2 and 3

[FLR] Common Methodology for Information Technology Security Evaluation (CEM-2001/0015R) Part 2: Evaluation Methodology Supplement: ALC_FLR – Flaw Remediation, Version 1.1 February 2002

[DER] ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) ITU-T Rec. X.690 (1997) | ISO/IEC 8825-1:1998, available at http://asn1.elibel.tm.fr/en/standards/ASN1-1997.htm

[DSA] Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, 27 January 2000 (http://www.csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf)

[PEM] Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services (http://www.ietf.org/rfc/rfc1424.txt)

[PKCS10] PKCS #10 v1.7: Certification Request Syntax Standard, RSA Laboratories, May 26 2000

[RFC1321] R. Rivest. RFC1321: The MD5 Message Digest Algorithm, April 1992.

[PKCS11] PKCS #11 Cryptographic Token Interface Standard, RSA Laboratories, v2.01 December 1997

[PKCS12] PKCS#12 Personal Information Exchange Syntax, RSA Laboratories, v1.0, June 24, 1999

[PKCS7] PKCS #7 v1.5: Cryptographic Message Syntax Standard, RSA Laboratories, Nov 1 1993

[PPST_G] Guide for production of Protection Profiles and Security Targets, version 0.8, ISO/IEC WD 15446, M. Donaldson, July 1999

[RSA] PKCS 1 (http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html)

[SCEP] Cisco System's Simple Certificate Enrolment Protocol, http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.htm

[SHA-1] Secure Hash Standard, Federal Information Processing Standards Publication 180-2, 1 August 2002 (http://www.csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf)

2. TOE Description

2.1 Product Type

2.1.1 UniCERT provides all the functionality needed to implement a PKI system, essentially a system that provides registration, PKI management and certification authority functions. This can then be used to manage all the keys necessary for a system requiring security for end users, such as a secure messaging system, or security on Web browsers. UniCERT provides the ability to set up a centralized or a distributed PKI for organizations of any size.

2.1.2 Public Key Infrastructure (PKI) provides the core framework for a wide variety of components, applications, policies and practices to combine and achieve the four principal security functions for commercial transactions:

2.1.3 **Confidentiality –** to keep information private

2.1.4 **Integrity** – to prove that information has not been manipulated

2.1.5 **Authentication** – to prove the identity of an individual or application

2.1.6 **Non-repudiation** – to ensure that information cannot be disowned

2.1.7 Lack of security is often cited as a major barrier to the growth of e-commerce, which can only be built on the confidence that comes from knowing that all transactions are protected by these core functions.

2.1.8 A Public Key Infrastructure is made up of hardware and software products combined with the policies and procedures to implement and operate the system. It provides the basic security required to carry out electronic business so that users, who do not know each other, or are widely distributed, can communicate securely through a chain of trust. PKI is based on digital IDs known as "digital certificates" which act like "electronic passports", and bind the user's public key to his or her private key.

2.1.9 A PKI should consist of:

2.1.9.1 Security Policy

A security policy sets out and defines an organization's top-level direction on information security, as well as the processes and principles for the use of cryptography. Typically it will include statements on how the organization will handle keys and valuable information, and will set the level of control required to match the levels of risk.

2.1.9.2 Certification Practices Statement (CPS)

Some PKI systems are Commercial CAs, and therefore require a CPS. This is a detailed document containing the operational procedures on how the Security Policy will be enforced and supported in practice. It typically includes definitions on how the CAs are constructed and operated, how certificates are issued, accepted and revoked, and how keys will be generated, registered and certified, where they will be stored, and how they will be made available to users.

2.1.9.3 Certification Authority

The CA system is the trust basis of a PKI, as it manages public key certificates for their whole life cycle. The CA will:

- Issue certificates by binding the identity of a user or system to a public key with a digital signature;
- Schedule expiry dates for certificates;
- Ensure certificates are revoked when necessary; and
- Informs users about revoked certificate by publishing Certificate Revocation Lists (CRLs).

2.1.9.4 Registration Authority

An RA provides the interface between the user and the CA. It captures and authenticates the identity of the users and submits the certificate request to the CA. The quality of this authentication process determines the level of trust that can be placed in the certificates.

2.1.9.5 Certificate Distribution System

A certificate distribution system is the mechanism for delivering end-user certificates and their status to the parties that will need to rely on them. This is typically an LDAP directory acting as a repository for certificates and/or revocation lists and also may be an Online Certificate Status Protocol (OCSP) responder that delivers certificate status.

2.1.9.6 PKI-enabled applications

A PKI is a means to an end, providing the security framework by which PKI-enabled applications can be confidently deployed to achieve the end benefits. Examples of applications are:

2.1.10 Communications between web servers and browsers

2.1.11 Email

2.1.12 Electronic Data Interchange (EDI)

2.1.13 Credit card transactions over the Internet

2.1.14 Virtual Private Networks (VPN)

2.2 Methods of Use

2.2.1 Within a PKI, the policies under which certificates are issued determine the level of confidence other parties will have in the certificates issued by a CA, and are normally published in a Certification Practice Statement (CPS). This states the policies for issuing various levels of certificates and the registration process that people must go though in order to obtain a certificate.

2.2.2 UniCERT is designed to accommodate the requirements of a wide variety of CPSs. In particular, the registration process may involve the acquisition and verification of a variety of data from users, directly in face-to-face requests or indirectly in remote requests via the UniCERT Protocol Handler, e.g., web browser, email and VPN.

2.2.3 UniCERT's unique Registration Policy editor enables you to be able to set up details of:

- How the registration process is to be done
- Information that needs to be checked or recorded
- The number of keys and hence certificates that are to be generated (typically separate keys are generated for signing and encryption purposes)
- Where and on what media the keys are to be generated, keys can be generated by the end user or by the WebRAO user, and can be stored on diskette, disk, smart card or token.
- Format of certificates that are to be produced
- The number of authorizers required to accept a certification request
- Additional business information to be collected during the registration process.

2.2.4 Face-to-Face Registration

2.2.4.1 For some PKI implementations, a direct registration system is the only secure means to correctly authenticate users and distribute/generate keys and certificates. In an Intranet environment, an organization may implement a policy whereby users must visit a security officer personally to receive a disk or smart card with their keys and certificates. This registration may involve the candidate showing an employee ID card, driver's license, passport or other means of identification.

2.2.4.2 In an Internet environment, organizations with public offices such as banks, post offices, etc. may require customers to present themselves at a branch or retail counter. UniCERT includes a face-to-face registration system, which offers a simple, easy-to-use Windows interfaces.

2.2.4.3 The person using the WebRAO program enters an end user's details and accepts or rejects the candidate's application. Keys can either be generated by the WebRAO program and are secured using a passphrase entered by the applicant, or the applicant can generate their own keys, and provide the public key to the WebRAO.

2.2.4.4 Once the certificate is processed, the certificate can be saved on a smart card or disk and given to the user.

2.2.5 Remote Registration

2.2.5.1 In many cases, a method of registration other than face-to-face is required, where the user is remote from the WebRAO, and wants to submit their registration request from a browser, email or VPN. In these cases the registration request is sent via the UniCERT Protocol Handlers, and the request is stored at the RA. A WebRAO user can then authorize the request in the same way as when doing face-to-face registration.

2.2.5.2 Alternatively, if allowed by the registration policy, the RA can send requests received from the UniCERT Protocol Handler automatically to the CA without being authorized by a WebRAO user. Registration policies that allow this are not permitted in the evaluated configuration.

2.2.6 Custom Registration

2.2.6.1 Another of the features that make UniCERT flexible is that custom registration processes can be built, typically using the UniCERT ARM or Cybertrust KeyTools. This may be done where it is required for the registration process to interact with another application or database, for example a human resources database. However, note that the ARM is outside of the evaluation and cannot be used with the product when it is in its evaluated configuration.

2.2.7 Certificate Distribution

2.2.7.1 Certificate distribution is one of the primary functions that a PKI must be able to perform in a flexible manner. There are three separate types of certificate distribution: Issued certificates need to be delivered to the requestor, the CA certificate needs to be exportable and published, it may also be necessary to put end-user certificates in a directory to allow other end-users access to them. All of this has to be done in a fashion that suits the end-user and utilizes the organization's infrastructure.

2.2.7.2 End-user certificates must be provided to the requestor by a method and in a format that matches the requestor requirements. UniCERT has the flexibility to issue certificates in a wide variety of formats and to deliver them by suitable mechanisms, the Registration Policy controls this. Typically, certificates dealt with in a face-to-face manner are distributed either in software or on cryptographic hardware e.g., smart cards and requests that have come remotely are distributed by the same method in which they were received: email, HTTP or sockets. However using the Registration Policy, alternative distribution mechanisms can be used.

2.2.7.3 The CA certificate typically needs to be made as public as possible. End-users must be able to download the CA certificate and manually trust it before they can take advantage of the services offered by the PKI. The CA certificate within UniCERT can be exported in a variety of different formats, and is included in PKCS#12 and PKCS#7 responses to end-users. If an X.500 or LDAP directory is being utilized then the certificate can be published to the directory using the Publisher.

2.2.7.4 The use of a directory in conjunction with UniCERT is optional but adds considerable functionality. In order to encrypt messages it is necessary to have the recipient's certificate. In order to verify a signature one must have access to the signer's certificate. For these two reasons it is common to store certificates and revocation information (CRLs) in a directory. This directory is made accessible to the user group.

2.2.7.5 The UniCERT Publisher handles all publishing. This is standards based and can be configured to use the lightweight directory access protocol (LDAP). This allows the PKI to take advantage of an already existing directory and gives maximum flexibility if a new one is required. UniCERT has a flexible schema in order to fit in with a corporate structure.

2.2.7.6 UniCERT also allows certificates and CRLs to be published to disk. This opens up possibilities for custom publication mechanisms to be implemented outside of the CA; however, the Publisher provides very flexible publishing capabilities.

2.2.8 Ease of Use

2.2.8.1 The "cost of ownership" of a CA system should always be considered before purchasing. Apart from the cost of the hardware and software components, issues such as training, maintenance, configuration and management function need to be considered. All modules run on standard operating systems, i.e., Windows, which are familiar to most computer users (the server components also run on Solaris). UniCERT is entirely controlled by graphical user interfaces (GUIs) that allow for a very short training cycle. Informational and instructional messages can be included within the policy to inform the user of correct procedure.

2.2.9 Configuration

2.2.9.1 UniCERT CAO offers a GUI based PKI editor, Registration Policy editor and Operational Policy editor. This eliminates the need for complicated file configurations and also allows users to quickly verify configuration details.

These facilities enable centralized (or regional) control with distributed authority. Cybertrust's philosophy of securely pushing registration and operation policies to the other UniCERT modules is in line with network-centric computing. This minimizes administration costs and reduces the risk of errors.

2.2.10 Auditing

2.2.10.1 UniCERT maintains a number of different system logs, which detail a number of system and user actions. These logs can be viewed through UniCERT screens and complex reports can be done through the use of SQL. All the database logs are signed by the entity logging the information and are verifiable via the GUI screens.

2.2.11 Backup and Recovery

2.2.11.1 No form of cryptography can ever protect against data loss. Any business critical PKI implementation needs to put in place the procedures and policies necessary to ensure that all data can be restored.

2.2.11.2 In order to restore UniCERT 5, the cryptographic tokens, PSEs, data and system configurations are required; these should be backed up and kept secure.

2.2.11.3 UniCERT stores its data, and audit events in a database. UniCERT uses Oracle as its database. Oracle supports many advanced features for the backup and restoration of data. These should be used to support the backup and restoration of the PKI.

2.2.12 Cloning and Continuity

2.2.12.1 UniCERT 5 support cloning this is where a component such as the CA, can be duplicated, either locally to share the processing load, or remotely to provide a continuity of service should a site or its host computer fail.

2.2.12.2 A cloned component will share the same tokens, database account and certificate, but may be on the same machine (on a different port) or different machine. The database may be put in failsafe mode, replicated, or kept synchronized using the various Oracle recommended techniques.

2.2.12.3 The use of clones is transparent to the user, since a certificate issued by a cloned system, or involving cloned components, will be identical.

2.3 Product Components

2.3.1 UniCERT 5 components can be broken down into core components and utilities that are provided with the basic CA and RA management installations. In addition a number of Advanced Components can be used with UniCERT 5 such as the Key Archive Server and the Advanced Registration Module, but these modules are not included as part of this evaluation.

2.3.2 The UniCERT 5 core components can be further sub-divided into Certification Authority components and Registration Authority components.

2.3.3 The Certification Authority components are responsible for the generation and publication of certificates and certificate revocation lists, and for the overall management of the PKI. The components are as follows:

- Certification Authority (CA) service
- CA Operator (CAO)
- Publisher (not part of the TOE)
- Certificate Status Server (CSS)

The relationship between these components is shown diagrammatically in Figure 2-1.

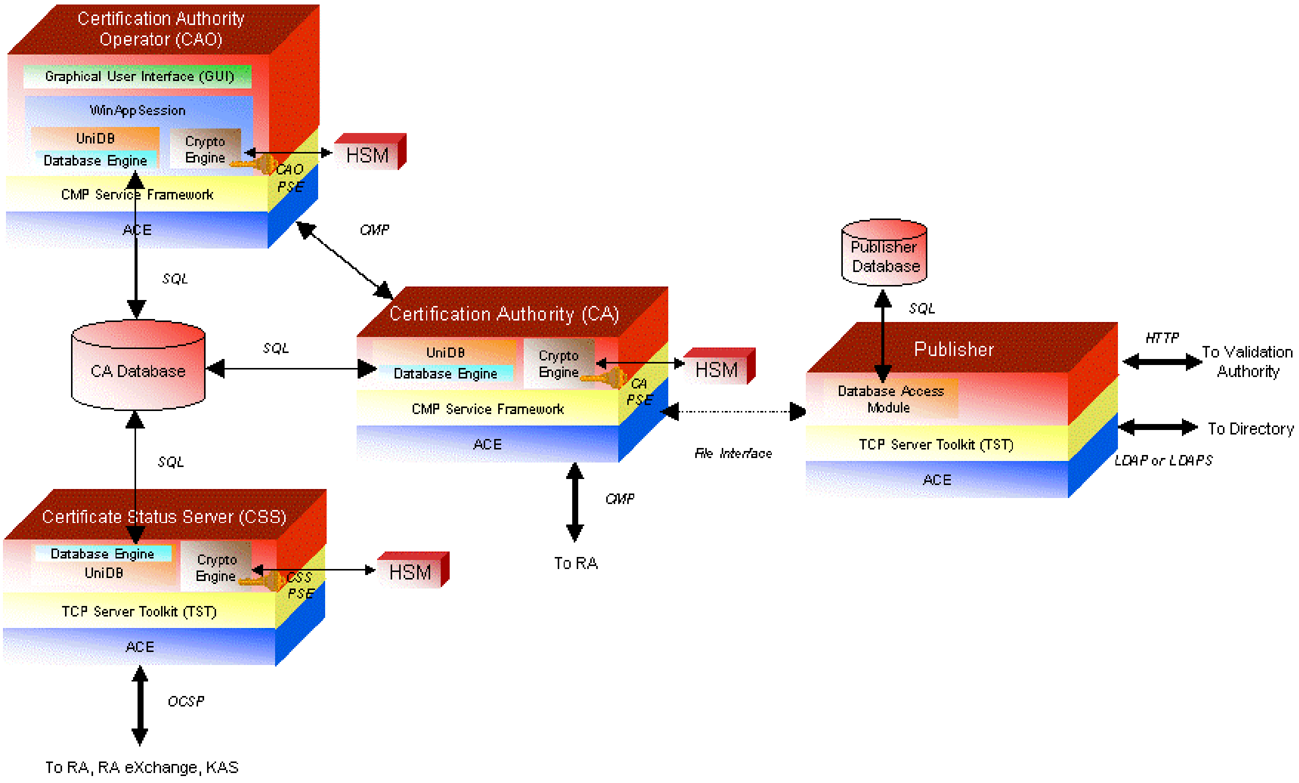

Figure 2-1 Certification Authority Components and Interface

2.3.4 The Registration Authority components are responsible for gathering registration information and revocation requests, authorizing requests, and handling renewals. The control over what registration authority components are allowed to do is provided by the Certification Authority components. The Registration Authority components are as follows:

- Registration Authority (RA) service
- The RA Event Viewer
- RA eXchange
- The protocol handlers: Web Handler, email Handler, SCEP Handler, and CMP Handler (the CMP Handler is out of scope of the evaluation.)
- Web RA Operator (WebRAO)

The relationship between these components is shown diagrammatically in Figure 2-2.

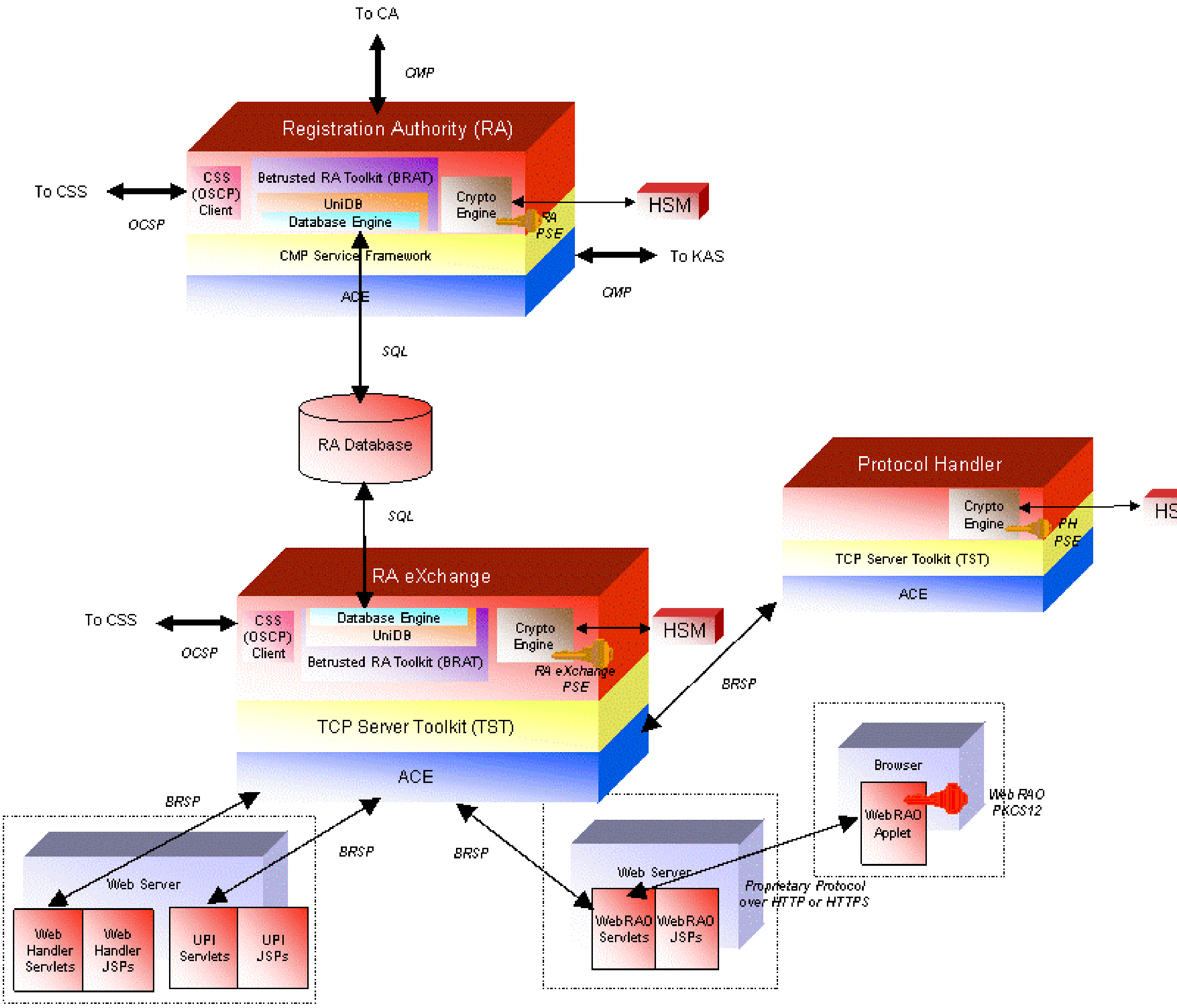

Figure 2-2 Registration Authority Components and Interface

2.3.5 UniCERT 5 utilities are as follows

- Database Wizard
- Key Generator

- Token Manager
- Service Manager

2.3.6 Certification Authority (CA)

2.3.6.1 Description of the CA Component of the TOE

The UniCERT CA is the highest hierarchical element in the UniCERT PKI. Its primary purpose is to sign and issue digital certificates, which provide a means of exchanging electronic information securely.

The Certification Authority (CA) module is the nucleus of a PKI. All trust within the infrastructure depends upon the CA's signature. The CA operates according to its own flexible operational policy, which is controlled using the Certification Authority Operator (CAO).

The functionality of the CA is as follows (note that the functions referred to are further described later in this document, in the TOE Summary Specification):

a) On starting up the CA user must identify themselves by choosing a key and accessing it by using a PIN or passphrase (IA_Identify).
b) When this is successfully done, the CA retrieves the latest PKI from the CA database and verifies it against its signature (it is stored with the signature of the CAO user that updated it) using the function PP_PKIVerify. If the latest PKI is not verifiable then processing stops with an error message. If no PKI exists in the database then the CAO user is required to use functionality described in the CAO section to create the PKI.
c) The CA checks the CRL in its database to ensure that it exists and has not expired. If either of these conditions is true then it generates a new one and signs it, updating the database as it does so using the function CR_Publish_Rev_Cert_Status.
d) The CA uses the retrieved PKI to identify and authenticate both it's own user, and all other entities that attempt to communicate to it when such communications are initiated, using the function IA_Authenticate to ensure that all of these entities are in the PKI and have valid, current certificates.
e) The CA uses CP_Authenticate to continue to authenticate those connections. It disconnects any connections made by entities that are not in the PKI or otherwise cannot be authenticated using the function CP_Disconnect.
f) The CA receives approved certificate requests from Registration Authorities (RAs) and CAOs, and returns certificates and an indication of success or error using the function CG_Generate.
g) Using CG_Generate, the CA signs all certificates that it generates and stores them in the CA database. If requested, CG_Generate can check that all certificates being generated have a unique DN and/or public key before producing a certificate – if requested to do this check, and one of these items is not unique, then it will not produce a certificate but will return an error. CG_Generate also maintains this information in the CA database so that it can continue to perform this check when requested to do so.
h) The CA receives approved revocation requests from Registration Authorities (RAs) and CAOs, and responds to them, using the functions CR_Suspend, CR_Revoke, or CR_Unsuspend, as appropriate. Note that certificates are

both suspended and unsuspended using a revocation request from a RA. These functions will result either in the certificate's status being changed in the CA's database as requested and an indication of success, or an indication of an error.

i) The CA signs the PKI using the function PP_PKIProtect prior to sending it to the RA (or KAS) using the PP_PKIExport function.

j) The CA can sign and publish CRLs, partitioned CRLs (CDPs) and ARLs to either the CA database or disk files using the function CR_Publish_Rev_Cert_Status. This can be done immediately, or by scheduling it using records in the CA database via CR_Publish_Rev_Cert_Status. The information in the disk files can then be published by UniCERT Publisher (which is not part of the TOE).

k) Message Signing – using the functions CP_Protect and CP_Origin, all messages sent by the CA are digitally signed with the CA's private key.

l) Message Verification - the CA verifies all messages it receives to ensure integrity and authenticity using the function CP_Verify. If any do not verify correctly they are discarded by that function and the connection is disconnected using CP_Disconnect.

m) Audit logging – audit records (as listed in Table 5-1) are stored by the CA in the CA's database by the functions AL_Logging and AL_Integrity. AL_Integrity is used to ensure that all audit log information stored is digitally signed by the CA, and each entry has a unique tracking number.

2.3.6.2 Features

a) Multi-language support (Unicode)

b) Extensive hardware security module (HSM) support.

c) Multiple key pairs – optionally the CA can have individual key pairs for each of its functions: certificate signing, CRL signing, digital signature and non-repudiation. Key usage can be grouped and combined as required.

d) Variable CRL publication time.

e) Supports RSA (up to 4096 bits) and DSA key pairs.

2.3.7 Certification Authority Operator (CAO)

2.3.7.1 Description of the CAO Component of the TOE

The Certification Authority Operator (CAO) module provides a GUI that the administrator of the PKI uses to configure the PKI. The CAO's purpose is to allow its user to control all of the administration functions and grant privileges to other UniCERT modules and users. There can be multiple CAO users each with diminished rights if distributed control is required.

The functionality of the CAO is as follows (note that the functions referred to are further described later in this document, in the TOE Summary Specification):

a) On starting up the CAO user is requested to identify themselves by choosing a key and accessing it by using a PIN or passphrase (IA_Identify). They can choose to not do so, which allows them to either create a new PKI, or work on registration policies, saving them to external files, using the functions described later in this section.

b) When the user has identified themselves with a private key and chosen a PKI to work on, the CAO retrieves the PKI from the CA database and verifies it using PP_PKIVerify. The settings within the PKI for the CAO user define the CAO user's permissions within that PKI and describe how the CAO should communicate to the CA entity.

c) The CAO then checks that it is in the retrieved PKI and has a valid and current certificate using the function IA_Authenticate.

d) Registration Policies control the information to be collected and processes used to issue certificates. The CAO provides facilities for working on Registration Policies as follows:

    i) The CAO user can create and maintain these policies using the function PG_PolicyConfigure to edit them and save them to the database.

    ii) The policies may be exported to disk for backup or to the other PKI entities using the function PG_PolicyExport: this function puts them into a format suitable for transmission or storage and writes them to disk or exports them to the entity that requires them.

    iii) Registration Policies may be retired or deleted when no longer required using the function PG_PolicyRetire and PG_PolicyDelete. When retired, they are marked as such in the CA's database but not deleted, so that they cannot be used for new registration requests but can still be referenced. They can only be deleted from the database by PG_PolicyDelete if they have not been published or used to register certificates at the CAO – if either of these conditions is true they can only be retired.

    iv) Registration Policies may also be configured in various ways, for example they can be assigned to Authorization Groups (see below) using PG_PolicyConfigure. Any changes made in this area are stored as part of the policy in the CA database.

    v) PG_PolicyImport is used to import registration policies from files that they had been exported to using PG_PolicyExport.

e) The CAO can be used to create Authorization Groups with the function GG_Create. It can then be used to assign WebRAO users to Authorization Groups (or remove them from those groups) using the function GG_Modify. Authorization Groups may also be marked as retired in the database, which stops them from still being used, while allowing reference to them – this is done by the function GG_Retire. Authorization group information is stored in the CA database by these functions.

f) The CAO is used to create and modify the PKI, using the functions PP_PKICreate and PP_PKIModify. When this is done, the PKI is stored in the CA database, signed with the CAO user's key using the function PP_PKIProtect. When the PKI is extracted for any reason it is verified against this signature using the function PP_PKIVerify.

g) Entities (including TOE administrator accounts and a hierarchy of CAs) can be created and updated by CAO facilities via the function PP_EntityModify. Not all of these "PKI entities" will always be part of a PKI – they may be registered as part of a PKI using PP_EntityRegister. They will all be stored in the CA database, and may be deleted when no longer required using PP_EntityDelete. The certificates created by the TOE are never deleted from the CA's database, but information about the entities that own them may be deleted.

h) The CAO is used to register and submit requests for certificates. This registration is done using the function CG_Register (for PKI entities) or CG_Request (for end entities, which may include certificate renewals), which is then authorized and submitted as a request to the CA (using CG_Authorize), which will generate the certificate. The generation, authorization and request all result in updating the CA's database to reflect these actions, and the request is sent to the CA using the communication channel between the CA and CAO. This process may involve the generation of keys for these entities using the function KG_Generate.

i) As well as generating keys, the CAO provides functionality to split access to keys via KG_Split, and to export keys in a protected manner via KG_Export. The CAO will also securely destroy all keys it holds in memory using KG_Destroy.

j) The CAO can be used to authorize the revocation of any certificate (note that revocation requests include requests to suspend and unsuspend) using the function CR_Authorize. Authorized revocation requests are communicated to the CA (which performs the requested action) using the function CR_Request.

k) Message Signing – using the functions CP_Protect and CP_Origin, all messages sent by the CAO are digitally signed with the CAO user's private key.

l) Message Verification - the CAO verifies all messages it receives to ensure integrity and authenticity using the function CP_Verify. If any do not verify correctly then the messages are discarded.

m) Audit logging – audit records (as listed in Table 5-2) are stored by the CAO in the CA's database by the functions AL_Logging and AL_Integrity. AL_Integrity is used to ensure that all audit log information stored is digitally signed by the CA, and each entry has a unique tracking number.

n) The CAO can be used to selectively view the audit records stored in the CA's database using AL_Selection. CAO users that have been assigned the correct permissions, can also check the integrity of audit records (AL_Integrity) and archive those audit records using AL_Archive, while still preserving the integrity of the audit log.

o) A CAO user can request the CA to publish CRLs, partitioned CRLs (CDPs) and ARLs to disk files using the function CR_Publish_Rev_Cert_Status.

p) A CAO user with the requisite permissions can use the function AL_CreateAuditor to assign (or remove assignations of) auditor roles to administrators. (If assigned the appropriate auditor roles, the administrator is able to review and/or archive records from either or both of the CA and/or RA databases as described elsewhere.) A CAO user cannot provide another CAO user with greater permissions than they have themselves.

2.3.7.2 Features

a) Multi-language support (Unicode)

b) CAO keys can be kept in a range of smart cards/tokens or in software.

c) Publication of CRL can be forced for immediate revocation

d) Easy to use GUI.

e) Log and certificate tracking interface.
f) Certificate and CRL retrieval.
g) Diminished roles – an individual CAO user can have limited privileges.

2.3.8 Certificate Status Server (CSS)

2.3.8.1 Description of the CSS Component of the TOE

The purpose of the CSS is to provide real-time certificate status information to the other UniCERT components. The CSS acts as a server listening for network connections. When a connection is established, the CSS checks for Online Certificate Status Protocols (OCSP) requests. The CSS responds to OCSP request message by sending OCSP response messages containing the status of each certificate listed in the request.

The functionality of the CSS is as follows (note that the functions referred to are further described later in this document, in the TOE Summary Specification):

a) On starting up the CSS user must identify themselves by choosing a key and accessing it by using a PIN or passphrase (IA_Identify).
b) When this is successfully done, the CSS retrieves the latest PKI from the CA database and verifies it against its signature using the function PP_PKIVerify. If there is no PKI or the latest PKI is not verifiable then processing stops with an error message.
c) The CSS then checks that it is in the retrieved PKI and has a valid and current certificate in order to identify and authenticate itself, using the function IA_Authenticate.
d) The CSS then responds to requests for certificate status and provides real time information on the status of the certificate using the function CR_Publish_Rev_Cert_Status
e) Message Signing – using the functions CP_Protect and CP_Origin, all messages sent by the CSS are digitally signed with the CSS user's private key.

2.3.9 UniCERT Publisher (NOT part of the TOE, but can be run with the TOE)

2.3.9.1 Description of UniCERT Publisher

The Publisher handles all the publishing requirements of the CA, including the ability to publish to a wide range of different directories (including Microsoft's Active directory) and OCSP responders, and to be able to publish to multiple directories. It supports flexible publishing schemas, and has the ability to only publish certain types of certificates. It takes files that can be output by the CA component and publishes them if requested to do so by an administrator. The UniCERT Publisher does not implement core UniCERT security functionality, and so has not been included as part of the TOE.

The functionality of the UniCERT Publisher is as follows:

a) Publication of CA certificates – the Publisher optionally publishes its CA certificates to one or more LDAP connected directories.

b) Publication of CRLs and ARLs – the Publisher optionally publishes CRLs and ARLs to one or more LDAP connected directories.
c) Publication of End Entity certificates – the Publisher optionally publishes end entity certificates to one or more LDAP connected directories. Control of whether end entities certificates are published is done via configurable filters.
d) Publication of CRLs to OCSP responder – the Publisher optionally publishes CRLs to Online Certification Status Protocol (OCSP) servers.

2.3.9.2 Features

a) Multi-language support (Unicode)
b) LDAP support
c) Extensive support for different directories
d) When certificates are published, other attributes can also be published
e) Configurable Filters to control which end entity certificates are published
f) Publication of CRLs to OCSP responders

2.3.10 Registration Authority (RA)

2.3.10.1 Description of the RA Component of the TOE

The purpose of the Registration Authority (RA) is to act as a router between RA Operators (WebRAOs), Protocol handlers and the CA.

The functionality of the RA is as follows (note that the functions referred to are further described later in this document, in the TOE Summary Specification):

a) On starting up the RA user must identify themselves by choosing a key and accessing it by using a PIN or passphrase (IA_Identify).
b) Then, using PP_PKIVerify the RA attempts to retrieve the PKI from the RA database, and also requests it from the CA (the CA sends it using PP_PKIExport). The RA requests the PKI from the CA so as to ensure that it has the most up-to-date copy (and updates the RA database with this copy if not). When the PKI is obtained the RA verifies it.
c) The RA then uses the retrieved PKI to identify and authenticate both it's own user and all entities that attempt to communicate to it when such communications are initiated, using the function IA_Authenticate.
d) It also uses CP_Authenticate to continue to authenticate those connections. It disconnects any connections made by entities that are not in the PKI or otherwise cannot be authenticated using the function CP_Disconnect.
e) The RA checks the RA database for processed requests and then communicates any approved end-user certificate and revocation requests received from the WebRAO users to the CA. It receives certificates and confirmation (or error) messages from the CA and makes them available to the WebRAO users, via the RA eXchange. It updates the database to reflect the request status of the certificates that it receives from the CA as it distributes them. The security-enforcing part of this functionality is performed by CG_Distribute.

f) If selected in the registration policy, the RA sends end users' private encryption keys that are marked to be archived to the Key Archive Server (KAS). These will have been encrypted by the WebRAO.

g) The RA is responsible for initiating end-user certificate rollover, when an end-user's certificate is about to expire and the associated registration policy dictates that a new certificate is to be issued. This is performed by the function CG_Request.

h) The RA securely destroys all private keys it holds in memory using the function KG_Destroy.

i) Message Verification - the RA verifies all messages it receives to ensure integrity and authenticity using the function CP_Verify. If any do not verify correctly they are discarded by that function and the connection is disconnected using CP_Disconnect.

j) Message Signing – using the functions CP_Protect and CP_Origin, all messages sent by the RA are digitally signed with the RA's private key.

k) Audit logging – audit records (as listed in Table 5-3) are stored by the RA in the RA's database by the functions AL_Logging and AL_Integrity. AL_Integrity is used to ensure that all audit log information stored is digitally signed by the RA, and each entry has a unique tracking number.

l) Security-relevant data (i.e., certificate request history) that is stored by the RA in the RA's database is protected by the function DP_Store using a digital signature. It is verified against its signature when retrieved, by the function DP_Verify.

2.3.10.2 Features

a) Multi-language support (Unicode)

b) Extensive HSM support

2.3.11 RA eXchange (RAX)

2.3.11.1 Description of the RA eXchange Component of the TOE

The purpose of the RA eXchange is to provide a communication link between the RA and the Protocol Handlers, WebRAOs and Web Handler. The RA eXchange acts as an entry point into UniCERT's RA, in particular, the RA's database. It is the server that receives requests, retrieves or inserts data into the RA's database according to the request, and then returns an appropriate response.

The functionality of the RA eXchange is as follows (note that the functions referred to are further described later in this document, in the TOE Summary Specification):

a) On starting up the RA eXchange user must identify themselves by choosing a key and accessing it by using a PIN or passphrase (IA_Identify).

b) The RA eXchange then retrieves the PKI from the RA database and verifies it using PP_PKIVerify.

c) It checks that it is in the PKI, and has a valid and current certificate, using IA_Authenticate, and, if not, it shuts down. Otherwise it then uses the retrieved PKI to identify and authenticate all entities that attempt to communicate to it when such communications are initiated, using the function IA_Authenticate respectively. It also uses CP_Authenticate to continue to authenticate those connections. It disconnects any connections made by entities that are not in the PKI or otherwise cannot be authenticated using the function CP_Disconnect.

d) The RA eXchange receives certificate and revocation requests from the Protocol Handlers and passes them to WebRAO users for authorization, and sends certificates and informational messages back to the Protocol Handlers. This is done using the functions CP_Verify, CG_Distribute and CP_Protect.

e) Message Verification - the RA eXchange verifies all signed messages it receives to ensure integrity and authenticity using the function CP_Verify. If any of these do not verify correctly they are discarded by that function and the connection is disconnected using CP_Disconnect.

f) Security-relevant data (i.e., certificate requests) that is stored by the RA eXchange in the RA's database is protected by the function DP_Store using the RA eXchange user's digital signature. It is verified against its signature when retrieved, by the function DP_Verify.

g) Audit logging – audit records (as listed in Table 5-4) are stored by the RA eXchange in the RA's database by the functions AL_Logging and AL_Integrity. AL_Integrity is used to ensure that all audit log information stored is digitally signed by the RA eXchange user, and each entry has a unique tracking number.

2.3.11.2 Features

a) Multi-language support (Unicode).

2.3.12 RA Event Viewer (RAE)

2.3.12.1 Description of the RA Event Viewer Component of the TOE

The purpose of the RA Event Viewer is to provide a GUI for retrieving and performing limited actions on the audit events from the RA database. All Registration Authority Components provide audit event records that are stored in the RA database.

The functionality of the RA Event Viewer is as follows (note that the functions referred to are further described later in this document, in the TOE Summary Specification):

a) On starting up the RA Event Viewer user must identify themselves by choosing a key and accessing it by using a PIN or passphrase (IA_Identify).

b) The RA Event Viewer then retrieves the PKI from the RA database and verifies it using PP_PKIVerify. It checks that its own user is in the PKI and has a valid and current certificate, using IA_Authenticate, and, if not, it shuts down. It also obtains the permissions of the current user from the PKI to determine their ability to use the RA Event Viewer.

c) The RA Event Viewer allows a RA Event Viewer user to review all, or a selection of audit records in the audit log table or all records in an audit log archive file using the function AL_Selection. This function selects audit records from the RA database according to criteria entered by the RA Event Viewer user and displays them to the RA Event Viewer user, or displays all the content of an audit log file.

d) The RA Event Viewer allows the RA Event Viewer user to confirm the integrity of the audit records using the function AL_Integrity. AL_Integrity checks the signatures on the audit records to do this.

e) The RA Event Viewer allows a RA Event Viewer user with the required permissions to archive part of the audit log whilst maintaining its integrity by using the function AL_Archive. This function moves the selected records from the standard audit log table in the RA database to an archive log file.

f) Audit logging – audit records are stored by the RA Event Viewer in the RA's database by the functions AL_Logging and AL_Integrity. AL_Integrity is used to ensure that all audit log information stored is digitally signed by the RA Event Viewer user, and each entry has a unique tracking number.

2.3.12.2 Features

g) Multi-language support (Unicode)

2.3.13 WebRAO

2.3.13.1 Description of the WebRAO Component of the TOE

The purpose of the WebRAO is to enable its users to authorize certification and revocation requests. These requests will have been sent from the Protocol Handlers, or from other WebRAO users. WebRAO users can also handle face-to-face registrations. . The WebRAO users belong to one or a number of Authorization Groups, and can only process requests associated with specific registration policies that have been assigned to their Authorization Groups by CAOs.

In the evaluated configuration of UniCERT v5, the WebRAO component can be used with SSL turned on to provide another layer of security to your PKI installation, but UniCERT v5 is not dependent on SSL or any other feature of the browser or the web server to achieve its security objectives.

The functionality of the WebRAO is as follows (note that the functions referred to are further described later in this document, in the TOE Summary Specification):

a) On starting up the WebRAO user must identify themselves by choosing a key and accessing it by using a PIN or passphrase (IA_Identify).

b) The WebRAO can be used to generate and authorize certificate requests using Registration Policies, which have been defined by the CAO users, for their Authorization Group. This is done using CG_Request and CG_Authorize respectively, and results in entries being made in the RA database (by the RA eXchange) to reflect these actions. The certificate requests can be made face-to-face, or can be sent to the WebRAO user from other WebRAO users or from the Protocol Handlers. Using CG_Distribute, the WebRAO can retrieve the certificates from the RA DB and distribute the generated certificates to those that should receive them.

c) The WebRAO user can also place a registration request using CG_Register. This allows the WebRAO user to register another PKI entity (note that the only other PKI entities that WebRAOs can register are other WebRAOs), and results in a request going to the CA to issue a certificate for the PKI entity using the same functionality as for CG_Request and CG_Authorize.

d) The WebRAO may be used to generate end user keys on a token or in software as part of this activity, using the function KG_Generate. It may also be used to export keys via the function KG_Export. The WebRAO will securely delete all keys that it holds in memory after use, via the function KG_Destroy. If the registration policy being used to generate the certificate specifies that the private key will be archived, then the WebRAO encrypts the private key before sending it with the certificate request (DP_KeyExport).

e) The WebRAO may also be used to reject a certification request. This is performed using the function CG_Authorize.

f) Under the control of the Registration Policies, the WebRAO can be used to provide additional authorization for certification requests received from other WebRAOs using the function CG_Authorize.

g) The WebRAO can be used to authorize or reject the revocation of a certificate (note that revocation requests include requests to suspend and unsuspend) with the function CR_Authorize. Authorized revocation requests are communicated to the CA (which performs the requested action) using the function CR_Request.

h) The WebRAO user can obtain certificate status using the function CR_Publish_Rev_Cert_Status.

i) Message Signing – using the functions CP_Protect and CP_Origin, messages sent by the WebRAO, which are important to the security objectives of the TOE, are digitally signed with the WebRAO user's private key.

2.3.13.2 Features

a) Multi-language support (Unicode)

b) WebRAO keys can be kept in a range of smart cards/tokens or in software.

c) Easy to use GUI.

d) Certificate tracking interface.

e) Extensive smart card support.

2.3.14 Protocol Handlers (PH)

2.3.14.1 Description of the PH Component of the TOE

The PH is an extensible set of request handlers, whose purpose is to handle certification requests using such protocols as Web, email, Cisco SCEP and PKIX CMP (although the PKIX CMP handler is not included in the evaluation and cannot be run in the evaluated configuration).

The Protocol Handlers handle the complexities of the various certificate management protocols, and pass the registration (or revocation) requests into the RA using a common internal format. Each request is automatically associated with a registration policy by the PH (which is then used to control it authorization path etc.)

If allowed by the registration policy, the Protocol Handlers receive the certificates back from the RA and communicate them to the end user according to the methods allowed by the protocol handler.

The functionality of the PH component is as follows (note that the functions referred to are further described later in this document, in the TOE Summary Specification):

a) On starting up the PH (except for the Web Handler) demands that its user identifies themselves by choosing a key and accessing it by using a PIN or passphrase (IA_Identify). If this is successful, it retrieves the PKI from the RA database via the RA eXchange and verifies it using PP_PKIVerify. It checks that its user is in the PKI, using IA_Authenticate, and, if not, it shuts down, disconnecting its own communications using CP_Disconnect.

b) The email PH provides the following functionality:

- It retrieves certificate requests in PKCS#10 or PEM format from a POP3 store and submits them using CG_Request. The email PH sends back certificates in PKCS#7 (certificate chain), X.509 (binary) or PEM format via a SMTP server using CG_Distribute.
- The email PH also distributes email notices, where these have been set up in a registration policy (note that this is not security functionality)
- Email notices can be configured to be sent out for any of the following status (note that this is not security functionality):
    - Pending - certificate request has been received into system,
    - Rejection - certificate request has been rejected,
    - Pickup - send out a URL where the certificate can be retrieved,
    - Expiry Warning Reminder - warns that a certificate is about to expire,
    - Certificate - which includes a certificate in response to a certificate request (which may have been requested by another registration method), or from auto renewal via the system.
    - Key Archival - successful archive of private key pair at Key Archive Server (KAS)

c) The Web PH provides the following functionality:

- It provides registration pages, which are dynamically built from the registration policies. Via these request pages customers may request certificates via the major browsers (Netscape and Microsoft IE) and via PKI-aware applications capable of generating PKCS#10 certificate requests (e.g., Web servers). This functionality is provided using CG_Request.
- Using the function CG_Distribute, the Web PH is able to distribute certificates that have been requested via the Web PH, or where web distribution has been configured in a registration policy.
- Where allowed by the registration policy, the Web PH supports end-user revocation by providing revocation specific web pages. End users may revoke or suspend their own certificate and must supply a password in order to perform this function, which is supplied by the function CR_Request.
- The Web PH also enables users to query the status of the certificate, and to down load CRLs via the function CR_Publish_Rev_Cert_Status.

d) The SCEP PH (SCEP - Simple Certificate Enrolment Protocol - is the certificate request and retrieval method used by Cisco and other VPN vendor devices and software – defined in [SCEP]):

- receives SCEP requests directly by sockets and generates certificate requests to the CA using CG_Request
- returns the certificate in the same manner using CG_Distribute.

2.3.14.2 Features

a) Multi-language support (Unicode)

2.3.15 UniCERT Utilities

UniCERT also contains a number of utilities for handling such things as token management, key generation, database setup, and service management. These are described below.

2.3.16 Token Manager Utility (TM)

2.3.16.1 Description of the Token Manager Component of the TOE

The purpose of the Token Manager is to allow an administrator to manage the various personal secure environments (PSEs) used in PKIs. The Token Manger is a stand-alone module that manages software and hardware (smart cards and HSMs) PSEs.

The functionality of the Token Manager component is as follows (note that the functions referred to are further described later in this document, in the TOE Summary Specification):

a) The Token Manager initializes tokens before they are used. This process protects the token with a PIN.
b) The Token Manager is responsible for changing the PINs on tokens. This is done by the function KG_Update.
c) The Token Manager is used to change the passphrase that protects keys stored in software. This is done by the function KG_Update.
d) PSE files can be written to tokens using this module. These actions are performed by the DP_Export, KG_Update and KG_Export functions. This does not apply to when PSEs are copied from one location to another, for example when copying a PSE from a file to a token.
e) The Token Manager can split access to a key, based on user input, using the function KG_Split. The KG_Split function is not available on the Solaris version of the Token Manager.
f) The Token Manager can securely destroy a key with the function KG_Destroy.

2.3.16.2 Features

a) On Windows the Token Manager runs as a GUI, and on Solaris as a command line utility.

2.3.17 Service Manager Utility (SM)

2.3.17.1 Description of the Service Manager Component of the TOE

The purpose of the Service Manager is to provide an interface that allows an administrator to start and stop all of the server components e.g., the CA, CSS, RA, RA eXchange and PHs (except the Web Handler).

The functionality of the Service Manager component is as follows (note that the functions referred to are further described later in this document, in the TOE Summary Specification):

a) The Service Manager provides an interface that allows an administrator to start the server components of the TOE. When the administrator attempts to do so, the Service Manager uses parts of IA_Identify to allow the administrator to identify themselves to services. The identification action is performed by allowing the user to choose their key and provide a passphrase or PIN to open it. The other TOE components provide the identification and authentication mechanism – the only part of IA_Identify that the Service Manager provides is an interface to allow the user to choose the key and enter their PIN or passphrase and request to start the service – these are passed on to the relevant TOE component. Services may be added using the Service Manager, by selecting from a list of supported services
b) Multiple instances of each service can be started
c) Services can be configured to be started manually or automatically (but the automatic start option is not allowed in the evaluated configuration of the TOE)
d) The Service Manager also allows the user to stop services. The administrator is not required to re-authenticate before stopping services.

2.3.17.2 Features

a) On Windows the Service Manager runs as a GUI, and on Solaris as a command line utility

2.3.18 Database Wizard Utility (DBW)

2.3.18.1 Description of the Database Wizard Component of the TOE

The Database Wizard is used to initially create the Oracle tables, and to create database user accounts for the UniCERT users. . The Database Wizard only works on database to create or destroy user accounts and database instances for the TOE components and to configure the database structure. The Database Wizard is unable to modify the data, or the account privileges. It can be used to change the account password. The Database Wizard does not contain security functionality, and does not handle security relevant data, but only exists to assist an administrator begin working with the TOE.

2.3.19 Key Generator Utility (KGU)

2.3.19.1 Description of the Key Generator Component of the TOE

The main purpose of the Key Generator is to perform key generation for the UniCERT components such as the CA, RA, and Protocol Handlers, etc. Once the keys have been generated, a PKCS#10 can be sent to a CAO for certification. The CAO returns a PKCS#7, which is then imported using this utility. The Key

Generator supports both hardware based cryptographic devices (HSMs, smart cards) as well as software.

The functionality of the Key Generator component is as follows (note that the functions referred to are further described later in this document, in the TOE Summary Specification):

a) The Key Generator enables the PKI entities to request certificates from the CAO using the function CG_Register.
b) The Key Generator generates keys in both hardware-based cryptographic devices and software using the function KG_Generate.
c) The Key Generator securely exports software keys using the KG_Export function.
d) The Key Generator enables a key to be split into a number of components when saving a PSE to file or token. The Key Generator uses KG_Split to provide this functionality. The KG_Split function is not available on the Solaris version of the Key Generator.

2.3.19.2 Features

a) On Windows the Key Generator runs as a GUI, and on Solaris as a command line utility

2.4 UniCERT Configurations

2.4.1 The diagrams in this section show various ways that UniCERT can be configured so as to run with other products. All of these configurations are possible in the evaluated configuration of the product: the evaluated configuration includes all configurations running on all supported platforms, within the limitations described in this document.

2.4.2 Section 2.3 describes which of these items form the TOE. All other items shown are products that can be used with the TOE – i.e., the CA database, the Publisher, the smart cards, HSM (hardware security module), OCSP (Online Certificate Status Protocol) directory, LDAP (Lightweight Directory Access Protocol) directory, and RA database.

2.4.3 The following sections demonstrate some of the ways that the product can be installed.

2.4.4 Root CA Configuration

2.4.4.1 Figure 2-3 shows the CA, CAO, database and optionally Publisher on one system, optionally using an HSM for the CA, and a smart card for the CAO.

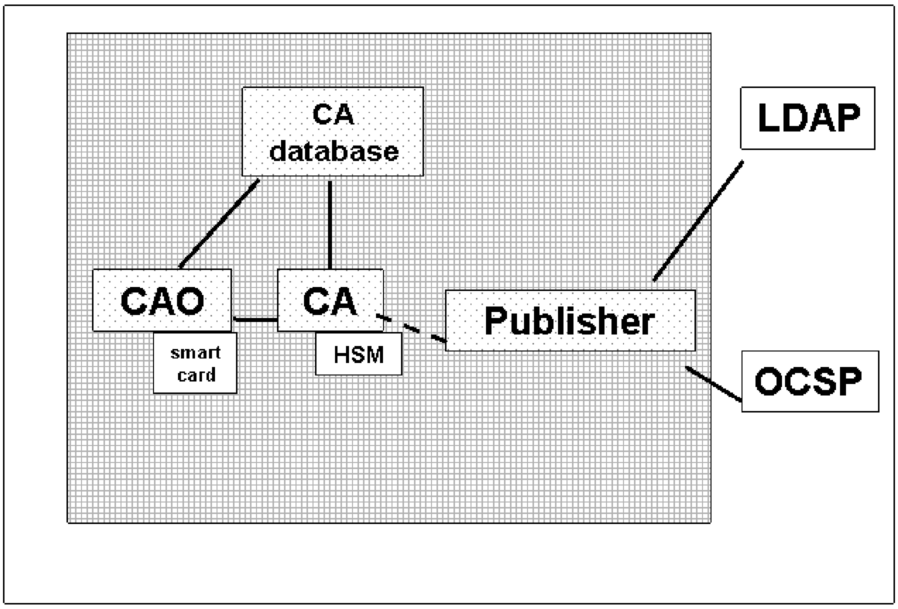

Figure 2-3 Root CA Configuration

2.4.5 Single CA/RA Configuration

2.4.5.1 Figure 2-4 shows all the components resident on one system, using software cryptography. Note that "Web Handler Servlets" form part of the Web Handler; "WebRAO Servlets" are part of the WebRAO.

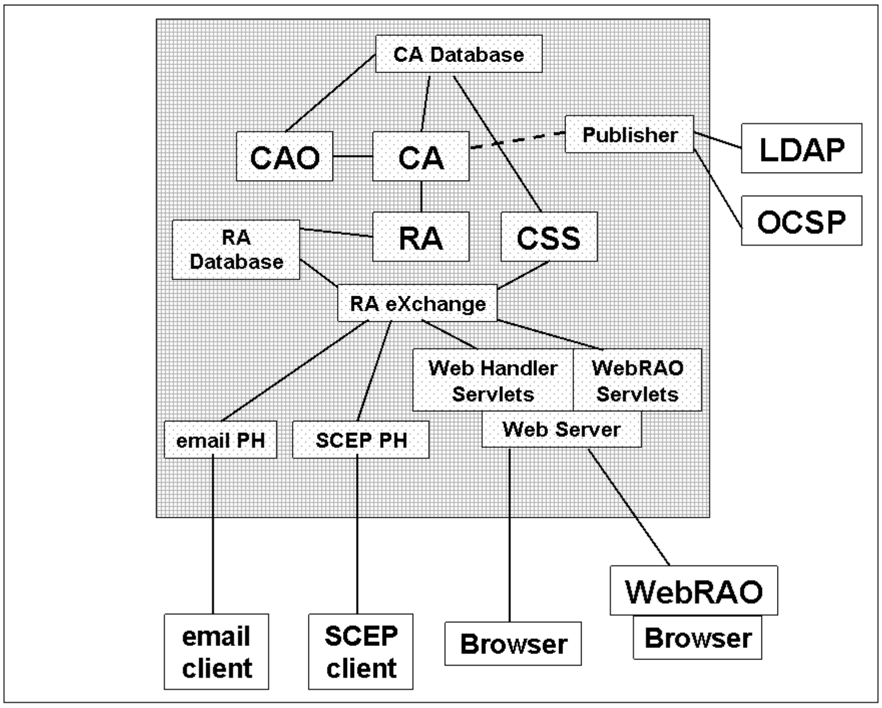

Figure 2-4 All components on one system with software cryptography

2.4.5.2 Figure 2-5 shows the system as in Figure 2-4 but with the databases on a separate system, and using HSMs and smart cards. As for the previous diagram, note that "Web Handler Servlets" form part of the Web Handler; "WebRAO Servlets" are part of the WebRAO.

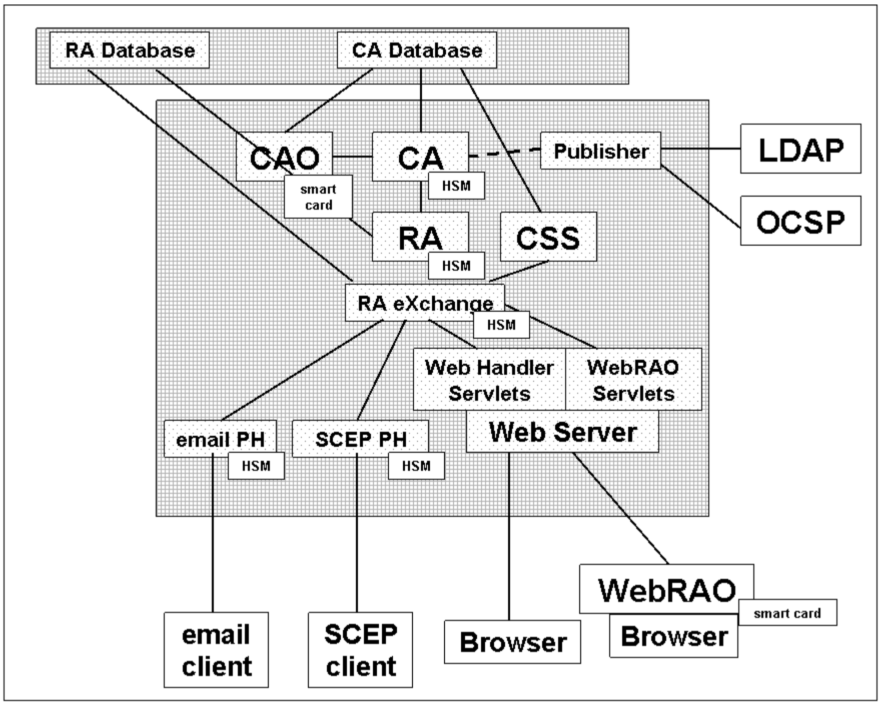

Figure 2-5 Single CA – RA with smart cards CA and RA on one system, and databases on separate system

2.4.6 Separate CA and RAs

As for Figure 2-5, note that in Figure 2-6 the "Web Handler Servlets" form part of the Web Handler; "WebRAO Servlets" are part of the WebRAO.

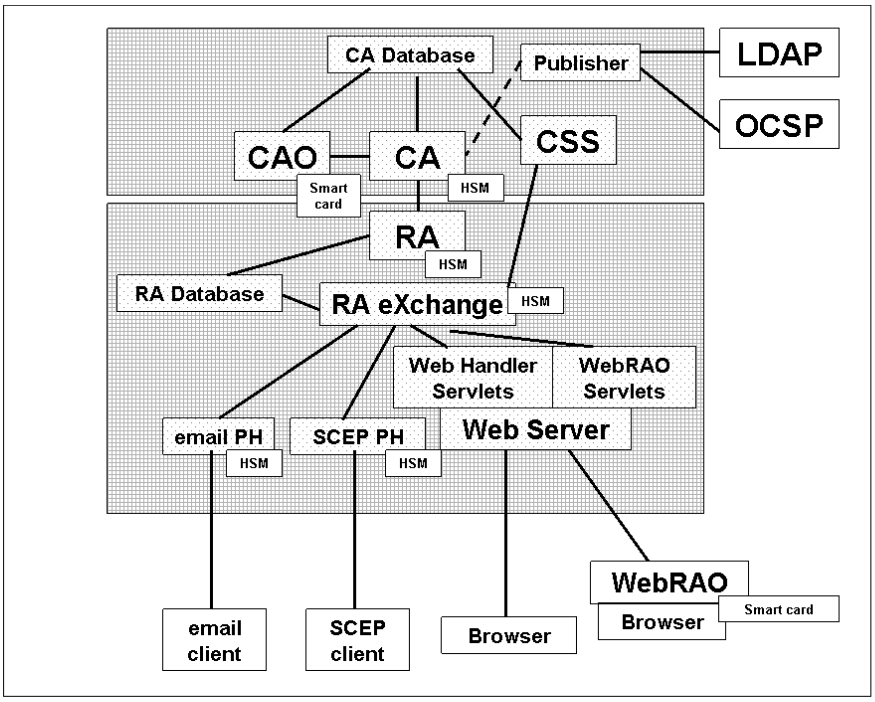

Figure 2-6 CA and RA on separate systems

2.5 UniCERT Evaluated Configuration

This section describes the items that may be used with the TOE in its evaluated configuration, and a number of configuration options that may not be used in the evaluated configuration.

2.5.1.1 Hardware

All UniCERT modules will run on the following minimum "customer" hardware platforms with the exception of the CAO and WebRAO client (applet) that are PC only:

Component	**Recommended Configuration**
Windows	1.8 GHz Pentium IV
	256 MB RAM without Oracle; or 512 MB RAM with Oracle
	4 GB for Oracle install 452 MB for Oracle data 390 MB for TOE Components

Component	**Recommended Configuration**
Unix[1]	Single Ultra Sparc 64 bit CPU
	1024 MB RAM with out Oracle; or 2048 MB RAM with Oracle
	4 GB for Oracle Install 452 MB for Oracle data 390 MB for TOE Components

Table 2-1 Platform Configurations

2.5.1.2 Operating Systems

The following operating systems will be supported by all UniCERT 5 modules except where explicitly stated.

Windows	**Server** Windows 2000 Server SP4; or Windows 2003 Enterprise Edition
	Client Windows 2000 Professional SP4; or Windows XP Professional SP2
Unix Except CAO, RA Event Viewer, and WebRAO which are Windows only components	Sun Solaris 8 (Patch Bundle 5/02 (May 2002))

Table 2-2 Supported Operating Systems

2.5.1.3 Web Servers

Table 2-3 indicates the web servers and servlet managers used in conjunction with UniCERT 5.

Web Server	**Servlet Manager**	**Operating System**	
		Windows	**Solaris 8**
Apache v1.3 or v2.0	Jakarta Tomcat	UniCERT 5 **WebRAO**	UniCERT 5 **WebRAO**

[1] Note, in a Unix configuration, the operator GUI's CAO and RA Event Viewer can only be run and installed on a Windows operating system.

	v4.1.27	**Web Handler**	**Web Handler**
IIS v5.0	ServletExec v4.2 patch 19	UniCERT 5 **WebRAO** **Web Handler**	N/A
Sun Java System Web Server v6.0 SP2	None Required	UniCERT 5 **WebRAO** **Web Handler**	UniCERT 5 **WebRAO** **Web Handler**

Table 2-3 Supported Web Servers and Servlet Managers

2.5.1.4 Browsers

Table 2-4 indicates the browsers used in conjunction with the WebRAO.

Browser	**Operating System**	
	Windows	**Sol8**
IE	v5.5 SP2 and v6.0	N/A
Netscape	v7.2	v7.2

Table 2-4 Supported Browsers at the WebRAO

Table 2-5 indicates the browsers used in conjunction with the Web Handler.

Browser	**Operating System**	
	Windows	**Sol8**
IE	v5.5 SP2 and v6.0	N/A
Netscape	v4.7 or v7.x	v4.7 or v7.x

Table 2-5 Supported Browsers at the Web Handler

2.5.1.5 Database - Oracle

UniCERT 5 will use Oracle 9i, as follows:

Configuration	**Supported Version**
Windows Server	Oracle v9.2.0.5 (9i) and security patch
	Oracle v8.1.7.4 and security patch

Configuration	Supported Version
Solaris Server	Oracle v9.2.0.6(9i)
Windows Client	Oracle v9.2.0.1 (9i)
Solaris Client	Oracle v9.2.0.6 (9i)

Table 2-6 Supported Oracle Versions

2.5.1.6 Crypto Modules

If a hardware security module is used within the evaluated configuration of UniCERT, this module must be certified under the Common Criteria to at least EAL4. This certification must cover the provision of the SFRs listed under OE.TamperNotify and OE.HardwareFunctions. At the time of writing only the Luna® CA^3, Version 3.97, Software Version 8.1, from SafeNet (formerly Chrysalis-ITS) has been certified in this way.

If the evaluated version of UniCERT is to be used with a smart card, then that smart card must be certified under the Common Criteria to at least EAL4. This certification must cover the provision of the SFRs listed under OE.HardwareFunctions. At the time of writing only the Oberthur Card Systems "COSMOPOLIC 2.1 V4 JavaCard Open Platform Embedded Software version 1" has been certified in this way.

2.5.1.7 Maintenance Agreement

In order to be in the evaluated configuration the owners of UniCERT 5 are required to participate in a maintenance agreement with Cybertrust. The maintenance agreement ensures that security flaws and vulnerabilities that have been discovered by users or by internal analysis are communicated to the user.

The maintenance agreement will also ensure that remedial or corrective actions will be communicated to the user in a timely manner.

2.5.1.8 Other Software

A number of Cybertrust products can be run with UniCERT 5 to provide extra functionality. Some of these may be run with the product when it is in its evaluated configuration, and some may not, as follows:

- Advanced Registration Module (ARM) – MAY NOT be used with the TOE in its evaluated configuration, unless a separate evaluation of the ARM software running with the TOE is performed
- UniCERT Programmatic Interface (UPI) – MAY NOT be used with the TOE in its evaluated configuration, unless a separate evaluation of the UPI software running with the TOE is performed
- The CMP handler MAY NOT be installed or used with the TOE in the evaluated configuration, unless a separate evaluation of the CMP handler software running with the TOE is performed

- Key Archive Server (KAS)– MAY be run with the TOE in its evaluated configuration. This product has a defined interface to the TOE and the security functions of the TOE that form this interface are part of the evaluation
- Publisher– MAY be run with the TOE in its evaluated configuration. This product only accepts output from an interface of the TOE – this interface is part of the evaluation.

2.5.1.9 Product Configuration

A number of configuration options of the product must be set as specified by the administrator for the product to be in its evaluated configuration, as follows:

- Automatic startup of the UniCERT services MAY NOT be used (unless a separate evaluation of the TOE with this option turned on is performed). All UniCERT services must be set to Manual startup in the UniCERT Service Manager so that the passphrases or PINs used to open the PKI keys are not stored anywhere on the machines running the TOE
- ECDSA key algorithm MAY NOT be used in registration policies – it does not form part of the evaluated product.
- Registration policies can provide an option to allow No Authorization. In the evaluated configuration, this MAY NOT be used.

2.6 CD Content Lists

The TOE is distributed on CDs. As of the time of the evaluation, there are CDs for the 5.2.1 release for Windows and Solaris, as well as 5.2.1.900 patch CDs for Windows and Solaris. Note that subdirectories that only contain other subdirectories (no files) are not listed in these subsections.

2.6.1 UniCERT 5.2.1 for Windows

Table 2-7 lists the files on the UniCERT Core v5.2.1 for Windows CD and their sizes. In the interest of space, the documentation files (those under D:\docs) are listed separately in Appendix A.

Filename	File size (bytes)
Root directory files (D:\)	
UniCERT.ico	766
autorun.inf	50
core_install.exe	18,359,193
Files in D:\MicroSoft\Redist	
MSVCP60.DLL	401,462
vcredist.exe	1,809,120
Files in D:\modules	
ca_install.exe	18,458,804
cao_install.exe	23,593,973
cmp_install.exe	17,996,098
common_install.exe	78,163,559
coredocs_install.exe	35,803,985
css_install.exe	18,348,200
email_install.exe	18,415,908
publisher_install.exe	21,635,824
ra_install.exe	18,480,554
rax_install.exe	18,074,152

Filename	File size (bytes)
scep_install.exe	18,420,427

Table 2-7 CD Contents for UniCERT Core v5.2.1 on Windows

Table 2-8 lists the files on the UniCERT Web Components v5.2.1 for Windows CD and their sizes.

Filename	File size (bytes)
Root directory files (D:\)	
UniCERT.ico	766
autorun.inf	50
webcomponents_install.exe	18,309,449
webreadme.html	7,371
Files in D:\modules	
webhandler_install.exe	69,927,834
webrao_install.exe	76,286,455

Table 2-8 CD Contents for UniCERT Web Components v5.2.1 on Windows

Table 2-9 lists the files on the UniCERT WebRAO Client v5.2.1 for Windows CD and their sizes. In the interest of space, the documentation files (those under D:\docs) are listed separately in Appendix A.

Filename	File size (bytes)
Root directory files (D:\)	
autorun.inf	52
installer.jar	90,131
Files in D:\Client	
IdentrusExtra.dll	81,920
IdentrusPkcs11.dll	208,896
JCryptoki.dll	245,760
KeyToolsProJava5220Signed.jar	993,178
US_export_policy.jar	4,355
local_policy.jar	4,368
ocs_lib.dll	376,832
Files in D:\jre	
CHANGES	1,126
COPYRIGHT	4,519
LICENSE	15,549
LICENSE.rtf	25,641
LICENSE_de.rtf	96,318
LICENSE_es.rtf	33,512
LICENSE_fr.rtf	50,533
LICENSE_it.rtf	62,114
LICENSE_ja.rtf	50,115
LICENSE_ko.rtf	305,403
LICENSE_sv.rtf	71,880
LICENSE_zh_CN.rtf	33,149
LICENSE_zh_TW.rtf	32,341
README.txt	10,313

Filename	File size (bytes)
THIRDPARTYLICENSEREADME.txt	10,367
Welcome.html	998
Files in D:\jre\bin	
JdbcOdbc.dll	49,278
NPJPI142_03.dll	65,650
NPJava11.dll	65,647
NPJava12.dll	65,647
NPJava13.dll	65,647
NPJava14.dll	65,647
NPJava32.dll	65,647
NPOJI610.dll	65,647
RegUtils.dll	110,707
awt.dll	970,862
axbridge.dll	94,323
cmm.dll	139,374
dcpr.dll	139,375
dt_shmem.dll	24,689
dt_socket.dll	20,595
eula.dll	61,547
fontmanager.dll	327,811
hpi.dll	28,791
hprof.dll	49,258
ioser12.dll	24,715
jaas_nt.dll	20,611
java.dll	102,515
java.exe	24,681
javaw.exe	28,779
jawt.dll	20,592
jcov.dll	61,544
jdwp.dll	102,505
jpeg.dll	122,992
jpicom32.dll	82,035
jpicpl32.cpl	61,555
jpicpl32.exe	16,501
jpiexp32.dll	94,323
jpins4.dll	28,783
jpins6.dll	41,071
jpins7.dll	45,167
jpinsp.dll	86,127
jpishare.dll	77,939
jsound.dll	139,384
jucheck.exe	241,777
jusched.exe	32,881
keytool.exe	28,801
kinit.exe	28,797
klist.exe	28,797
ktab.exe	28,795
msvcrt.dll	266,293
net.dll	57,455

Filename	File size (bytes)
nio.dll	32,880
orbd.exe	28,820
policytool.exe	28,807
rmi.dll	20,590
rmid.exe	28,795
rmiregistry.exe	28,807
servertool.exe	28,832
tnameserv.exe	28,822
verify.dll	57,453
w2k_lsa_auth.dll	20,563
zip.dll	53,364
Files in D:\jre\bin\client	
Xusage.txt	1,410
jvm.dll	1,212,546
Files in D:\jre\bin\server	
Xusage.txt	1,410
jvm.dll	2,740,354
Files in D:\jre\javaws	
JavaCup.ico	25,214
JavaWebStart.dll	139,264
Readme.html	12,382
Readme_de.html	15,799
Readme_es.html	15,028
Readme_fr.html	15,293
Readme_it.html	14,947
Readme_ja.html	14,976
Readme_ko.html	11,878
Readme_sv.html	13,013
Readme_zh_CN.html	9,718
Readme_zh_TW.html	11,881
cacerts	21,653
javalogo52x88.gif	2,841
javaws-l10n.jar	98,420
javaws-license.txt	10,540
javaws.exe	135,168
javaws.jar	1,198,733
javaws.policy	138
javawspl.dll	36,864
sunlogo64x30.gif	980
Files in D:\jre\javaws\resources	
copyright.jpg	19,014
messages.properties	1,734
messages_de.properties	2,135
messages_es.properties	2,189
messages_fr.properties	2,171
messages_it.properties	2,026
messages_ja.properties	3,747
messages_ko.properties	3,172
messages_sv.properties	2,172

Filename	File size (bytes)
messages_zh_CN.properties	2,215
messages_zh_TW.properties	2,283
miniSplash.jpg	5,076
splash.jpg	10,008
Files in D:\jre\lib	
charsets.jar	5,604,126
content-types.properties	5,778
flavormap.properties	3,904
font.properties	4,520
font.properties.CP1250	4,589
font.properties.CP1251	4,589
font.properties.CP1253	4,589
font.properties.CP1254	4,589
font.properties.CP1256	4,359
font.properties.CP1257	4,589
font.properties.MS950_HKSCS	7,610
font.properties.hi	5,711
font.properties.iw	3,079
font.properties.ja	6,218
font.properties.ko	5,645
font.properties.ru	4,607
font.properties.th	5,575
font.properties.zh	5,524
font.properties.zh.98	5,527
font.properties.zh_CN_GB18030	5,763
font.properties.zh_TW	6,020
font.properties.zh_TW.95	5,678
font.properties.zh_TW_MS950_HKSCS	7,616
jce.jar	69,596
jsse.jar	895,647
jvm.hprof.txt	2,748
jvm.jcov.txt	4,890
logging.properties	2,299
plugin.jar	2,003,473
psfont.properties.ja	3,177
psfontj2d.properties	10,981
rt.jar	26,429,417
sunrsasign.jar	89,343
tzmappings	6,867
Files in D:\jre\lib\audio	
soundbank.gm	493,589
Files in D:\jre\lib\cmm	
CIEXYZ.pf	51,236
GRAY.pf	632
LINEAR_RGB.pf	1,044
PYCC.pf	274,474
sRGB.pf	150,368
Files in D:\jre\lib\ext	
dnsns.jar	8,896

Filename	File size (bytes)
jh.jar	500,623
ldapsec.jar	53,248
localedata.jar	769,335
sunjce_provider.jar	111,374
Files in D:\jre\lib\fonts	
LucidaBrightDemiBold.ttf	75,144
LucidaBrightDemiItalic.ttf	75,124
LucidaBrightItalic.ttf	80,856
LucidaBrightRegular.ttf	344,908
LucidaSansDemiBold.ttf	317,896
LucidaSansRegular.ttf	698,236
LucidaTypewriterBold.ttf	234,068
LucidaTypewriterRegular.ttf	242,700
Files in D:\jre\lib\i386	
jvm.cfg	695
Files in D:\jre\lib\im	
indicim.jar	10,441
thaiim.jar	7,939
Files in D:\jre\lib\images\cursors	
cursors.properties	1,359
invalid32x32.gif	153
win32_CopyDrop32x32.gif	165
win32_CopyNoDrop32x32.gif	153
win32_LinkDrop32x32.gif	168
win32_LinkNoDrop32x32.gif	153
win32_MoveDrop32x32.gif	147
win32_MoveNoDrop32x32.gif	153
Files in D:\jre\lib\security	
US_export_policy.jar	2,440
cacerts	21,653
java.policy	2,271
java.security	7,059
local_policy.jar	2,921
Files in D:\jre\lib\zi	
CET	1,168
EET	1,072
GMT	27
MET	1,168
WET	1,068
ZoneInfoMappings	12,970
Files in D:\jre\lib\zi\Africa	
Abidjan	65
Accra	181
Addis_Ababa	65
Algiers	333
Asmera	65
Bamako	85
Bangui	65
Banjul	77

Filename	File size (bytes)
Bissau	77
Blantyre	65
Brazzaville	65
Bujumbura	27
Cairo	1,500
Casablanca	213
Ceuta	1,112
Conakry	85
Dakar	77
Dar_es_Salaam	85
Djibouti	65
Douala	65
El_Aaiun	77
Freetown	313
Gaborone	77
Harare	65
Johannesburg	105
Kampala	97
Khartoum	337
Kigali	65
Kinshasa	27
Lagos	65
Libreville	65
Lome	27
Luanda	65
Lubumbashi	27
Lusaka	65
Malabo	77
Maputo	65
Maseru	89
Mbabane	65
Mogadishu	73
Monrovia	77
Nairobi	97
Ndjamena	89
Niamey	89
Nouakchott	85
Ouagadougou	65
Porto-Novo	77
Sao_Tome	65
Timbuktu	65
Tripoli	293
Tunis	265
Windhoek	824
Files in D:\jre\lib\zi\America	
Adak	1,224
Anchorage	1,224
Anguilla	65
Antigua	77

Filename	File size (bytes)
Araguaina	1,036
Aruba	77
Asuncion	1,116
Barbados	137
Belem	297
Belize	513
Boa_Vista	329
Bogota	89
Boise	1,284
Buenos_Aires	517
Cambridge_Bay	1,096
Cancun	792
Caracas	77
Catamarca	517
Cayenne	77
Cayman	65
Chicago	1,960
Chihuahua	816
Cordoba	517
Costa_Rica	137
Cuiaba	1,116
Curacao	77
Danmarkshavn	341
Dawson	1,108
Dawson_Creek	509
Denver	1,336
Detroit	1,200
Dominica	65
Edmonton	1,316
Eirunepe	313
El_Salvador	105
Fortaleza	377
Glace_Bay	1,204
Godthab	1,036
Goose_Bay	1,792
Grand_Turk	1,044
Grenada	65
Guadeloupe	65
Guatemala	121
Guayaquil	65
Guyana	89
Halifax	1,924
Havana	1,372
Hermosillo	189
Indianapolis	329
Inuvik	1,096
Iqaluit	1,092
Jamaica	233
Jujuy	517

Filename	File size (bytes)
Juneau	1,224
La_Paz	81
Lima	169
Los_Angeles	1,560
Louisville	1,500
Maceio	393
Managua	153
Manaus	313
Martinique	89
Mazatlan	840
Mendoza	517
Menominee	1,216
Merida	788
Mexico_City	880
Miquelon	1,032
Monterrey	788
Montevideo	581
Montreal	1,928
Montserrat	65
Nassau	1,284
New_York	1,960
Nipigon	1,144
Nome	1,228
Noronha	329
Panama	65
Pangnirtung	1,096
Paramaribo	101
Phoenix	141
Port-au-Prince	313
Port_of_Spain	65
Porto_Velho	297
Puerto_Rico	77
Rainy_River	1,144
Rankin_Inlet	1,088
Recife	377
Regina	497
Rio_Branco	297
Santiago	1,360
Santo_Domingo	201
Sao_Paulo	1,116
Scoresbysund	1,040
St_Johns	2,048
St_Kitts	65
St_Lucia	65
St_Thomas	65
St_Vincent	65
Swift_Current	241
Tegucigalpa	105
Thule	852

Filename	File size (bytes)
Thunder_Bay	1,192
Tijuana	1,276
Tortola	65
Vancouver	1,592
Whitehorse	1,108
Winnipeg	1,568
Yakutat	1,220
Yellowknife	1,088
Files in D:\jre\lib\zi\America\Indiana	
Knox	765
Marengo	361
Vevay	185
Files in D:\jre\lib\zi\America\Kentucky	
Monticello	1,260
Files in D:\jre\lib\zi\America\North_Dakota	
Center	1,276
Files in D:\jre\lib\zi\Antarctica	
Casey	65
Davis	81
DumontDUrville	81
Mawson	65
McMurdo	1,124
Palmer	1,144
Rothera	65
Syowa	65
Vostok	65
Files in D:\jre\lib\zi\Asia	
Aden	65
Almaty	1,016
Amman	1,052
Anadyr	1,044
Aqtau	1,016
Aqtobe	1,016
Ashgabat	269
Baghdad	1,004
Bahrain	77
Baku	984
Bangkok	65
Beirut	1,208
Bishkek	1,024
Brunei	77
Calcutta	97
Choibalsan	361
Chongqing	181
Colombo	121
Damascus	1,300
Dhaka	97
Dili	93
Dubai	65

Filename	File size (bytes)
Dushanbe	261
Gaza	1,236
Harbin	205
Hong_Kong	617
Hovd	357
Irkutsk	1,040
Jakarta	129
Jayapura	85
Jerusalem	1,236
Kabul	65
Kamchatka	1,040
Karachi	121
Kashgar	193
Katmandu	77
Krasnoyarsk	1,040
Kuala_Lumpur	121
Kuching	217
Kuwait	65
Macau	393
Magadan	1,040
Makassar	85
Manila	125
Muscat	65
Nicosia	1,116
Novosibirsk	1,048
Omsk	1,040
Oral	1,016
Phnom_Penh	97
Pontianak	125
Pyongyang	101
Qatar	77
Qyzylorda	1,028
Rangoon	85
Riyadh	65
Riyadh87	4,661
Riyadh88	4,581
Riyadh89	4,581
Saigon	97
Sakhalin	1,044
Samarkand	281
Seoul	165
Shanghai	201
Singapore	121
Taipei	381
Tashkent	277
Tbilisi	1,008
Tehran	924
Thimphu	77
Tokyo	27

Filename	File size (bytes)
Ulaanbaatar	357
Urumqi	181
Vientiane	97
Vladivostok	1,040
Yakutsk	1,040
Yekaterinburg	1,040
Yerevan	1,016
Files in D:\jre\lib\zi\Atlantic	
Azores	1,868
Bermuda	1,124
Canary	1,044
Cape_Verde	97
Faeroe	1,016
Madeira	1,864
Reykjavik	577
South_Georgia	27
St_Helena	65
Stanley	1,080
Files in D:\jre\lib\zi\Australia	
Adelaide	1,224
Brisbane	189
Broken_Hill	1,224
Darwin	125
Hobart	1,288
Lindeman	221
Lord_Howe	1,012
Melbourne	1,224
Perth	157
Sydney	1,224
Files in D:\jre\lib\zi\Etc	
GMT	27
GMT+1	27
GMT+10	27
GMT+11	27
GMT+12	27
GMT+2	27
GMT+3	27
GMT+4	27
GMT+5	27
GMT+6	27
GMT+7	27
GMT+8	27
GMT+9	27
GMT-1	27
GMT-10	27
GMT-11	27
GMT-12	27
GMT-13	27
GMT-14	27

Filename	File size (bytes)
GMT-2	27
GMT-3	27
GMT-4	27
GMT-5	27
GMT-6	27
GMT-7	27
GMT-8	27
GMT-9	27
UCT	27
UTC	27
Files in D:\jre\lib\zi\Europe	
Amsterdam	1,544
Andorra	968
Athens	1,196
Belfast	2,032
Belgrade	1,040
Berlin	1,236
Brussels	1,564
Bucharest	1,180
Budapest	1,312
Chisinau	1,212
Copenhagen	1,152
Dublin	1,916
Gibraltar	1,676
Helsinki	1,036
Istanbul	1,464
Kaliningrad	1,140
Kiev	1,048
Lisbon	1,868
London	2,024
Luxembourg	1,568
Madrid	1,416
Malta	1,440
Minsk	1,064
Monaco	1,576
Moscow	1,152
Oslo	1,216
Paris	1,568
Prague	1,216
Riga	1,108
Rome	1,440
Samara	1,040
Simferopol	1,064
Sofia	1,088
Stockholm	1,040
Tallinn	1,080
Tirane	1,164
Uzhgorod	1,052
Vaduz	1,008

Filename	File size (bytes)
Vienna	1,200
Vilnius	1,060
Warsaw	1,400
Zaporozhye	1,072
Zurich	1,056
Files in D:\jre\lib\zi\Indian	
Antananarivo	89
Chagos	65
Christmas	27
Cocos	27
Comoro	65
Kerguelen	65
Mahe	65
Maldives	65
Mauritius	65
Mayotte	65
Reunion	65
Files in D:\jre\lib\zi\Pacific	
Apia	77
Auckland	1,336
Chatham	856
Easter	1,264
Efate	233
Enderbury	89
Fakaofo	65
Fiji	105
Funafuti	65
Galapagos	77
Gambier	65
Guadalcanal	65
Guam	65
Honolulu	117
Johnston	27
Kiritimati	89
Kosrae	85
Kwajalein	89
Majuro	77
Marquesas	65
Midway	65
Nauru	97
Niue	89
Norfolk	77
Noumea	121
Pago_Pago	77
Palau	65
Pitcairn	77
Ponape	65
Port_Moresby	27
Rarotonga	285

Filename	File size (bytes)
Saipan	77
Tahiti	65
Tarawa	65
Tongatapu	133
Truk	65
Wake	65
Wallis	65
Yap	77
Files in D:\vm	
j2re-1_4_2_06-windows-i586-p.exe	15,691,488

Table 2-9 CD Contents for UniCERT WebRAO Client v5.2.1 on Windows

2.6.2 UniCERT 5.2.1.900 for Windows

Table 2-10 lists the files on this CD and their sizes.

Filename	File size (bytes)
RAGateway521.dll	880,640
RAService.exe	610,304
UniCERT_v5.2.1_Windows_patch_900readme.html	13,723
unicert_5_additional_cc_guidance.pdf	462,798

Table 2-10 CD Contents for UniCERT v5.2.1.900 on Windows

2.6.3 UniCERT Core 5.2.1 for Solaris

Table 2-11 lists the files on the UniCERT Core v5.2.1 CD for Solaris and their sizes. As there is only a Windows version of the CAO, its Windows installer and associated files are also included on this CD.

In the interest of space, the documentation files (those under /docs) are listed separately in Appendix A.

Filename	File size (bytes)
Root directory files (/)	
UniCERT.ico	766
autorun.inf	52
core_install.bin	33,225,676
Files in /cao	
cao_master.exe	18,383,669
Files in /MicroSoft/Redist	
MSVCP60.DLL	401,462
vcredist.exe	1,809,120
Files in /cao/modules	
cao_install.exe	23,593,973
common_install.exe	78,163,559
coredocs_install.exe	35,803,985
Files in /modules	
ca_install.bin	34,274,056
cmp_install.bin	35,126,638
common_install.bin	118,810,163
css_install.bin	33,279,195
email_install.bin	34,297,705
publisher_install.bin	41,618,400

Filename	File size (bytes)
ra_install.bin	34,140,552
rax_install.bin	38,079,509
scep_install.bin	34,352,477
serversdocs_install.bin	49,555,426

Table 2-11 CD Contents for UniCERT Core v5.2.1 on Solaris

Table 2-12 lists the files on the UniCERT Web Components v5.2.1 for Solaris CD and their sizes.

Filename	File size (bytes)
Root directory files (/)	
<translation table>	1
webcomponents_install.bin	34,194
webreadme.html	11
Files in /modules	
<translation table>	1
webhandler_install.bin	91,776
webrao_install.bin	97,648

Table 2-12 CD Contents for UniCERT Web Components v5.2.1 on Solaris

As there is only a Windows version of the WebRAO Client (which also gets distributed with UniCERT v5.2.1 for Solaris), see Table 2-9 for a listing of its files.

2.6.4 UniCERT 5.2.1.900 for Solaris

Table 2-13 lists the files on this CD and their sizes.

Filename	File size (bytes)
unicert521_900.tar, which includes:	7,742,976
o libRAGateway_521u.so	5,609,200
o RAService	1,667,920
o unicert_5_additional_cc_guidance.pdf	462,798
unicert521solaris900readme.html	15,242

Table 2-13 CD Contents for UniCERT v5.2.1.900 on Solaris

3. TOE Security Environment

3.1 Introduction

3.1.1 This section contains a statement of the TOE Security Environment. It describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be employed.

3.2 Secure Usage Assumptions

3.2.1 User

3.2.1.1 A.DisposalofAuthenticationData: Proper disposal of authentication data

Authentication data and associated privileges should be properly disposed of and/or removed as appropriate when no longer required. This includes the removal from the PKI, the revocation of certificates and the secure deletion of authentication data for both human and non-human users (i.e., the CAO user or the CA) when appropriate. For example, if a CAO administrator leaves the organization that runs a PKI, then their certificate should be revoked, their private key securely destroyed, and the CAO entity that they managed should be removed from the PKI. Similarly, if it is suspected that a private key has been compromised, then the associated certificate should be promptly suspended or revoked.

3.2.1.2 A.AuditReview: It is assumed that authorized auditor(s) will regularly review audit records.

The auditor roles are responsible for regularly reviewing audit records for signs of attempted attacks. They should perform regular audits of the audit records (including checking the integrity of the audit logs) and respond to any such attempted attacks as appropriate. They should also ensure that the audit data is regularly archived to prevent audit data storage exhaustion.

3.2.1.3 A.CPS: It is assumed that the PKI users are familiar with and uphold the CP and CPS that the PKI operates.

All PKI users, especially the TOE administrators and users, will be familiar with and trusted to uphold the requirements of their PKI's Certification Policy and Certification Practices Statement.

3.2.1.4 A.CompetentPKIUsers: Assume competent PKI users

All PKI users, especially the administrators and users are competent, either by training or experience, to manage, operate and use the TOE and the security and privacy of the data it contains. In order to be competent all such persons will read, understand and follow the guidance documentation that is relevant to them, and will have a good understanding of the principles of computer security and Public Key Infrastructures.

3.2.1.5 A.MaliciousCodeNotExecuted: Assume the TOE trusted users do not execute malicious code.

It is assumed that the TOE administrators and users do not install and execute malicious code on the same platform as the TOE.

3.2.1.6 A.SecureInstallation: Ensure that the system is set up and operated securely.

The Systems administrators are responsible for securely installing, operating and maintaining the TOE and other IT components used when operating the TOE. These persons are trusted to do so in a secure fashion. The TOE, and the IT components that are associated with it (i.e., hardware, operating systems, web server, RA and CA databases, browsers) should be physically and logically protected from access by untrusted persons.

3.2.1.7 A.Guidance: Assume the PKI administrators and users read and follow the guidance material.

The Guidance contains all necessary information to securely install, configure, operate and maintain the TOE. It is assumed that administrators and users read the guidance material so they can appropriately perform their duties. This material provides information on what the TOE is able to do securely. An example of this is the value of the assets that the TOE is able to protect: as the TOE is evaluated to an EAL 4+ level, it is only able to provide protection to information assets of less than a moderate value.

3.2.2 Physical/Logical

3.2.2.1 A.CommunicationsProtection: Protect communications both logically and physically

The system owners are responsible for providing adequate logical and physical protection on the communications channels used by the TOE.

This includes the use of firewalls to prevent logical intrusions, and the physical protection of the communications system, to guard against unauthorized access or malicious modification and destruction by users.

The protection is to extend to the boundary of the protected network of the TOE components.

3.2.2.2 A.PhysicalProtection: Protect physical boundary

The system owners are responsible for providing adequate physical protection for the TOE and the other items it runs with in the evaluated configuration.

This includes user access controls to restrict access to only authorized, trusted persons, and monitoring entries, to guard against unauthorized access or malicious modification and destruction by users.

3.2.3 System

3.2.3.1 A.Timesource: There is a trusted, accurate and reliable time source.

It is assumed that TOE owners will ensure that a time source for timestamping audit records is available, and that its reliability and accuracy is acceptable to the TOE owner.

3.3 Threats to Security

3.3.1 This section describes all threats to the assets against which specific protection within the TOE or its environment is required. Each threat is described in terms of an identified threat agent, the attack, and the asset that is the subject of the attack. Threat agents are described by addressing their required expertise, available resources, and motivation. Attacks are described by addressing the attack methods, any vulnerability that would need to be exploited to perform the attack, and opportunity.

Threat	Threat Agent	Attack	Asset
T.AdminErrCommit: Administrative errors of commission A TOE administrator or system administrator commits errors that directly compromise organizational security objectives or change the technical security policy enforced by the system or application.	**Expertise** N/A - unintentional **Resources** N/A - unintentional **Motivation** N/A - unintentional	**Attack Methods** Unintentional Error **Vulnerabilities Exploited** Any poor design of the TOE, which might increase the possibility of such an error. The developer has measures in place to ensure that this does not occur. **Opportunity** Substantial, as the "attacker" is an administrator.	Certificates produced by the TOE, linking an identity to a private key.
T.AdminErrOmit: Administrative errors of omission The TOE administrator or system administrator unintentionally fails to perform some function essential to security.	**Expertise** N/A - unintentional **Resources** N/A - unintentional **Motivation** N/A - unintentional	**Attack Methods** Unintentional Error **Vulnerabilities Exploited** Any poor design of the TOE, which might increase the possibility of such an error. The developer has measures in place to ensure that this does not occur. **Opportunity** Substantial, as the "attacker" is an administrator.	Certificates produced by the TOE, linking an identity to a private key.

Threat	**Threat Agent**	**Attack**	**Asset**
T.PKIKeyCompromise: A TOE administrator or user's key is compromised. A TOE administrator or user's key is compromised, by theft, accidental exposure, modification, or by an attacker masquerading as an authorized user. This could lead to the production of certificates that cannot be trusted, as well as compromise of a key, or the masquerading as an administrator/user by the attacker.	**Expertise** To successfully perform cryptanalysis to discover a private key would require high levels of expertise. The other attacks would require less expertise. **Resources** A moderate or high level of resources would be required to successfully execute this attack. However, the resources applied to this task would always be less than moderate due to the fact that administrators are instructed to only use the TOE to protect assets of less than this value. **Motivation** A moderate or high level of motivation would be required to successfully execute this attack. However, the motivation level for attackers would always be less than moderate due to the fact that administrators are instructed to only use the TOE to protect assets of less than this value.	**Attack Methods** Cryptanalysis to discover a private key using the public key or a signature done using the private key; stealing or copying of private key in storage and obtaining PIN or passphrase either by "social engineering", accident or cryptanalysis. **Vulnerabilities Exploited** Any weaknesses in the cryptographic algorithms used to generate the key pair or to protect the private key. The developer has measures in place to ensure that these do not occur. **Opportunity** In the case of PKI Entities, the opportunity to steal a key would be reduced due to the greater security awareness of the administrator, and the physical protection of the TOE environment. In the case of the end user, this would be increased.	Compromise of administrator or user's key. Compromise of this could lead to allowing an attacker to produce of compromised certificates, or to masquerade as someone else.

Threat	Threat Agent	Attack	Asset
T.ExportKeyMaterial The TOE may export secret or private keys in a form that an attacker can interpret and use the keys for launching other attacks on the TOE/PKI. An administrator or user's keys may be compromised by the TOE exporting the key in a form that an attacker can interpret and use. This could lead to the production of certificates that cannot be trusted, as well as compromise of end user or other entity or user keys, or the masquerading as an administrator or user by the attacker.	**Expertise** Low – if this fault existed, the attacker would just need to find the material that they could use. **Resources** Low – this would occur due to either faults in the TOE, or bad design of the TOE. If this fault existed, the attacker would just need to find it. **Motivation** Low – this would occur due to either faults in the TOE, or bad design of the TOE. If this fault existed, the attacker would just need to find it.	**Attack Methods** To examine the output of the TOE to attempt to discover the private keys of either an administrator or user in a format that the attacker can use. **Vulnerabilities Exploited** A faulty or badly designed TOE, which exports secret material in clear text. Inadequate design or testing could lead to this situation. The developer has measures in place to ensure that this does not occur. **Opportunity** This would depend on where the private key material was exported. If it was in publicly distributed information, such as certificates, then substantial opportunity would be presented to execute this attack.	Private keys protected by the TOE security mechanisms.

Threat	Threat Agent	Attack	Asset
T.Cryptography: Inappropriate cryptographic operations or parameters are used by the TOE. Inappropriate cryptographic operations or parameters are accidentally used, chosen or specified by the TOE administrators or users that may be exploited by cryptographic analysis techniques that lead to key certificate or PKI message compromises.	**Expertise** Low: this threat arises due to administrators or users using TOE resources wrongly, accidentally. **Resources** Low: this threat arises due to administrators or users using TOE resources wrongly, accidentally. **Motivation** Low: this threat arises due to administrators or users using TOE resources wrongly, accidentally.	**Attack Methods** Administrators or users using TOE resources wrongly, accidentally. **Vulnerabilities Exploited** If the guidance documentation did not give adequate guidance on secure use of the TOE then this threat may arise. The developer has measures in place to ensure that this does not occur. **Opportunity** High, due to the fact that TOE administrators and users have access to the TOE.	The privacy or integrity of private keys, certificate integrity, or the integrity or privacy of messages between PKI components.

Threat	Threat Agent	Attack	Asset
T.NonRepudiation: An administrator or user denies having sent a message or initiating a TSF that would violate the TSP.	**Expertise** In order to successfully perform this attack, a high level of expertise would be required due to the cryptographic protection on messages and log event records afforded by the TOE. **Resources** A moderate or high level of resources would be required to successfully execute this attack. However, the resources applied to this task would always be less than moderate due to the fact that administrators are instructed to only use the TOE to protect assets of less than this value. **Motivation** A moderate or high level of motivation would be required to successfully execute this attack. However, the motivation level for attackers would always be less than moderate due to the fact that administrators are instructed to only use the TOE to protect assets of less than this value.	**Attack Methods** Cryptanalysis in order to modify the log and/or messages without detection. **Vulnerabilities Exploited** Any weaknesses in the cryptographic algorithms employed. The developer has measures in place to ensure that these do not occur. **Opportunity** The administrator or user has substantial access to the TOE, as they are able to use the TOE as they wish. They could, therefore have substantial opportunity to access the messages sent between their TOE component and the others. However, apart from auditors, the administrators and users do not have access to the logs and so has little opportunity to attack them.	Certificates and certificate status records produced by the TOE.

Threat	Threat Agent	Attack	Asset
T.DevFlawedCode: Software containing security-related flaws A system or applications developer delivers code that does not perform according to specifications or contains security flaws, thereby unintentionally allowing an attacker to access the assets that the TOE protects.	**Expertise** Potentially Low – if the TOE contained security faults, an attacker would just need to find the flaw – this could be easy. **Resources** Potentially Low – as for expertise. **Motivation** Potentially Low – as for expertise.	**Attack Methods** To examine the output of the TOE to discover any security flaws. **Vulnerabilities Exploited** Inadequate design or testing, or inadequate control over the development environment could lead to this situation. However, the developer has measures in place to ensure that this does not occur. **Opportunity** The opportunity to exploit such a flaw would depend on the type of flaw it is.	Certificates and certificate status information produced by the TOE.

Threat	Threat Agent	Attack	Asset
T.FlawDiscovery: A flaw is discovered that could potentially affect the TSF During the product lifecycle a flaw may be discovered that could potentially affect the TSF. This may occur during development or post release. A user may not be aware of this flaw and potentially be vulnerable to an attack.	**Expertise** Potentially Low – if the TOE contained security flaws, an attacker would just need to find it – this could be easy. **Resources** Potentially Low – as for expertise. **Motivation** Potentially Low – as for expertise.	**Attack Methods** To examine the output of the TOE to discover any security flaws. **Vulnerabilities Exploited** Inadequate design or testing, or inadequate control over the development environment could lead to this situation. However, the developer has measures in place to ensure that this does not occur. **Opportunity** The opportunity to exploit such a flaw would depend on the type of flaw it is.	Certificates and certificate status information produced by the TOE.

Threat	Threat Agent	Attack	Asset
T.LossOfAuditData: An attacker gains access to the audit data and then deletes or modifies it to mask an attack on the TOE.	**Expertise** In order to successfully perform this attack, a high level of expertise would be required due to the cryptographic protection on log event records afforded by the TOE. **Resources** A moderate or high level of resources would be required to successfully execute this attack. However, the resources applied to this task would always be less than moderate due to the fact that administrators are instructed to only use the TOE to protect assets of less than this value. **Motivation** A moderate or high level of motivation would be required to successfully execute this attack. However, the motivation level for attackers would always be less than moderate due to the fact that administrators are instructed to only use the TOE to protect assets of less than this value.	**Attack Methods** Cryptanalysis in order to modify the log without detection. **Vulnerabilities Exploited** Any weaknesses in the cryptographic algorithms employed. The developer has measures in place to ensure that these do not occur. **Opportunity** Due to the physical and logical protection afforded to the TOE by A.PhysicalProtection, A.CommunicationsProtection, , an attacker is likely to have little opportunity to access the TOE directly. The TOE, in turn affords protection to the audit log. Therefore there would be little opportunity to perform this attack.	Certificates and certificate status records produced by the TOE.

Threat	Threat Agent	Attack	Asset
T.MaliciousCode: An attacker causes an administrator or user to execute malicious code with the TOE. An attacker either gains access to the TOE and installs malicious code or causes an administrator or user to do so such that the TSP is violated.	**Expertise** An attacker would need considerable expertise to access the machine running the TOE as it is protected both physically and logically. They could alternatively trick an administrator or user to do so, but this would still require some expertise. Furthermore, most types of malicious code would be unlikely to work on the user's or administrator's machine because of the cryptographic controls in place – to develop code that would do so would require a moderate to high level of expertise. **Resources** A moderate or high level of resources would be required to successfully execute this attack by either means. However, the resources applied to this task would always be less than moderate due to the fact that administrators are instructed to only use the TOE to protect assets of less than this value. **Motivation** A moderate or high level of motivation would be required to successfully execute this attack due to the level of resources required. However, the motivation level for attackers would always be less than moderate due to the fact that administrators are instructed to only use the TOE to protect assets of less than this value.	**Attack Methods** These are listed under "expertise". **Vulnerabilities Exploited** Any vulnerabilities in the TOE's access controls or its cryptographic mechanisms that protect certificates could potentially permit this attack. Also vulnerabilities in the assumed physical and logical protection of machines running the TOE. **Opportunity** There may be substantial opportunity to access the TOE's administrators and users to attempt this attack, depending on the environment the TOE is installed in, though this is unlikely due to the assumed trusted nature and competence of the administrators and users. There would be little opportunity to access the machines running the TOE directly either physically or logically due to the assumed physical and logical protection of machines running the TOE.	Certificates and certificate status records produced by the TOE. These would be attacked indirectly by attempting to cause the TOE to violate the TSP, whilst still being able to execute.

Threat	**Threat Agent**	**Attack**	**Asset**
T.UnAuthorizedConfigurationChange: An attacker modifies the PKI configuration. An attacker modifies the configuration of the PKI to allow for the production of untrustworthy certificates, replacing authentic components with masquerades.	**Expertise** An attacker would need considerable expertise to gain access to the TOE and perform this action, as they would need to falsely obtain a certificate that allows them to do so. **Resources** A moderate or high level of resources would be required to successfully execute this attack. However, the resources applied to this task would always be less than moderate due to the fact that administrators are instructed to only use the TOE to protect assets of less than this value. **Motivation** A moderate or high level of motivation would be required to successfully execute this attack. However, the motivation level for attackers would always be less than moderate due to the fact that administrators are instructed to only use the TOE to protect assets of less than this value.	**Attack Methods** The attacker would need to create or steal a certificate that provided them with access to the TOE, or otherwise bypass the TOE's access controls. They would then need to physically or logically access the TOE and perform this change, whilst overcoming the cryptographic controls on PKI components. **Vulnerabilities Exploited** Any vulnerabilities in the TOE's access controls or its cryptographic mechanisms that protect certificates and the PKI could potentially permit this attack. The developer has procedures and mechanisms in place to ensure that these do not arise. **Opportunity** There may be substantial opportunity to access the TOE and attempt this attack, depending on the environment it is installed in, though this is unlikely.	Certificates and certificate status records produced by the TOE. These would be attacked indirectly by attempting to modify the configuration of the PKI so as to allow for the production of untrustworthy certificates.

Threat	Threat Agent	Attack	Asset
T.MessageModification: An Intercepted message is modified and sent on. An attacker modifies intercepted messages between TOE entities, to gain access, or higher privilege or to initiate an unauthorized TSF.	**Expertise** An attacker would need considerable expertise to successfully intercept and modify messages between the TOE entities, as they would need overcome the cryptographic protection on these messages. **Resources** A moderate or high level of resources would be required to successfully execute this attack. However, the resources applied to this task would always be less than moderate due to the fact that administrators are instructed to only use the TOE to protect assets of less than this value. **Motivation** A moderate or high level of motivation would be required to successfully execute this attack. However, the motivation level for attackers would always be less than moderate due to the fact that administrators are instructed to only use the TOE to protect assets of less than this value.	**Attack Methods** The attacker would need to obtain access to the communication channels and intercept the messages, whilst overcoming the cryptographic controls on PKI components. **Vulnerabilities Exploited** Any vulnerabilities in the TOE's cryptographic protection of messages could potentially permit this attack. The developer has mechanisms in place to ensure that these do not arise. **Opportunity** There would be little opportunity to perform this attack due to A.CommunicationsProtection.	Certificates and certificate status records produced by the TOE. These would be attacked by attempting to modify the messages between the TOE components without detection.

Threat	Threat Agent	Attack	Asset
T.UnTrustedEntity: An untrusted entity is used to register or create certificates An untrusted entity masquerading as the TOE is used to register or create certificates bypassing the process and procedures of the PKI, and leading to untrustworthy certificates.	**Expertise** An attacker would need considerable expertise to successfully masquerade as the TOE, as they would need create or obtain the CA's private key to do so. **Resources** A moderate or high level of resources would be required to successfully execute this attack. However, the resources applied to this task would always be less than moderate due to the fact that administrators are instructed to only use the TOE to protect assets of less than this value. **Motivation** A moderate or high level of motivation would be required to successfully execute this attack. However, the motivation level for attackers would always be less than moderate due to the fact that administrators are instructed to only use the TOE to protect assets of less than this value.	**Attack Methods** The attacker would need to steal or create the CA's private key so as to masquerade as the TOE. This might be done by cryptanalysis of the public key or of something signed by the CA, or it might be done by stealing a copy of the CA's private key. **Vulnerabilities Exploited** Vulnerabilities in the cryptographic algorithm used to create the CA's key, or possibly a "social engineering" attack used to obtain the private key. The TOE has mechanisms in place to address these attacks. **Opportunity** There would be little opportunity to perform this attack due to the mechanisms in place to protect the CA's private key.	Certificates and certificate status records produced by the TOE. These would be attacked by attempting to masquerade as the TOE without detection.

Table 3-1 Threats and Attacks

3.4 Organizational Security Policies

3.4.1 This section identifies the organizational security policy statements or rules with which the TOE must comply.

3.4.2 User

3.4.2.1 P.Accountability: Individual accountability

Individuals shall be held accountable for their actions.

3.4.2.2 P.DisposalOfAuthenticationData: Disposal of authentication data and privileges

The TOE owner will ensure that there are appropriate procedures to ensure authentication data is destroyed and privileges removed after access has been removed or redefined. This applies to administrators and users.

3.4.2.3 P.Guidance: Installation and usage guidance

Guidance shall be provided for the secure installation and use of the system. The guidance shall be unambiguous and contain sufficient information for a secure set up and operation of the TOE.

3.4.2.4 P.QualifiedTOEUsers: The TOE users should be sufficiently qualified to perform their duties.

The TOE owner is responsible for ensuring the TOE users (as defined in section 9.2.2) are appropriately qualified by means of training, knowledge, and or experience.

3.4.2.5 P.RoleSeparation: The TOE owners must ensure that there is independence in roles**.**

a) The System administrators cannot assume any other role;
b) The WebRAO users cannot assume any other role (although they may install their software); and
c) The Audit Log Managers cannot assume any other role.

3.4.3 Cryptography

3.4.3.1 P.Cryptography: Appropriate use of cryptographic functions

The TOE owners are responsible for insuring the TOE uses secure algorithms and parameters for all cryptographic functions. This extends to ensuring the TOE administrators and users use only secure algorithms and parameters. The CAO user enforces this objective through the certificate practice statement and by defining the certificate registration (policy) requirements.

3.4.3.2 P.HardwareCryptography: Appropriate selection of cryptographic devices

The TOE owners are responsible for insuring if the TOE uses external cryptographic devices, then secure algorithms and parameters for all cryptographic functions, and that there is sufficient protection of the keys. This extends to ensuring the TOE administrators and users use only secure algorithms and parameters and devices.

3.4.4 System

3.4.4.1 P.ApplyFlawRemediation: Maintaining Security of TOE Functions

The TOE owners are responsible for insuring the TOE security functionality is maintained by applying developer supplied flaw remediation.

4. Security Objectives

4.1 Introduction

4.1.1 This section defines the security objectives to be satisfied by the TOE and the security objectives to be satisfied by IT and non-IT measures within the TOE environment. It addresses all of the identified aspects of the security environment.

4.2 Security Objectives for the TOE

4.2.1 The following security objectives for the TOE trace back to aspects of identified threats to be countered by the TOE and/or organizational security policies to be met by the TOE.

4.2.2 User

4.2.2.1 O.AuditLogs: Review of Audit Logs.

The auditors are responsible for identifying and monitoring security relevant events – they are required to review audit logs sufficiently regularly.

This requires both administrator guidance and a policy to ensure that the auditors fulfill their duties.

4.2.2.2 O.DisposalOfAuthenticationData: Proper disposal of authentication data

Proper disposal of authentication data and associated privileges is performed after access has been removed. This would be enforced by the key destruction function of the TOE and HSMs coupled with removal of PKI entities from the PKI.

4.2.2.3 O.IndividualAccountability: Ensure adequate information in the audit data

Provide individual accountability for audited events. This means role separation should be enforced, based upon user attributes and system roles.

4.2.2.4 O.Installation: Install, operate, and maintain.

The TOE owners are responsible for the TOE being installed, operated and maintained in a secure manner.

4.2.2.5 O.CPS: All users familiar with CP and CPS under which TOE operates

To ensure that administrators and users are familiar with the CP and CPS under which the TOE is operated.

4.2.3 Cryptography

4.2.3.1 O.CryptographicFunctions: To ensure appropriate cryptographic functions and parameters are used.

The TOE must implement secure cryptographic functions and parameters for:
a) Authentication; Signing and Verification
b) Encryption/Decryption: Symmetric Key Generation, Encryption and Decryption.
c) Key Management; Key Generation, Key Storage, and Key Destruction.

4.2.3.2 O.NonRepudiation: All users are to be accountable.

To prevent users from avoiding responsibility for their actions, all TOE users are to provide evidence of origin for messages and TSF initiation.

4.2.4 System

4.2.5 O.Audit:

The TOE will provide the means of recording security related events so as to assist auditors in the detection of potential attacks or misconfiguration of the TOE security features that would leave the TOE susceptible to attack. The TOE will provide the means for generating evidence in each security related event record of the log and for the whole log that allows the auditor to verify the integrity of the record.

4.2.5.1 O.DataImportExport: Ensure data integrity and confidentiality when transferring data to/from the TOE

To protect confidentiality and integrity when transmitting data to/from TOE either directly or via an intermediate channel.

Confidentiality and Integrity is required for the following data:

- All private, secret key material, all passphrase and PIN information.

Integrity is required for the following data:

- All PKI CMP messages, all user data, all registration data, all revocation request data, some BRSP messages, all PKI data, all identification and authentication and authorization material, audit and all archived audit records.

This is specified in SPM_TOE_INTEGRITY and SPM_USER_INTEGRITY.

4.2.5.2 O.FlawUnknownToUser: If a security flaw is discovered, there needs to be a way to notify users of the flaw.

In order to maintain the assurance level, after a discovery of a flaw, the user must be aware of the impact and any corrective action.

4.2.5.3 O.FlawRemediation: If a flaw is discovered in the TOE, a process will be in place to provide a corrective action and distribute the corrective action.

In order to maintain the assurance level, after a discovery of a flaw, the developer should provide remedial or corrective action to the user to protect the TOE from exploits that were not addressed during the evaluation.

4.2.5.4 O.Guidance: Provide guidance documentation

To minimize user and administrator errors by providing adequate documentation, covering installation, startup, operating and maintaining a secure state for the TOE. All user interfaces, and messages shall be explained as well as any secure parameters so the users will put the system in a secure state. Guidance should also contain enough information for the users to recognize whether the TOE is in a secure state and explain any errors, warnings and audit information to help the users maintain the secure state of the TOE.

4.2.5.5 O.IntegrityTOEData: Provide adequate measures for integrity of TOE data.

Provide sufficient measures to ensure that TOE data is adequately maintained. The TOE data that requires its integrity to be maintained is specified in SPM_TOE_INTEGRITY.

4.2.5.6 O.IntegrityUserData: Provide adequate measures for integrity of user data

Provide sufficient measures to ensure that user data is adequately maintained. The user data that requires its integrity to be maintained is specified in SPM_USER_INTEGRITY.

4.2.5.7 O.ConfidentialityTOEData: Provide adequate measures for confidentiality of TOE data.

Provide sufficient measures to ensure that secret or private TOE data is kept confidential. The user data to be kept confidential is specified in SPM_TOE_CONFIDENTIALITY.

4.2.5.8 O.ConfidentialityUserData: Provide adequate measures for confidentiality of user data.

Provide sufficient measures to ensure that secret or private user data is kept confidential. The user data to be kept confidential is specified in SPM_USER_CONFIDENTIALITY.

4.2.5.9 O.LifecycleSecurity: Tools and Techniques

Tools and Techniques used during the development phase to ensure security are designed into the TOE. By defining the techniques used there is greater assurance that the implementation is appropriate and no obvious flaws have been designed into the TOE. By specifying the tools used there is greater assurance that the limitations of the tools have not conspired to create unknown flaws in the TOE.

4.2.5.10 O.MaintainUserAttributes: Maintain user attributes is in addition to user identities.

Maintain a list of security attributes that may include:

a) The access privileges – i.e., access to CA/CAO/RA/ WebRAO/Audit data;

b) The group membership; and or

c) The level of authority – i.e., CAO/WebRAO.

The PKI entities also have attributes for example which CA/RA/RA eXchange does the WebRAO connect to, and send/authorize requests to.

4.2.5.11 O.ProtectAuditRecords: This is to detect modification of audit records, and detect audit record deletion.

The TOE is to provide for mechanism to detect the modification and deletion of audit records.

4.2.5.12 O.ProtectConfiguration: Protect the PKI configuration from unauthorized changes.

The TOE will provide for mechanism to preserve the integrity of the PKI configuration and to ensure only authorized configuration changes can be accepted.

4.2.5.13 O.ProvideEvidenceOfOrigin: Enforced proof of origin

Ensure that the origin of a message can be established. This is required for all PKIX-CMP messages between: the PKI trusted entities; the BRSP message between the RA eXchange and WebRAO components; all CRLs; all OCSP messages.

4.2.5.14 O.Passphrase: No weak passphrase.

To prevent the use of weak passphrase for PSE and P12's the TOE enforces the use of passphrases that achieve a minimum requirement.

4.2.6 Physical

4.2.6.1 O.ControlUnknownOriginComms: To ensure only authorized entities can connect to the TOE

To protect the TOE, communications from unknown sources should be controlled. This also requires that the TOE ignore security attributes on user data that is imported from external sources.

4.2.6.2 O.MaliciousCodeNotExecuted: To ensure only trusted code is executed on the TOE platform

To protect the TOE, any installed code should be signed and the TOE users are only to execute code signed by a trusted entity.

4.3 Security Objectives for the Environment

4.3.1 The following security objectives for the environment trace back to aspects of identified threats not completely countered by the TOE and/or organizational security policies or assumptions not completely met by the TOE.

4.3.1.1 OE.BackupStorageRestoration: Backup, Storage and effective restoration

There must be sufficient backup storage and effective restoration to ensure the system can be re-created. There must be a method to ensure data integrity. There must be a method to ensure confidentiality of secret and or private key material and other confidential data.

🗎 As a guide, two roles should be used to recover the system to prevent a rogue administrator from temporarily creating a masquerading TOE, for example:

1. System administrator who performs backup and restore duties
2. CAO user who can restore key material.

4.3.1.2 OE.Audit: Manage the audit log to ensure it is regularly reviewed and checked and to prevent loss of audit data.

The TOE owners must ensure that A.AuditReview is upheld.

4.3.1.3 OE.CPS: PKI users will be familiar with and uphold the CP and CPS that the PKI operates

The TOE owners must ensure that A.CPS is upheld.

4.3.1.4 OE.CompetentPKIUsers: PKI users will be competent

The TOE owners must ensure that A.CompetentPKIUsers is upheld.

4.3.1.5 OE.MaliciousCodeNotExecuted: TOE users will not execute malicious code

The TOE owners must ensure that A.MaliciousCodeNotExecuted is upheld.

4.3.1.6 OE.SecureInstallation: Ensure that the system is set up and operated securely

The TOE owners must ensure that A.SecureInstallation is upheld.

4.3.1.7 OE.Guidance: Ensure that the administrators and users read and follow the guidance material

The TOE owners must ensure that A.Guidance is upheld.

4.3.1.8 OE.TamperNotify: The HSM must provide passive detection of physical tampering.

Any HSMs holding secret, private or signing keys must provide the ability to allow users to detect physical tampering.

FPT_PHP.1 Passive detection of physical attack
Hierarchical to: No other components.
FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

4.3.1.9 OE.Cryptography: Selection of Appropriate Crypto algorithms and parameters.

Those responsible for the TOE must ensure that all cryptographic operations have been implemented correctly.

4.3.1.10 OE.HardwareFunctions: All hardware crypto modules, if used, must provide specified security functions.

When any crypto modules are used with the TOE they must be certified to at least the EAL 4 level to provide the following functions:

FIA_UID.1 and FIA_UAU.1
To force all users to be uniquely identified and authenticated as authorized users before accessing the other functions
FCS_CKM.4
To destroy keys securely
FCS_COP.1 Cryptographic Operation
FCS_COP.1.1 The TSF shall perform
digital signature creation.
a) RSA signature with SHA-1 hashing; or
b) RSA signature with MD5 hashing; or
c) DSA signature with SHA-1 hashing
in accordance with a specified cryptographic algorithm
a) RSA and SHA-1; or
b) RSA and MD5; or
c) DSA and SHA-1
and cryptographic key sizes

a) RSA 1024, 2048 or 4096 bit and SHA-1 160 bit
b) RSA 1024, 2048 or 4096 bit and MD5 128 bit
c) DSA 1024 or 1536 bit and SHA-1 160 bit

that meet the following:

a) [RSA] and [SHA-1]
b) [RSA] and [RFC1321]
c) [DSA] and [SHA-1] FCS_COP.1.1

FCS_COP.1 Cryptographic operation

The TSF shall perform

digital signature verification.

a) RSA signature with SHA-1 hashing; or
b) RSA signature with MD5 hashing; or
c) DSA signature with SHA-1 hashing

in accordance with a specified cryptographic algorithm

a) RSA and SHA-1; or
b) RSA and MD5; or
c) DSA and SHA-1

and cryptographic key sizes

a) RSA 1024, 2048 or 4096 bit and SHA-1 160 bit
b) RSA 1024, 2048 or 4096 bit and MD5 128 bit
c) DSA 1024 or 1536 bit and SHA-1 160 bit

that meet the following:

a) [RSA] and [SHA-1]
b) [RSA] and [RFC1321]
c) [DSA] and [SHA-1] FCS_COP.1.1_VERIFY

4.3.1.11 OE.TimeSource: Reliable and Accurate Time source

Those responsible for the TOE are responsible for ensuring that a time source for timestamping is available, and that its reliability and accuracy is acceptable to the TOE owner.

4.3.1.12 OE.PassphrasePIN: No weak passphrase and PIN.

Those responsible for the TOE must ensure that procedures exist for the secure selection and management of passphrases and PINs.

4.3.1.13 OE.Keys: Secure storage of keys.

Those responsible for the TOE must ensure that all private keys used in the operation and administration of the TOE are securely stored to prevent access by persons other than TOE administrators.

4.3.1.14 OE.Physical: Physical Security.

Those responsible for the TOE must ensure that A.PhysicalProtection is upheld.

4.3.1.15 OE.DisposalOfAuthenticationData: Proper disposal of authentication data and keys.

Those responsible for the TOE must ensure that A.DisposalofAuthenticationData is upheld.

4.3.1.16 OE.FlawRemediation: Once obtained the corrective action should be implemented.

Those responsible for the TOE must ensure that any flaw remediation corrective action provided as part of the TOE should be implemented.

4.3.1.17 OE.Connectivity: External connections.

Those responsible for the TOE must ensure that A.CommunicationsProtection is upheld

5. IT Security Requirements

5.1 Introduction

5.1.1 This section defines the detailed IT security requirements that shall be satisfied by the TOE or its environment.

5.2 TOE Security Functional Requirements

5.2.1 Security audit (FAU)

5.2.1.1 Audit data generation (FAU_GEN.1)

The TSF shall be able to generate an audit record of the following auditable events:

a) Startup and shutdown of the audit functions;

b) All auditable events for the not **specified** level of audit; and

c) **As per the following tables: Audit Data events by component, Table 5-1 to Table 5-5**.FAU_GEN.1.1

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **as detailed in the following tables** FAU_GEN.1.2

Dependencies: **[**

FPT_STM.1 Reliable Time Stamps

]

Audit Events for the CA

LABEL	Audit Event	Event description	Contents
AE_SIG_VERIFY	Signature Verification Failure	Signature Verification failure	Event type, CAO user (e.g., Windows user name), time/date, identifiable description of what failed verification and where it came from.

LABEL	Audit Event	Event description	Contents
AE_CERT_GENERATED	Certificate Generation	A Certificate has been generated, signed and stored	Event type, CA user (e.g., Windows user name), time/date, Reference #, issuer DN, subject DN, serial No, certificate
AE_CERT_REVOCATION	Certificate Revoked	A Revocation request has been processed and revoked (marked in the database as revoked, suspended, released from suspension)	Event type, CA user (e.g., Windows user name), identification of RA that revocation request was received from, time/date, unique identity of revocation message including certificate revoked, suspended or released from suspension and the revocation reason, unique identity of revocation requester and approver.
AE_CRL_GENERATION	CRL Generated	A CRL has been generated, signed and stored. Including Success and Failure	Event type, CA user (e.g., Windows user name), time/date, unique identity of CRL.
AE_CA_PKI_PUSH	PKI Information sent	PKI data is signed and pushed	Event type, CA user (e.g., Windows user name), time/date, unique identity of PKI and identity of entity it was pushed to
AE_CONNECT	User or System access initiated	A connection to the CA has been established. Including Success and Failure	Event type, CA user (e.g., Windows user name), Unique identity of user or system accessing the CA (e.g., identification of CAO user), time/date
AE_CONNECT_END	User or System access terminated	A connection to the CA has been terminated	Event type, CA user (e.g., Windows user name), Unique identity of user or system disconnected from the CA (e.g., identification of CAO user), time/date
AE_PKI_TAMPER	PKI Event	Tampered PKI detected	Event type, CA user (e.g., Windows user name), Unique identity of profile that was tampered, time/date

Table 5-1 Audit Events for the CA

Audit Events for the CAO

LABEL	Audit Event	Event description	Contents
AE_CERT_REVOKE_SUBMIT	Certificate Revoked	A Revocation request has been submitted to the CA. Including if it's successfully sent or not.	Event type, CAO user (e.g., Windows user name), time/date, unique identity of revocation message including certificate revoked, suspended or released from suspension and the revocation reason.

LABEL	Audit Event	Event description	Contents
AE_CERT_REVOKE_CONFIRM	Certificate Revoked	A Revocation request has been submitted to the CA and the CA has responded with success or fail.	Event type, CAO user (e.g., Windows user name), time/date, unique identity of revocation message including certificate revoked, suspended or released from suspension and the revocation reason.
AE_CERT_REQUEST_SEND	Certificate Request Sent	A Certificate request has been signed and sent to the CA	Event type, CAO user (e.g., Windows user name), time/date, Reference #, Request data, identification of CA to which the request was sent
AE_CERT_REQUEST_RECEIVED	Received Certificate Request	A Certificate request has been received	Event type, CAO user (e.g., Windows user name), time/date, certificate request data uniquely identifying the certificate request, certificate request receipt method (e.g., imported from floppy,)
AE_POLICY_CREATE	Policy Created	A policy was created and saved to the database	Event type, CAO user (e.g., Windows user name), time/date, unique identity of policy and policy type
AE_POLICY_RETIRED	Policy Retired	A policy was retired and saved to the database	Event type, CAO user (e.g., Windows user name), time/date, unique identity of policy and policy type
AE_POLICY_DELETED	Policy Deleted	A policy was deleted.	Event type, CAO user (e.g., Windows user name), time/date, unique identity of policy and policy type
AE_AUTHORISATION_PATH_CREATE	Processing (Authorization) Path Events	When an authorization path is added	Event type, CAO user (e.g., Windows user name), time/date, unique identity of path, group and policy and identity of entity it is to be pushed to.
AE_AUTHORISATION_PATH_MODIFY	Processing (Authorization) Path Events	CAO user uses the Authorization group definitions to define which, a subset or all, of an authorization group is required to authorize a request. This event is added when a modification of path is committed.	Event type, CAO user (e.g., Windows user name), time/date, unique identity of path, group and policy and identity of entity it is to be pushed to.

LABEL	Audit Event	Event description	Contents
AE_AUTHORISATION_PATH_RETIRE	Processing (Authorization) Path Events	CAO user uses the Authorization group definitions to define which, a subset or all, of an authorization group is required to authorize a request. This event is added when a path is retired	Event type, CAO user (e.g., Windows user name), time/date, unique identity of path, group and policy and identity of entity it is to be pushed to.
AE_SESSION_START	Session events	The CAO application may log on to a number of PKIs, but only one per session	Type, CAO user (e.g., Windows user name), time/date, unique identity of PKI.
AE_SESSION_END	Session events	The CAO application may log on to a number of PKIs, but only one per session	Type, CAO user (e.g., Windows user name), time/date, unique identity of PKI.
AE_AUDIT_ARCHIVE	Audit Archive	An archive function has been performed on the audit log within the CA database and an audit log archive file has been created.	Event type, CAO user (e.g., Windows user name), time/date, identification of audit log archive file created.

Table 5-2 Audit Events for the CAO

Audit Events for the RA

LABEL	Audit Event	Event description	Contents
AE_SIG_VERIFY	Signature Verification	Signature Verification. Success or failure	Event type, RA user (e.g., Windows user name), Unique identity of issuer of data failing signature (e.g., RAO user), time/date, identifiable description of what failed verification.
AE_MSG_VERIFY	Message Validation	Received request message validation success or failure	Event type, RA user (e.g., Windows user name), Unique identity of issuer of data failing validation (e.g., RAO user), time/date, identifiable description of the request that failed validation, a description of the validation failure (e.g., what was revoked, why and when it was revoked)

LABEL	Audit Event	Event description	Contents
AE_CERT_REQUEST_GEN	Certificate Request Generated	A Certificate Request has been generated signed and saved	Event type, RA user (e.g., Windows user name), time/date, certificate request data uniquely identifying the certificate request, indication of the type of request (e.g., renewed certificate request)
AE_CERT_REQUEST_SEND	Certificate Request Sent	A Certificate request has been signed and sent to the CA	Event type, RA user (e.g., Windows user name), time/date, Reference #, Request data, identification of CA to which the request was sent
AE_CERT_RECEIVED	Received signed certificate	A Signed Certificate was received and stored in the RA database	Event type, RA user (e.g., Windows user name), identification of CA certificate was received from, time/date, Reference #, issuer DN, subject DN, serial No, certificate
AE_CERT_STORAGE	Storage of received Certificate failed	A Signed Certificate was received but storage of that certificate failed	Event type, RA user (e.g., Windows user name), identification of CA certificate was received from, time/date, Reference #, issuer DN, subject DN, serial No, certificate, reason for failure
AE_REVOKE_REQUEST_SEND	Revocation Request Sent	A Revocation request has been signed and sent to the CA	Event type, RA user (e.g., Windows user name), time/date, Request data including unique identity of revocation request message including certificate revoked or suspended and the revocation reason, identification of entity revocation request was received from (e.g., RA eXchange, RAO), identification of entity that revocation request was received from and approved by (e.g., RA eXchange)
AE_REVOKE_MSG_RECEIVED	Received signed revocation	A Signed Revocation message was received and stored in the RA database	Event type, RA user (e.g., Windows user name), identification of CA revocation was received from, time/date, Request data including unique identity of revocation request message including certificate revoked or suspended and the revocation reason, identification of entity revocation request was received from and approved by (e.g., RA eXchange)
AE_REVOKE_MSG_STORAGE	Storage of received revocation message failed	A Signed revocation message was received but storage of that message failed	Event type, RA user (e.g., Windows user name), identification of CA revocation was received from, time/date, request data, unique identity of revocation message including certificate revoked, reason for failure

LABEL	Audit Event	Event description	Contents
AE_CONNECT_SUCCESS	RA has connected to a CA	A connection to the CA has been established	Event type, RA user (e.g., Windows user name), Unique identity of system accessing the CA (e.g., identification of RA), time/date
AE_CONNECT_END	RA has disconnected from the CA	A connection to the CA has been terminated	Event type, RA user (e.g., Windows user name), Unique identity of system disconnected from the CA (e.g., identification of RA), time/date
AE_ANNOUNCE	RA is trying to connect to a CA	Announce message sent to the CA	Event type, RA user (e.g., Windows user name), Identity of the CA (e.g., identification of CA inc port machine name), time/date
AE_PKI_RECEIVED	PKI information is received.	Event includes CRL, Policies, Auth Groups and PKI entities	Event type, RA user (e.g., Windows user name), identification of entity the policy was received from, time/date, unique identity of policy

Table 5-3 Audit Events for the RA

Audit Events for the RA Event Viewer

LABEL	Audit Event	Event description	Contents
AE_AUDIT_ARCHIVE	Audit Archive	An archive function has been performed on the audit log within the RA database and an audit log archive file has been created.	Event type, RA Event Viewer user (e.g., Windows user name), time/date, identification of audit log archive file created.

Table 5-4 Audit Events for the RA Event Viewer

Audit Events for the RA eXchange

LABEL	Audit Event	Event description	Contents
AE_SIG_VERIFY	Signature Verification Failure	Signature verification failure	Event type, Unique RA eXchange, or RA eXchange interface identifier, Unique identity of issuer of data failing signature (e.g., end entity cert requester), time/date, identifiable description of what failed verification (e.g., request data)
AE_CERT_REQUEST_RECD	Certificate Request Received	Certificate request is received	Event type, Unique RA eXchange or RA eXchange interface identifier, Cert Request data, time/date

LABEL	Audit Event	Event description	Contents
AE_CERT_REQUEST_SEND	Certificate Request Sent for Authentication	Certificate request sent (stored) for authentication	Event type, Unique RA eXchange or RA eXchange interface identifier, auth ID, issuer DN, subject DN, time/date
AE_CERT_RECD	Received signed certificate	A signed certificate was received	Event type, Unique RA eXchange or RA eXchange interface identifier, identification of RA certificate was received from, time/date, Reference #, issuer DN, subject DN, serial No, certificate
AE_CERT_MOD	Certificate Identity Data Modified	A certificate's identity data has been modified, the new request is also logged	Event type, Unique RA eXchange or RA eXchange interface identifier, identification of RA certificate was received from, time/date, Reference #, issuer DN, subject DN, date time.
AE_CERT_NOTICE	A notification message has been sent	A certificate rejection notice has been sent to the requestor.	Event type, Unique RA eXchange or RA eXchange interface identifier, time/date, description of certificate, and end user, reason the request was rejected, distribution method (e.g., email), and address (e.g., email address)

Table 5-5 Audit Events for the RA eXchange

5.2.1.2 User identity association (FAU_GEN.2)

The TSF shall be able to associate each auditable event with the identity of the user that caused the event.$^{FAU\_GEN.2.1}$

Dependencies: **[**

FAU_GEN.1 Audit Data Generation

FIA_UID.1 Timing of identification

]

5.2.1.3 Audit review (FAU_SAR.1)

The TSF shall provide the **auditors** with the capability to read **all audit records; or a user defined selection of audit records** from the audit records.$^{FAU\_SAR.1.1}$

The TSF shall provide the audit records in a manner suitable for the user to interpret the information.$^{FAU\_SAR.1.2}$

Dependencies: [

FAU_GEN.1 Audit Data Generation

]

5.2.1.4 Restricted audit review (FAU_SAR.2)

The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. FAU_SAR.2.1

Dependencies: [
FAU_SAR.1 Audit Review
]

5.2.1.5 Selectable audit review (FAU_SAR.3)

The TSF shall provide the ability to perform **searches, sorting, ordering** of audit data based on **queries as defined in the CAO documentation**, **or as selected by auditor**.]FAU_SAR.3.1

Dependencies: [
FAU_SAR.1 Audit Review
]

5.2.1.6 Protected audit trail storage (FAU_STG.1)

The TSF shall protect the stored audit records from unauthorized deletion.FAU_STG.1.1

The TSF shall be able to **detect** modifications to the audit records.FAU_STG.1.2

Dependencies: [
FAU_GEN.1 Audit Data Generation
]

5.2.2 Communication (FCO)

5.2.2.1 Enforced proof of origin (FCO_NRO.2)

The TSF shall enforce the generation of evidence of origin for transmitted

- PKI Certificates;
- PKI Entity interactions;
- P11 Interactions;
- End user Certificates;
- Certificate Revocation Lists (CRL/ARL); and
- Group Lists.

at all times.FCO_NRO.2.1

The TSF shall be able to relate the **signature** of the originator of the information, and the **all information fields above** of the information to which the evidence applies.FCO_NRO.2.2

The TSF shall provide a capability to verify the evidence of origin of information to **originator and recipient all other users** given **the originators public key certificate and access to certificate status**[2].FCO_NRO.2.3

Dependencies: [
FIA_UID.1 Timing of identification.
]

5.2.3 Cryptographic support (FCS)

5.2.3.1 Cryptographic key generation (FCS_CKM.1)

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm
a) 3DES
b) DSA
c) RSA
and specified cryptographic key sizes
a) 168 (3 key) bits
b) 1024, 1536
c) 1024, 2048, 4096
that meet the following:
a) [3DES]
b) [DSA]
c) [RSA] FCS_CKM.1.1

Dependencies: [
[FCS_CKM.2 Cryptographic key distribution or
FCS_COP.1 Cryptographic Operation]
FCS_CKM.4 Cryptographic Key Destruction
FMT_MSA.2 Secure Security Attributes
]

5.2.3.2 Cryptographic key distribution (FCS_CKM.2_PublicKey)

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method
a) X.509 public key certificate in PEM format
b) X.509 public key certificate in DER format
c) X.509 public key certificate in P7c format
d) PKCS#10
that meets the following:
a) [PEM]
b) [DER]
c) [PKCS7]
d) [PKCS10] FCS_CKM.2.1

[2] **SPM_SIGNATURE_VALIDITY**

Dependencies: [
[FDP_ITC.1 Import of user data without security attributes or
FCS_CKM.1 Cryptographic Key Generation]
FCS_CKM.4 Cryptographic Key Destruction
FMT_MSA.2 Secure Security Attributes
]

Application Note:
This SFR applies to the distribution of public keys.

5.2.3.3 Cryptographic key distribution (FCS_CKM.2)

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method
a) PKCS#11
b) PKCS#12
that meets the following:
a) [PKCS11]
b) [PKCS12] FCS_CKM.2.1

Dependencies: [
[FDP_ITC.1 Import of user data without security attributes or
FCS_CKM.1 Cryptographic Key Generation]
FCS_CKM.4 Cryptographic Key Destruction
FMT_MSA.2 Secure Security Attributes
]

Application Note:
This SFR applies to the distribution of private, secret, or signing keys by the WebRAO component of the TOE.

5.2.3.4 Cryptographic key access (FCS_CKM.3)

The TSF shall perform **provision of ability to use keys from a PKCS#12 file or PKCS#11 device** in accordance with a specified cryptographic key access method **as allowed by standard** that meets the following **PKCS#12[PKCS12] or PKCS#11[PCKS11] standards**.FCS_CKM.3.1

Dependencies: [
[FDP_ITC.1 Import of user data without security attributes or
FCS_CKM.1 Cryptographic Key Generation]
FCS_CKM.4 Cryptographic Key Destruction
FMT_MSA.2 Secure Security Attributes
]

5.2.3.5 Cryptographic key destruction (FCS_CKM.4)

The **TSF** shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **memory overwrite before deallocation** that meets the following **none**.FCS_CKM.4.1

Dependencies: [
[FDP_ITC.1 Import of user data without security attributes or

FCS_CKM.1 Cryptographic Key Generation]
FMT_MSA.2 Secure Security Attributes
]

Application Note:
This SFR applies to the destruction of private, secret, or signing keys that are held in memory.

5.2.3.6 Cryptographic operation (FCS_COP.1_SIGN)

The TSF shall perform
digital signature creation.
a) RSA signature with SHA-1 hashing; or
b) RSA signature with MD5 hashing; or
c) DSA signature with SHA-1 hashing
in accordance with a specified cryptographic algorithm
a) RSA and SHA-1; or
b) RSA and MD5; or
c) DSA and SHA-1
and cryptographic key sizes
a) RSA 1024, 2048 or 4096 bit and SHA-1 160 bit
b) RSA 1024, 2048 or 4096 bit and MD5 128 bit
c) DSA 1024 or 1536 bit and SHA-1 160 bit
that meet the following:
a) [RSA] and [SHA-1]
b) [RSA] and [RFC1321]
c) [DSA] and [SHA-1] $^{\text{FCS\_COP.1.1\_SIGN}}$

Dependencies: [
[FDP_ITC.1 Import of user data without security attributes or
FCS_CKM.1 Cryptographic Key Generation]
FCS_CKM.4 Cryptographic Key Destruction
FMT_MSA.2 Secure Security Attributes
]

5.2.3.7 Cryptographic operation (FCS_COP.1_VERIFY)

The TSF shall perform
digital signature verification.
a) RSA signature with SHA-1 hashing; or
b) RSA signature with MD5 hashing; or
c) DSA signature with SHA-1 hashing
in accordance with a specified cryptographic algorithm
a) RSA and SHA-1; or
b) RSA and MD5; or
c) DSA and SHA-1
and cryptographic key sizes
a) RSA 1024, 2048 or 4096 bit and SHA-1 160 bit
b) RSA 1024, 2048 or 4096 bit and MD5 128 bit
c) DSA 1024 or 1536 bit and SHA-1 160 bit
that meet the following:
a) [RSA] and [SHA-1]

b) [RSA] and [RFC1321]
c) [DSA] and [SHA-1] FCS_COP.1.1_VERIFY

Dependencies: [
[FDP_ITC.1 Import of User Data Without Security Attributes
Or
FCS_CKM.1 Cryptographic Key Generation]
FCS_CKM.4 Cryptographic Key Destruction
FMT_MSA.2 Secure Security Attributes
]

5.2.3.8 Cryptographic operation (FCS_COP.1_HASH)

The TSF shall perform
secure hash.
in accordance with a specified cryptographic algorithm
a) SHA-1
b) MD5
and cryptographic key sizes
a) 160 bit
b) 128 bit
that meet the following:
a) [SHA-1]
b) [RFC1321] FCS_COP.1.1_HASH

Dependencies: [
[FDP_ITC.1 Import of User Data Without Security Attributes
Or
FCS_CKM.1 Cryptographic Key Generation]
FCS_CKM.4 Cryptographic Key Destruction
FMT_MSA.72 Secure Security Attributes
]

5.2.3.9 Cryptographic operation (FCS_COP.1_ENCRYPT)

The TSF shall perform **symmetric encryption** in accordance with a specified cryptographic algorithm **Triple DES** and cryptographic key sizes **168 (3 key) bits** that meet the following **[3DES]**.FCS_COP.1.1_ENCRYPT

Dependencies: [
FDP_ITC.1 Import of User Data Without Security Attributes
Or
FCS_CKM.1 Cryptographic Key Generation
FCS_CKM.4 Cryptographic Key Destruction
FMT_MSA.2 Secure Security Attributes
]

5.2.3.10 Cryptographic operation (FCS_COP.1_DECRYPT)

The TSF shall perform **symmetric decryption** in accordance with a specified cryptographic algorithm **Triple DES** and cryptographic key sizes **168 (3 key) bits** that meet the following **[3DES]**.[FCS_COP.1.1_DECRYPT]

Dependencies: [
FDP_ITC.1 Import of User Data Without Security Attributes
Or
FCS_CKM.1 Cryptographic Key Generation
FCS_CKM.4 Cryptographic Key Destruction
FMT_MSA.2 Secure Security Attributes
]

5.2.4 User data protection (FDP)

5.2.4.1 Subset access control (FDP_ACC.1)

The TSF shall enforce the **Access_Control_SFP** on **list of subjects, objects and operations defined in Table 5-7**.[FDP_ACC.1.1]

Dependencies: [
FDP_ACF.1 Security Attribute based access control
]

5.2.4.2 Security attribute based access control (FDP_ACF.1)

The TSF shall enforce the Access_Control_SFP defined in Table 5-7 to objects based on security attributes defined in Table 5-7.[FDP_ACF.1.1]

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed **if the user has been explicitly granted access to the object as specified in Table 5-7**.[FDP_ACF.1.2]

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **user having the attributes for the roles as listed in Table 5-7**.[FDP_ACF.1.3]

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **user not having the attributes for the roles as listed in Table 5-7**.[FDP_ACF.1.4]

Dependencies: [
FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization
]

5.2.4.3 Subset information flow control (FDP_IFC.1)

The TSF shall enforce the **Information_Flow_Control_SFP** on **subjects, information and operations as described in Section 9.3**.[FDP_IFC.1.1]

			Relevant to the following SFR?

Subjects, as defined in section 9.2.2	Information	Permitted Operation The subject can:	FDP_ IFC.1	FDP_ IFF.1	FDP_ ITT.1	FDP_ ITT.3
Other entity to CA	• Announce Messages to the CA	The entity may • Create connection request The CA will accept a connection if the entity is a valid member of the PKI and is one of: • A CAO GUI connection on behalf of a valid CAO user, • A RA that is a current member of the PKI, • A KAS that is a current member of the PKI The CA will • Accept • Reject (and disconnect) The CA verifies that the announce message has not been delayed, has not been replayed and has been signed by a valid entity.	Yes	Yes	No	Yes
CAO to the CA	• Certificate Requests • Cross Certification Requests • Revocation Requests • CRL generation messages • PKI configuration messages	• Submit	Yes	Yes	Yes	Yes
CA to the CAO	• Certificate response • Revocation response	• Accept • Reject	Yes	Yes	No	Yes
CAO Audit Manager to other entity	• Audit events	The entity may • Access the audit records to create a set of archive audit events for export to file	Yes	No	No	No
RA Audit Manager to other entity	• Audit events	The entity may • Access the audit records to create a set of archive audit events for export to file	Yes	No	No	No
RA to the RA eXchange	• Certificate response • Revocation response	• Accept • Reject	Yes	Yes	No	No
RA eXchange to RA	• Certificate Requests • Renewal Requests • Revocation Requests	• Submit	Yes	Yes	No	No
CSS to other entity	• Certificate Status Information	• Accept • Reject	Yes	Yes	No	No
Other entity to CSS	• Certificate Status Information	• Request • Accept	Yes	Yes	No	No

			Relevant to the following SFR?			
Subjects, as defined in section 9.2.2	Information	Permitted Operation The subject can:	FDP_ IFC.1	FDP_ IFF.1	FDP_ ITT.1	FDP_ ITT.3
Other entity to RA eXchange	• Announce Messages to the RA eXchange	The entity may • Create connection request The RA eXchange will accept a connection if the entity is a valid member of the PKI and is a Protocol Handler that is from a(n): • WebRAO • Web Handler • email Handler • SCEP Handler • CMP Handler The RA eXchange will • Accept • Reject (and disconnect) The RA eXchange verifies that the announce message has not been delayed, has not been replayed and has been signed by a valid entity.	Yes	Yes	No	Yes
RA eXchange to email Handler	• Certificate response	The email Handler will accept notification requests from the RA eXchange including the Certificate message which is used to deliver certificates to any end entity,	Yes	Yes	Yes	Yes
Other entity to Web Handler	• Connection request • Certificate Request • Revocation Request • Status request	The Web Handler will accept any appropriately formatted request from any end entity	Yes	Yes	Yes	No
Other entity to email Handler	• Certificate Request •	The email Handler will accept any appropriately formatted request from any end entity	Yes	Yes	Yes	No
Other entity to SCEP Handler	• Connection request • Certificate Request •	The SCEP Handler will accept any appropriately formatted request from any end entity	Yes	Yes	Yes	No

Table 5-6 Subjects, Information and Permitted Operations for Information_Flow_Control_SFP

This table is used in multiple SFRs. The Information Flow Control SFP is relevant to that SFR only where row is marked "yes" as being relevant to the SFR in the heading column.

Dependencies: [
FDP_IFF.1 Simple Security Attributes
]

5.2.4.4 Simple security attributes (FDP_IFF.1)

The TSF shall enforce the **Information_Flow_Control_SFP (table 5-6)** based on the following types of subject and information security attributes: **those defined for each subject in Section 9.2.2** FDP_IFF.1.1

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold **as described in Section 9.3**. FDP_IFF.1.2

The TSF shall enforce the **no additional requirements**.FDP_IFF.1.3

The TSF shall provide the following **no additional capabilities.**FDP_IFF.1.4

The TSF shall explicitly authorize an information flow based on the following rules **refer to Section 9.3.**FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules **refer to Section 9.3.**FDP_IFF.1.6

Dependencies: [
FDP_IFC.1 Subset Information Flow Control.
FMT_MSA.3 Static Attribute Initialization.
]

5.2.4.5 Import of user data without security attributes (FDP_ITC.1)

The TSF shall enforce the **Information_Flow_Control_SFP (table 5-6)** when importing user data, controlled under the SFP, from outside of the TSC. FDP_ITC.1.1

The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.FDP_ITC.1.2

The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **no additional controls**.FDP_ITC.1.3

Dependencies: [
FDP_ACC.1 Subset Access Control.
FDP_IFC.1 Subset Information Flow Control.
FMT_MSA.3 Static Attribute Initialization.
]

5.2.4.6 Basic internal transfer protection (FDP_ITT.1)

The TSF shall enforce the **Access_Control_SFP (table 5-7) and Information_Flow_Control_SFP (table 5-6)** to prevent the **modification** of user data when it is transmitted between physically-separated parts of the TOE.FDP_ITT.1.1

Dependencies: [
FDP_ACC.1 Subset Access Control or
FDP_IFC.1 Subset Information Flow Control.
]

5.2.4.7 Integrity monitoring (FDP_ITT.3)

The TSF shall enforce the **Access_Control_SFP (table 5-7) and Information_Flow_Control_SFP (table 5-6)** to monitor user data transmitted between physically separated parts of the TOE for the following errors. **If the signature is not verified, the data is assumed to be corrupt or from an untrusted source**.FDP_ITT.3.1

Upon detection of a data integrity error, the TSF shall **logically disconnect the entity that sent the message and log the event**FDP_ITT.3.2

Dependencies: [
[FDP_ACC.1 Subset Access Control or
FDP_IFC.1 Subset Information Flow Control]
FDP_ITT.1 Basic Internal Transfer Protection
]

5.2.4.8 Subset residual information protection (FDP_RIP.1)

The TSF shall ensure that any previous information content of a resource is made unavailable upon the **de-allocation of the resource from** the following objects:

Secret or Private Key Material held in memory when a software cryptographic operations (e.g., sign/encrypt) has occurred; and
Passphrase and PIN used to open PSE/P12 files or P11 devices
].FDP_RIP.1.1

Dependencies: None

5.2.4.9 Data authentication with identity of guarantor (FDP_DAU.2)

The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of

Certificate Requests and Certificate Response
Certificate Request Authorizations and associated Response
CRL announcement
PKI Confirmation Message
PKI Error Message
Announce Message
Certificates
Certificate Revocation Lists
PKCS#10 Cross Certification Message
Certificate Status Messages
]. FDP_DAU.2.1

The TSF shall provide **All PKI Entities and users** with the ability to verify evidence of validity using **SPM_SIGNATURE_VALIDITY (section 9.1) of** the indicated information and the identity of the user that generated that evidence. FDP_DAU.2.2

Dependencies: [
FIA_UID.1 Timing of identification
]

5.2.4.10 Data authentication with identity of guarantor – CAO FDP_DAU.2_CAO

The **CAO** shall provide a capability to generate evidence that can be used as a guarantee of the validity of:

Certificate Requests
Certificate Request Authorizations
Revocation Requests
Certificate Request Authorizations
PKI Confirmation
PKI Error
Announce

]. FDP_DAU.2.1_CAO

The **CAO** shall provide **CAO users** with the ability to verify evidence of validity using **SPM_SIGNATURE_VALIDITY (Section 9.1)**
of the indicated information and the identity of the user that generated that evidence. FDP_DAU.2.2_CAO

Dependencies: [
FIA_UID.1 Timing of Identification
]

5.2.4.11 Data authentication with identity of guarantor – WebRAO (FDP_DAU.2_WebRAO)

The **WebRAO applet** shall provide a capability to generate evidence that can be used as a guarantee of the validity of

Initialization Request/Response
Certificate Requests
Certificate Request Authorizations
Revocation Requests
Revocation Request Authorizations
PKI Confirmation
PKI Error Message

. FDP_DAU.2.1_WebRAO

The **WebRAO applet** shall provide **WebRAO users (section 9.2.2)** with the ability to verify evidence of validity using **SPM_SIGNATURE_VALIDITY**
of the indicated information and of the indicated information and the identity of the user that generated that evidence. FDP_DAU.2.2_WebRAO

Dependencies: [
FIA_UID.1 Timing of Identification
]

5.2.5 Identification and authentication (FIA)

5.2.5.1 User attribute definition (FIA_ATD.1)

The TSF shall maintain the following list of security attributes belonging to individual users:

(See Section 9.2.2) User's Identity including:
X500 Distinguished Name.
Authentication Information:
User Role
Group – based on DN, defined by the CAO user
Registered Entity
Authentication Method – Fixed Digital Signature.
Access Information
Audit Data
PKI Entity – e.g., CA/RA
]. FIA_ATD.1.1

Dependencies: [
No dependencies
]

5.2.5.2 Timing of authentication (FIA_UAU.1)

The TSF shall allow

Starting of TOE modules
Shutting down of TOE modules
Bootstrapping
Editing CA and CAO policies
Requesting registration
Requesting revocation
Requesting certificate status information
Accessing the Web Handler web pages
Submitting email requests for registration

on behalf of the user to be performed before the user is authenticated.FIA_UAU.1.1

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.FIA_UAU.1.2

Dependencies: [
FIA_UID.1 Timing of Identification
]

5.2.5.3 User Authentication Before any action (FIA_UAU.2_CAO)

The **CAO** shall require each user to be successfully authenticated before allowing **any other CAO mediated actions** on behalf of that user.FIA_UAU.2.1_CAO

Dependencies: [
FIA_UID.1_CAO Timing of Identification
]

5.2.5.4 User Authentication Before any action (FIA_UAU.2_WebRAO)

The **WebRAO** shall require each user to be successfully authenticated before allowing **any other WebRAO mediated actions** on behalf of that user.FIA_UAU.2.1_WebRAO

Dependencies: [
FIA_UID.1_WebRAO Timing of Identification
]

5.2.5.5 Timing of identification (FIA_UID.1)

The TSF shall allow:

Starting of TOE modules
Shutting down of TOE modules
Bootstrapping
Editing registration policies
Requesting registration
Requesting revocation
Requesting certificate status information
Accessing the Web Handler web pages
Submitting email requests for registration

on behalf of the user to be performed before the user is identified.FIA_UID.1.1

The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.FIA_UID.1.2

Dependencies: [
No Dependencies
]

5.2.5.6 User identification before any action (FIA_UID.2_CAO)

The **CAO** shall require each user to identify itself before allowing any other **CAO**-mediated actions on behalf of that user.FIA_UID.2.1_CAO

Dependencies: [
No Dependencies
]

5.2.5.7 User identification before any action (FIA_UID.2_WebRAO)

The **WebRAO** shall require each user to identify itself before allowing any other **WebRAO**-mediated actions on behalf of that user.FIA_UID.2.1_WebRAO

Dependencies: [
No Dependencies
]

5.2.5.8 User-subject binding (FIA_USB.1)

The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.FIA_USB.1.1

Dependencies: [
FIA_ATD.1 User Attribute Definition
]

Application Note:

The following are valid security attributes (see section 9.2.2)

- *X.509 certificate*
- *X.509 certificate extensions*
- *X.509 certificate custom extensions such as BLT {used for PKI Entity certificate}*
- *User role attributes {e.g., CA auditor role}*
- *Group Membership rules for WebRAO defined by the CAO administrator*

5.2.5.9 Verification of Secrets (FIA_SOS.1)

The TSF shall provide a mechanism to verify that secrets meet **SPM_PASSWORD_METRIC (Section 9.1)**.FIA_SOS.1.1

Dependencies: [
No Dependencies
]

5.2.6 Security management (FMT)

5.2.6.1 Management of security functions behavior (FMT_MOF.1)

The TSF shall restrict the ability to **determine the behavior of** the functions **in Table 5-6** to the **subjects in Table 5-7**.FMT_MOF.1.1

Subjects, as defined in section 9.2.2	Object	Permitted Operation	Relevant to FMT_MSA.1?	Relevant to FMT_MTD.1?
CAO Audit Manager	CA Audit Log	Archive Query	No	Yes
CAO Auditor	CA Audit Log	Query	No	Yes
CAO user WebRAO user	Certificate	Register certificate requests, and check the status of these requests Approve or reject a certificate request Approve or reject a revocation request View certificates and certificate status	Yes	Yes
CAO user with required permissions	Cryptographic keys	Key Generation Key Distribution Key Access Key Destruction Determine cryptographic algorithms Determine cryptographic key sizes	No	Yes

Subjects, as defined in section 9.2.2	Object	Permitted Operation	Relevant to FMT_MSA.1?	Relevant to FMT_MTD.1?
CAO user with required permissions	PKI	View and Modify the PKI Read Access Rights Manage Other Users' permissions Create and Manage Registration Policies Authorize CA Certificates Revoke CA Certificates Authorize PKI Entity Certificates Revoke PKI Entity Certificates Authorize End Entity Certificates Revoke End Entity Certificates Create and edit authorization groups	Yes	No
All CAO users, CA	CA Audit Log	Insert signed records as a result of actions	No	Yes
Key owner	PSE or P12 file	Access private key accessed from file as owner and use it to sign data Use the Token Manager component functionality to operate on	No	No
Owners of certificates for PKI entities	PKI Entities (CA, CAO, RA, RA eXchange, Web PH, email PH, SCEP PH, CSS)	Start the relevant TOE component	No	No
RA Audit Manager	RA Audit Log	Archive Query	No	Yes
RA Auditor	RA Audit Log	Query	No	Yes
All RA users, RA eXchange user	RA Audit Log	Insert signed records as a result of actions	No	Yes
WebRAO user	Cryptographic keys	Key Generation Key Distribution Key Access Key Destruction Determine cryptographic algorithms Determine cryptographic key sizes	No	Yes

Table 5-7 Subjects, Objects and Permitted Operations for Access_Control_SFP

This table is used in multiple SFRs. The Access Control SFP is relevant to that SFR only where row is marked "yes" as being relevant to the SFR in the heading column.

Dependencies: [
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles.
]

5.2.6.2 Management of security attributes (FMT_MSA.1)

The TSF shall enforce the **Access_Control_SFP** to restrict the ability to **query, modify, delete** the security attributes **objects, as listed in Table 5-7 (where row**

is marked as being relevant to FMT_MSA.1) to **subjects, as listed in Table 5-7 (where row is marked as being relevant to FMT_MSA.1)** .FMT_MSA.1.1

Dependencies: [
[FDP_ACC.1 Subset Access Control or
FDP_IFC.1 Subset Information Flow Control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security Roles
]

5.2.6.3 Secure security attributes (FMT_MSA.2)

The TSF shall ensure that only secure values are accepted for security attributes.FMT_MSA.2.1

Dependencies: [
ADV_SPM.1 Informal TOE Security Policy Model
[FDP_ACC.1 Subset Access Control
Or
FDP_IFC.1 Subset Information Flow Control]
FMT_MSA.1 Management of Security Attributes
FMT_SMR.1 Security Roles
]

5.2.6.4 Static attribute initialization (FMT_MSA.3)

The TSF shall enforce the **SFP in Table 5-7** to provide **permissive** default values for security attributes that are used to enforce the SFP.FMT_MSA.3.1

The TSF shall allow the **roles in Table 5-7** to specify alternative initial values to override the default values when an object or information is created.FMT_MSA.3.2

Dependencies: [
FMT_MSA.1 Management of Security Attributes
FMT_SMR.1 Security Roles
]

5.2.6.5 Management of TSF data (FMT_MTD.1)

The TSF shall restrict the ability to **query, modify, delete or clear according to Table 5-7** the **data listed in Table 5-7 as "objects" (in rows noted as being relevant to FMT_MTD.1)** to **subjects listed in Table 5-7 (in rows noted as being relevant to FMT_MTD.1)** FMT_MTD.1.1

Dependencies: [
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security Roles
]

5.2.6.6 Management of limits on TSF data (FMT_MTD.2)

The TSF shall restrict the specification of the limits for **Certificate Validity** to **CAO users, WebRAO users**.FMT_MTD.2.1

The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits **Certificate request to be rejected or modified**.FMT_MTD.2.2

Dependencies: [

FMT_MTD.1 Management of TSF Data

FMT_SMR.1 Security Roles

]

5.2.6.7 Revocation (FMT_REV.1)

The TSF shall restrict the ability to revoke security attributes associated with the **users and PKI entities** within the TSC to **users and administrators (as defined in 9.2.2)** .FMT_REV.1.1

The TSF shall enforce the rules **SPM_REVOKE_CERTIFICATE, SPM_REMOVE_PKI, SPM_CHANGE_WEBRAO_GROUP, SPM_CHANGE_CAO_ATTRIBUTE**.FMT_REV.1.2

Dependencies: [

FMT_SMR.1 Security Roles

]

Application notes:

The following are valid security attribute

- X.509 certificate
- X.509 certificate extensions
- X.509 certificate custom extensions such as BTL
- User role attributes, i.e., CAO auditor role
- Group membership rules

The following cannot be controlled by the TSF

- Database access

The following can have their attributes revoked:

- PKI entities
- PKI entity users
- PKI trusted users, e.g., KAS
- PKI entity user attributes – e.g., CAO auditor role

Revocation can occur by:

- The CAO user removing the entity from the PKI.
- Changing the attributes of the entity in the PKI definition
- When the certificate expires
- Trust list is compromised
- Revoking the certificate

5.2.6.8 Time-limited authorization (FMT_SAE.1)

The TSF shall restrict the capability to specify an expiration time for **all digital certificate expiry dates** to **CAO user and WebRAO users, defined by the registration policy and CA expiry**.FMT_SAE.1.1

For each of these security attributes, the TSF shall be able to **reject all requests signed with that certificate, reject connection requests, and optionally notify the user or forward a renewal** after the expiration time for the indicated security attribute has passed.FMT_SAE.1.2

Dependencies: [

FMT_SMR.1 Security Roles
FPT_STM.1 Reliable Time Stamps

]

5.2.6.9 Specification of Management Functions (FMT_SMF.1)

The TSF shall be capable of performing the following security management functions: **Archive Audit Log and Delete Archived Audit Records**. FMT_SMF.1.1

Dependencies: [

No Dependencies

]

5.2.6.10 Security roles (FMT_SMR.1)

The **TSF** shall maintain the roles **the "Subjects" defined in Section 9.2.2**. FMT_SMR.1.1

The **TSF** shall be able to associate users with roles.FMT_SMR.1.2

Dependencies:

[
FIA_UID.1 Timing of Identification
]

5.2.7 Protection of the TOE Security Functions (FPT)

5.2.7.1 Inter-TSF confidentiality during transmission (FPT_ITC.1_RA)

The **RA** shall protect all **confidential** TSF data transmitted from the TSF to a remote trusted IT product **(the KAS)** from unauthorized disclosure during transmission.FPT_ITC.1.1_RA

🗎 This applies only to exporting the private key to the KAS.

Dependencies: [
No Dependencies
]

5.2.7.2 Inter-TSF detection of modification (FPT_ITI.1)

The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: **SPM_Signature_Validity**.FPT_ITI.1.1

The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform : **the TSF shall logically disconnect the connecting entity, reject the message, and log the event** if modifications are detected.FPT_ITI.1.2

Dependencies: [
No Dependencies
]

5.2.7.3 Basic Internal TSF data transfer protection (FPT_ITT.1_WebRAO)

The TSF shall protect TSF data from **disclosure and modification** when it is transmitted between separate parts of the TOE.FPT_ITT.1.1_WebRAO

Dependencies: [
No Dependencies
]

Application note:

This SFR is intended to refer to the functionality where the WebRAO protects TSF data from disclosure (when sending private keys via the RA eXchange to the KAS for archive) and modification (for all messages) between itself and the RA eXchange.

5.2.7.4 Basic Internal TSF data transfer protection (FPT_ITT.1)

The TSF shall protect TSF data from **modification** when it is transmitted between separate parts of the TOE.FPT_ITT.1.1

Dependencies: [
No Dependencies
]

5.2.7.5 Simple trusted acknowledgement (FPT_SSP.1)

The TSF shall acknowledge, when requested by another part of the TSF, the receipt of an unmodified TSF data transmission. FPT_SSP.1.1

Dependencies: [
FPT_ITT.1 basic Internal TSF Data Transfer Protection
]

5.3 TOE Security Assurance Requirements

5.3.1 This section defines the Security Assurance Requirements (SARs) of the TOE as Evaluation Assurance Level (EAL) 4 augmented with ALC_FLR.2, specified in terms of assurance components in the Common Criteria (CC) Part 3. The SARs are summarized in the following table.

Assurance Class		Assurance Component	
ASE	Security Target	ASE_DES.1	TOE Description
		ASE_ENV.1	Security Environment
		ASE_INT.1	ST Introduction
		ASE_OBJ.1	Security Objectives
		ASE_PPC.1	PP Claims
		ASE_REQ.1	IT Security Requirements
		ASE_SRE.1	Explicitly stated IT Security Requirements
		ASE_TSS.1	TOE Summary Specification
ACM	Configuration Management	ACM_AUT.1	Partial CM automation
		ACM_CAP.4	Generation support and acceptance procedures
		ACM_SCP.2	Problem tracking CM coverage
ADO	Delivery and Operation	ADO_DEL.2	Detection of modification
		ADO_IGS.1	Installation, Generation, and Startup Procedures
ADV	Development	ADV_FSP.2	Fully defined external interfaces
		ADV_HLD.2	Security Enforcing High-Level Design
		ADV_IMP.1	Subset of the implementation of the TSF
		ADV_LLD.1	Descriptive low-level design
		ADV_RCR.1	Informal Correspondence Demonstration
		ADV_SPM.1	Informal TOE security policy model

Assurance Class		Assurance Component	
AGD	Guidance Documents	AGD_ADM.1	Administrator Guidance
		AGD_USR.1	User Guidance
ALC	Life Cycle Support	ALC_DVS.1	Identification of Security Measures
		ALC_FLR.2	Flaw reporting procedures
		ALC_LCD.1	Developer defined life-cycle model
		ALC_TAT.1	Well-defined development tools
ATE	Tests	ATE_COV.2	Analysis of Coverage
		ATE_DPT.1	Testing: High Level Design
		ATE_FUN.1	Functional Testing
		ATE_IND.2	Independent Testing - Sample
AVA	Vulnerability Assessment	AVA_MSU.2	Validation of analysis
		AVA_SOF.1	Strength of TOE Security Function Evaluation
		AVA_VLA.2	Independent vulnerability analysis

Table 5-8 – TOE Security Assurance Requirements

5.3.2 The remainder of this section contains details of the assurance components, listed above, from Part 3 of the CC.

5.3.3 Configuration management (ACM)

5.3.3.1 Partial CM automation (ACM_AUT.1)

The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation.[ACM_AUT.1.1C]

The developer shall use a CM system.[ACM_AUT.1.1D]

The CM system shall provide an automated means to support the generation of the TOE.[ACM_AUT.1.2C]

The developer shall provide a CM plan.[ACM_AUT.1.2D]

The CM plan shall describe the automated tools used in the CM system.[ACM_AUT.1.3C]

The CM plan shall describe how the automated tools are used in the CM system.[ACM_AUT.1.4C]

5.3.3.2 Generation support and acceptance procedures (ACM_CAP.4)

The CM system shall provide measures such that only authorized changes are made to the configuration items.[ACM_CAP.4.10C]

The CM system shall support the generation of the TOE.[ACM_CAP.4.11C]

The acceptance plan shall describe the procedures used to accept modified or newly created configuration items as part of the TOE.[ACM_CAP.4.12C]

The reference for the TOE shall be unique to each version of the TOE.[ACM_CAP.4.1C]

The developer shall provide a reference for the TOE.[ACM_CAP.4.1D]

The TOE shall be labelled with its reference.[ACM_CAP.4.2C]

The developer shall use a CM system.[ACM_CAP.4.2D]

The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.[ACM_CAP.4.3C]

The CM list shall identify all configuration items that comprise the TOE.

The developer shall provide CM documentation.[ACM_CAP.4.3D]

The configuration list shall describe the configuration items that comprise the TOE.[ACM_CAP.4.4C]

The CM documentation shall describe the method used to uniquely identify the configuration items.[ACM_CAP.4.5C]

The CM system shall uniquely identify all configuration items.[ACM_CAP.4.6C]

The CM plan shall describe how the CM system is used.[ACM_CAP.4.7C]

The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.[ACM_CAP.4.8C]

The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.[ACM_CAP.4.9C]

5.3.3.3 Problem tracking CM coverage (ACM_SCP.2)

The list of configuration items shall include the following: implementation representation; security flaws; and the evaluation evidence required by the assurance components in the ST.[ACM_SCP.2.1C]

The developer shall provide a list of configuration items for the TOE.[ACM_SCP.2.1D]

5.3.4 Delivery and operation (ADO)

5.3.4.1 Detection of modification (ADO_DEL.2)

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user’s site.[ADO_DEL.2.1C]

The developer shall document procedures for delivery of the TOE or parts of it to the user.[ADO_DEL.2.1D]

The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.[ADO_DEL.2.2C]

The developer shall use the delivery procedures.[ADO_DEL.2.2D]

The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user’s site.[ADO_DEL.2.3C]

5.3.4.2 Installation, generation, and startup procedures (ADO_IGS.1)

The installation, generation, and startup documentation shall describe the steps necessary for secure installation, generation, and startup of the TOE.[ADO_IGS.1.1C]

The developer shall document procedures necessary for the secure installation, generation, and startup of the TOE.[ADO_IGS.1.1D]

5.3.5 Development (ADV)

5.3.5.1 Fully defined external interfaces (ADV_FSP.2)

The functional specification shall describe the TSF and its external interfaces using an informal style.[ADV_FSP.2.1C]

The developer shall provide a functional specification.[ADV_FSP.2.1D]

The functional specification shall be internally consistent.[ADV_FSP.2.2C]

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.[ADV_FSP.2.3C]

The functional specification shall completely represent the TSF.[ADV_FSP.2.4C]

The functional specification shall include rationale that the TSF is completely represented.[ADV_FSP.2.5C]

5.3.5.2 Security enforcing high-level design (ADV_HLD.2)

The presentation of the high-level design shall be informal.$^{\text{ADV\_HLD.2.1C}}$

The developer shall provide the high-level design of the TSF.$^{\text{ADV\_HLD.2.1D}}$

The high-level design shall be internally consistent.$^{\text{ADV\_HLD.2.2C}}$

The high-level design shall describe the structure of the TSF in terms of subsystems.$^{\text{ADV\_HLD.2.3C}}$

The high-level design shall describe the security functionality provided by each subsystem of the TSF.$^{\text{ADV\_HLD.2.4C}}$

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.$^{\text{ADV\_HLD.2.5C}}$

The high-level design shall identify all interfaces to the subsystems of the TSF.$^{\text{ADV\_HLD.2.6C}}$

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.$^{\text{ADV\_HLD.2.7C}}$

The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.$^{\text{ADV\_HLD.2.8C}}$

The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems. $^{\text{ADV\_HLD.2.9C}}$

5.3.5.3 Subset of the implementation of the TSF (ADV_IMP.1)

The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.$^{\text{ADV\_IMP.1.1C}}$

The developer shall provide the implementation representation for a selected subset of the TSF.$^{\text{ADV\_IMP.1.1D}}$

The implementation representation shall be internally consistent.$^{\text{ADV\_IMP.1.2C}}$

5.3.5.4 Descriptive low-level design (ADV_LLD.1)

The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.$^{\text{ADV\_LLD.1.10C}}$

The presentation of the low-level design shall be informal.$^{\text{ADV\_LLD.1.1C}}$

The developer shall provide the low-level design of the TSF.$^{\text{ADV\_LLD.1.1D}}$

The low-level design shall be internally consistent.$^{\text{ADV\_LLD.1.2C}}$

The low-level design shall describe the TSF in terms of modules.ADV_LLD.1.3C

The low-level design shall describe the purpose of each module.ADV_LLD.1.4C

The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.ADV_LLD.1.5C

The low-level design shall describe how each TSP-enforcing function is provided.ADV_LLD.1.6C

The low-level design shall identify all interfaces to the modules of the TSF.ADV_LLD.1.7C

The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.ADV_LLD.1.8C

The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate.ADV_LLD.1.9C

5.3.5.5 Informal correspondence demonstration (ADV_RCR.1)

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.ADV_RCR.1.1C

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.ADV_RCR.1.1D

5.3.5.6 Informal TOE security policy model (ADV_SPM.1)

The TSP model shall be informal.ADV_SPM.1.1C

The developer shall provide a TSP model.ADV_SPM.1.1D

The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.ADV_SPM.1.2C

The developer shall demonstrate correspondence between the functional specification and the TSP model.ADV_SPM.1.2D

The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.ADV_SPM.1.3C

The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.ADV_SPM.1.4C

5.3.6 Guidance documents (AGD)

5.3.6.1 Administrator guidance (AGD_ADM.1)

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.[AGD_ADM.1.1C]

The developer shall provide administrator guidance addressed to system administrative personnel.[AGD_ADM.1.1D]

The administrator guidance shall describe how to administer the TOE in a secure manner.[AGD_ADM.1.2C]

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.[AGD_ADM.1.3C]

The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.[AGD_ADM.1.4C]

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.[AGD_ADM.1.5C]

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.[AGD_ADM.1.6C]

The administrator guidance shall be consistent with all other documentation supplied for evaluation.[AGD_ADM.1.7C]

The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.[AGD_ADM.1.8C]

5.3.6.2 User guidance (AGD_USR.1)

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE. [AGD_USR.1.1C]

The developer shall provide user guidance.[AGD_USR.1.1D]

The user guidance shall describe the use of user-accessible security functions provided by the TOE.[AGD_USR.1.2C]

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.[AGD_USR.1.3C]

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.[AGD_USR.1.4C]

The user guidance shall be consistent with all other documentation supplied for evaluation.[AGD_USR.1.5C]

The user guidance shall describe all security requirements for the IT environment that are relevant to the user.[AGD_USR.1.6C]

5.3.7 Life cycle support (ALC)

5.3.7.1 Identification of security measures (ALC_DVS.1)

The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.[ALC_DVS.1.1C]

The developer shall produce development security documentation.[ALC_DVS.1.1D]

The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.[ALC_DVS.1.2C]

5.3.7.2 Flaw reporting procedures (ALC_FLR.2)[3]

The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.[ALC_FLR.2.1C]

The developer shall provide flaw remediation procedures addressed to TOE developers.[ALC_FLR.2.1D] [4]

The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.[ALC_FLR.2.2C]

The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.[ALC_FLR.2.2D]

The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.[ALC_FLR.2.3C]

The developer shall provide flaw remediation guidance addressed to TOE users.[ALC_FLR.2.3D]

The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.[ALC_FLR.2.4C]

[3] ALC_FLR is not part of an EAL 4 evaluation. This component is used to augment the EAL4 evaluation to allow flaw remediation and corrective actions, which are security relevant, to be distributed to end users.

[4] This has been affected by [FLR] – the updated text is shown.

The flaw remediation procedures documentation shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.$^{\text{ALC\_FLR.2.5C}}$

The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.$^{\text{ALC\_FLR.2.6C}}$

The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.$^{\text{ALC\_FLR.2.7C}}$

The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaw in the TOE.$^{\text{ALC\_FLR.2.8C}}$

5.3.7.3 Developer defined life-cycle model (ALC_LCD.1)

The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.$^{\text{ALC\_LCD.1.1C}}$

The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.$^{\text{ALC\_LCD.1.1D}}$

The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.$^{\text{ALC\_LCD.1.2C}}$

The developer shall provide life-cycle definition documentation.$^{\text{ALC\_LCD.1.2D}}$

5.3.7.4 Well-defined development tools (ALC_TAT.1)

All development tools used for implementation shall be well-defined.$^{\text{ALC\_TAT.1.1C}}$

The developer shall identify the development tools being used for the TOE.$^{\text{ALC\_TAT.1.1D}}$

The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.$^{\text{ALC\_TAT.1.2C}}$

The developer shall document the selected implementation-dependent options of the development tools.$^{\text{ALC\_TAT.1.2D}}$

The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.$^{\text{ALC\_TAT.1.3C}}$

5.3.8 Tests (ATE)

5.3.8.1 Analysis of coverage (ATE_COV.2)

The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.$^{\text{ATE\_COV.2.1C}}$

The developer shall provide an analysis of the test coverage.$^{\text{ATE\_COV.2.1D}}$

The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete. $^{\text{ATE\_COV.2.2C}}$

5.3.8.2 Testing: high-level design (ATE_DPT.1)

The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.$^{\text{ATE\_DPT.1.1C}}$

The developer shall provide the analysis of the depth of testing.$^{\text{ATE\_DPT.1.1D}}$

5.3.8.3 Functional testing (ATE_FUN.1)

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.$^{\text{ATE\_FUN.1.1C}}$

The developer shall test the TSF and document the results.$^{\text{ATE\_FUN.1.1D}}$

The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.$^{\text{ATE\_FUN.1.2C}}$

The developer shall provide test documentation.$^{\text{ATE\_FUN.1.2D}}$

The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.$^{\text{ATE\_FUN.1.3C}}$

The expected test results shall show the anticipated outputs from a successful execution of the tests.$^{\text{ATE\_FUN.1.4C}}$

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.$^{\text{ATE\_FUN.1.5C}}$

5.3.8.4 Independent testing - sample (ATE_IND.2)

The TOE shall be suitable for testing.$^{\text{ATE\_IND.2.1C}}$

The developer shall provide the TOE for testing.$^{\text{ATE\_IND.2.1D}}$

The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF. $^{\text{ATE\_IND.2.2C}}$

5.3.9 Vulnerability assessment (AVA)

5.3.9.1 Validation of analysis (AVA_MSU.2)

The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.$^{AVA\_MSU.2.1C}$

The developer shall provide guidance documentation. $^{AVA\_MSU.2.1D}$
The guidance documentation shall be complete, clear, consistent and reasonable.$^{AVA\_MSU.2.2C}$

The developer shall document an analysis of the guidance documentation.$^{AVA\_MSU.2.2D}$
The guidance documentation shall list all assumptions about the intended environment.$^{AVA\_MSU.2.3C}$

The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).$^{AVA\_MSU.2.4C}$

The analysis documentation shall demonstrate that the guidance documentation is complete.$^{AVA\_MSU.2.5C}$

5.3.9.2 Strength of TOE security function evaluation (AVA_SOF.1)

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.$^{AVA\_SOF.1.1C}$

The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.$^{AVA\_SOF.1.1D}$

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.$^{AVA\_SOF.1.2C}$

5.3.9.3 Independent vulnerability analysis (AVA_VLA.2)

The vulnerability analysis documentation shall describe the analysis of the TOE deliverables performed to search for ways in which the a user can violate the TSP.$^{AVA\_VLA.2.1C}$

The developer shall perform a vulnerability analysis.$^{AVA\_VLA.2.1D}$

The vulnerability analysis documentation shall describe the disposition of identified vulnerabilities.$^{AVA\_VLA.2.2C}$

The developers shall provide vulnerability analysis documentation.$^{AVA\_VLA.2.2D}$

The vulnerability analysis documentation shall show, for all identified vulnerabilities that the vulnerability cannot be exploited in the intended environment for the TOE.$^{AVA\_VLA.2.3C}$

The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.AVA_VLA.2.4C

5.4 Security Requirements for the IT Environment

5.4.1 Each of the environmental security objectives is either met by IT or non-IT means.

5.4.2 Table 5-7 summarizes the way in which environmental security objectives are addressed and lists the Security Requirements on the IT Environment. The actual SFRs to be provided by the IT environment are listed under the Environmental Security Objectives they relate to, as listed in this table:

Environmental Security Objective	IT Environment Security Requirement	Comment and justification where appropriate
OE.BackupStorageRestoration	Nil	addressed by Non-IT means
OE.Audit	Nil	addressed by Non-IT means
OE.TamperNotify	IT for HSM	FPT_PHP.1, which contributes to achieving this security objective because it matches the security objective exactly.
OE.Cryptography	Nil	addressed by Non-IT means
OE.HardwareFunctions	IT for HSM, Smart cards	FIA_UAU.1, FIA_UID.1, FCS_COP.1, FCS_CKM.4, which contribute to achieving this security objective because they match the security objective exactly.
OE.TimeSource	Nil	addressed by Non-IT means
OE.PassphrasePIN	Nil	addressed by Non-IT means
OE.Keys	Nil	addressed by Non-IT means
OE.Physical	Nil	addressed by Non-IT means
OE.DisposalOfAuthenticationDate	Nil	addressed by Non-IT means
OE.FlawRemediation	Nil	addressed by Non-IT means
OE.CPS	Nil	addressed by Non-IT means
OE.CompetentPKIUsers	Nil	addressed by Non-IT means
OE.MaliciousCodeNotExecuted	Nil	addressed by Non-IT means
OE.SecureInstallation	Nil	addressed by Non-IT means
OE.Guidance	Nil	addressed by Non-IT means

Environmental Security Objective	IT Environment Security Requirement	Comment and justification where appropriate
OE.Connectivity	Nil	addressed by Non-IT means

Table 5-9 – Method for addressing the environmental security objectives

5.5 Minimum Strength of Function Level

Most of the TOE's Security Functional Requirements that are realized by probabilistic or permutational mechanisms are cryptographic in nature and therefore the assessment of their algorithmic strength is out of scope of the evaluation, being assessed by the National Authority.

However one mechanism does require a strength of function assessment. This is the mechanism that protects the privacy and integrity of the ".pse" file. This is implemented by the functions IA_Identify, KG_Generate, KG_Split, KG_Update and KG_Export, and has a strength of function of SOF-Basic, so the minimum strength of function for the TOE Security Functional Requirements is SOF-Basic.

6. TOE Summary Specification

6.1 Introduction

This section defines the instantiation of the security requirements of the TOE. This specification describes the security functions and assurance measures of the TOE that meet the TOE security requirements.

6.2 TOE Security Functions

This section covers the IT security functions and specifies how these functions satisfy the TOE security functional requirements. It includes a mapping between functions and requirements that shows which functions satisfy which requirements and that all requirements are met.

6.2.1 IT Security Functions

The IT security functions provided by the TOE are described in Table 6.1. The SFR(s) that they implement are given in brackets within the description, and so the descriptions of the SFRs (provided in Chapter 5) that each IT security function is mapped to in this way also provides part of the description of the IT security function.

The description of each function in Table 6.1 provides the justification as to why the function is suitable to meet the SFRs that are mapped to it. Table 6.1 also shows which security mechanisms are implemented by which IT security function, by the mapping to the SFR(s).

Finally, Table 6.1 shows which IT security functions are realized by probabilistic or permutational mechanisms (apart from those requiring a strength-of-function claim, which are listed in the following section). This is because all such mechanisms that are implemented by the TSF are implemented using cryptographic functions (apart from those requiring a strength-of-function claim, which are listed in the following section). Therefore, all IT security functions mapped to cryptographic SFRs (i.e., Any SFR whose name begins with “FCS_”) are realized by probabilistic or permutational mechanisms.

Security Function	Description
AL_Archive	**Archive Audit Records** This function is used to allow an authorized auditor to archive the audit log and to ensure that the integrity of the log is maintained (FIA_UAU.2_CAO, FIA_UID.2_CAO, FDP_IFC.1, FMT_SAE.1, FMT_SMF.1, FMT_SMR.1).

Security Function	**Description**
AL_CreateAuditor	**Register Auditor** This function is used when assigning the auditor roles to an administrator (FIA_ATD.1). The following types of Auditor roles exist in the TOE, the CAO auditor, the CAO Audit Manager, the RA auditor, the RA Audit Manager. Only those administrators that are assigned an appropriate auditor role are able to review these logs (FAU_SAR.1, FAU_SAR.2 and FAU_SAR.3, FDP_ACC.1, FDP_ACF.1, FDP_IFF.1, FIA_UAU.2_CAO, FIA_UID.2_CAO, FMT_MOF.1, FMT_MSA.1, FMT_MTD.1). These functions cannot be used to provide greater permissions to a user than the current user has.
AL_Integrity	**Protect Audit Log.** This function is used to ensure the integrity of the audit data and prevent unauthorized deletion and detect modifications (FAU_STG.1, FPT_ITT.1) using hashing (FCS_COP.1_HASH) and digital signatures (FCS_COP.1_SIGN and FCS_COP.1_VERIFY).
AL_Logging	**Events Logging.** This function is used by various components to add audit data to the log, which is stored in a database (FAU_GEN.1). The identity of the user that caused the event is included in each log record (FAU_GEN.2).
AL_Selection	**Audit Selection** This function is used to allow an authorized auditor to select all or portions of the audit record from a database and perform sorting to facilitate checking of the audit logs (FAU_SAR.3, FIA_UAU.2_CAO, FIA_UID.2_CAO, FMT_SAE.1, FMT_SMR.1).
CG_Authorize	**Authorize Registration Request** This function is used to authorize a registration request. The action of authorizing a request involves first verifying the signature on the request (FCS_COP.1_VERIFY) then digitally signing an authorization (FCS_COP.1_SIGN, FDP_DAU.2_CAO, FDP_DAU.2_WebRAO). These functions can be used by the CAO and WebRAO users if they are valid and current users of the TSF (FIA_UID.1, FIA_UAU.2_CAO, FIA_UID.2_CAO, FIA_UAU.2_WebRAO, FIA_UID.2_WebRAO, FIA_UID.1, FMT_SAE.1, FMT_SMR.1) or may be bypassed if automatic authorization is enabled. (Note that this ST excludes the use of automatic authorization.)

Security Function	Description
CG_Distribute	**Distribute Certificate** This function is used to retrieve a certificate from the database, update its status to reflect the action, and return it to the end entity via an assigned return path (FDP_IFC.1).
CG_Generate	**Generate Certificate** This function is used to create a certificate on the basis of an authorized certificate request (FDP_DAU.2_CAO). This involves querying the status of the certificate in the database while creating it, and storing the certificate in the database after creation. This is performed by the appropriate CA. Certificates will be digitally signed by the CA (FCS_COP.1_SIGN, FDP_DAU.2). They are also used to check whether the certificate being generated has a unique DN and/or public key before producing the certificate by checking the database. If requested to do this check, and one of the items is not unique, then it will not produce a certificate but will return an error. Otherwise, as well as producing the certificate, it will update the database to reflect DNs and public keys it produces so as to perform this check in future. A CA will not generate a certificate for any PKI entity except a WebRAO if the request has come from a WebRAO (i.e., requests for certificates for PKI entities must come from CAOs to be accepted – all others will be discarded).
CG_Register	**Register Entity** This function is used to generate a certificate request for a PKI entity. This function is performed by the CAO user or the WebRAO user (when issuing certificates for other WebRAOs) if they are a valid and current user of the TSF (FMT_SAE.1, FMT_SMR.1), and may initiate KG_Generate to generate keys. The certificate request process may be done as a face-to-face process or it may involve the export of a PKCS10 certificate request and import of a PKCS7 certificate chain. This function covers certificate generation for the CA and the CAO entities, which occurs during the bootstrap process (initial creation of the PKI)as well as certificate generation associated with the addition of any PKI entity into an existing PKI. The entity may also use the Key Generator to generate a certificate request to become part of the PKI.

Security Function	Description
CG_Request	**Generate Registration Request** This function is used to create a certification request for an end entity, which may include specifying renewals. This may involve importing a private key from the end entity (FDP_ITC.1), or it may involve generating a key pair by initiating KG_Generate. These requests will be signed by the originator to prove that they are a valid and current user of the TSF (FCS_COP.1_SIGN, FDP_DAU.2_CAO, FDP_DAU.2_WebRAO, FMT_SAE.1, FMT_SMR.1). These functions can be used by the CAO user, WebRAO user and end entities (but note that requests generated by end entities are not considered in this ST).
CP_Authenticate	**Authenticate Entity** This function is used to validate the entity trying to establish a communications channel. This is done by verifying the signature on those communications (FCS_COP.1_VERIFY).
CP_Disconnect	**Disconnect Entity** This function is used to logically disconnect an entity from a communications channel. This may be because the entity sent data that could not be successfully verified – i.e., it had been modified in transit, or was not from a valid and current member of the PKI (FDP_ITT.3, FPT_SSP.1).
CP_Origin	**Embed Origin.** This function is used to embed proof of origin information in message, when required. This is done by the hashing (FCS_COP.1_HASH) and then digital signing by the originator of the message, using the originator's private key (FCO_NRO.2, FCS_COP.1_SIGN, FDP_DAU.2, FDP_DAU.2_CAO, FIA_USB.1).
CP_Protect	**Protect Messages** This function is used to ensure messages are protected from either/both disclosures, modification, replay and other attacks (FPT_ITC.1_RA, FPT_ITI.1, FPT_ITT.1_WebRAO, FPT_ITT.1). Integrity will be protected by signing (FCS_COP.1_SIGN, FDP_ITT.1, FDP_ITT.3, FDP_DAU.2, FDP_DAU.2_CAO) and confidentiality will be protected by encryption (FCS_COP.1_ENCRYPT, FPT_ITC.1_RA, FPT_ITI.1, FPT_ITT.1_WebRAO).

Security Function	Description
CP_Verify	**Verify Messages** This function is used to verify the origin, integrity, validity of messages (FPT_ITC.1_RA, FPT_ITI.1, FPT_ITT.1_WebRAO). This is done by checking the digital signature on the message, using the originator's public key (FCO_NRO.2, FDP_ITT.1, FDP_ITT.3) and ensuring that it decrypts correctly (FCS_COP.1_DECRYPT).
CR_Authorize	**Authorize Certificate Revocation Request** This function is used to authorize a certificate revocation request. This can be done by the CAO user or WebRAO user. This action involves checking the signature on the certificate revocation request (FCS_COP.1_VERIFY) and then signing the authorization (FCS_COP.1_SIGN, FDP_DAU.2_CAO, FDP_DAU.2_WebRAO). These functions can only be performed by authorized persons (FIA_UID.1, FIA_UAU.2_CAO, FIA_UID.2_CAO, FIA_UAU.2_WebRAO, FIA_UID.2_WebRAO, FIA_UID.1, FMT_REV.1).
CR_Publish_Rev_Cert_Status	**Publish Revocation and Certificate Status** This function is used to publish or create a list of suspended and revoked certificates, or the status of individual certificates. For lists (which may be created in the database or as a message), this can be done either periodically, via scheduling using records in the CA database, or automatically when a revocation or suspension occurs, or on request. For individual certificates, the status can be published (in messages) by this function on request from the CAO, the CSS, Web Handler or WebRAO. In all cases the indication of status will be signed by the originator (FCS_COP.1_SIGN, FDP_DAU.2, FIA_UAU.2_CAO, FIA_UID.2_CAO, FDP_IFC.1).
CR_Request	**Generate Revocation Request** This function is used to create a revocation, suspension or unsuspension request, which will be signed by the originator (FCS_COP.1_SIGN, FDP_DAU.2_CAO, FDP_DAU.2_WebRAO). This does not cover the case where an end user has generated the request, which is outside the scope of the ST.

Security Function	Description
CR_Revoke	**Revoke Certificate** This function is used to revoke a certificate, by updating the database to show its change in status. This is done by the CA on receipt of a request from an authorized person (FIA_UID.1, FIA_UAU.2_CAO, FIA_UID.2_CAO, FIA_UAU.2_WebRAO, FIA_UID.2_WebRAO, FMT_MOF.1, FMT_MSA.1, FMT_REV.1). Note that when a PKI entity is revoked all of its certificates are revoked at the same time.
CR_Suspend	**Suspend Certificate** This function is used to suspend a certificate, by updating the database to show its change in status. This is done by the CA on request from an authorized person (FIA_UAU.2_CAO, FIA_UID.2_CAO, FIA_UAU.2_WebRAO, FIA_UID.2_WebRAO, FMT_MOF.1, FMT_MSA.1, FMT_REV.1). Note that when a PKI entity is suspended all of its certificates are suspended at the same time.
CR_Unsuspend	**Unsuspended Certificate** This function is used to unsuspend a suspended certificate, by updating the database to show its change in status. A revoked certificate cannot be unrevoked. This is done by the CA on request from an authorized person (FIA_UAU.2_CAO, FIA_UID.2_CAO, FIA_UAU.2_WebRAO, FIA_UID.2_WebRAO, FMT_MOF.1, FMT_MSA.1). Note that when a PKI entity is unsuspended then all of its certificates will be unsuspended.
DP_Export	**Protect Data Exported** This function is to ensure that data is protected when exported (if required) (FDP_IFC.1, FPT_ITC.1_RA, FPT_ITI.1, FPT_ITT.1_WebRAO, FPT_ITT.1) from modification or disclosure. Integrity will be protected by signing (FCS_COP.1_SIGN) and confidentiality will be protected by encryption (FCS_COP.1_ENCRYPT)
DP_KeyExport	**Export Private Key** These functions are a special case of the above. The Keys are only exported to authorized end entities and are protected from disclosure and modification (FDP_IFC.1, FPT_ITC.1_RA, FPT_ITI.1, FPT_ITT.1_WebRAO, FPT_ITT.1). Integrity will be protected by signing (FCS_COP.1_SIGN) and confidentiality will be protected by encryption (FCS_COP.1_ENCRYPT) with a key generated for the purpose (FCS_CKM.1).

Security Function	Description
DP_Store	**Protect Data Storage** These functions are used to protect the data stored by the TOE in the database. Integrity will be protected by signing (FCS_COP.1_SIGN, FDP_ITT.1, FDP_ITT.3) and confidentiality will be protected by encryption (FCS_COP.1_ENCRYPT).
DP_Verify	**Verify Data Store.** These functions are to verify the integrity and to ensure only data that has been stored by authorized users is used by the TOE (FPT_ITC.1_RA, FPT_ITI.1, FPT_ITT.1_WebRAO) when retrieved from the database. This is done by verifying the hash (FCS_COP.1_HASH) and signature (FCS_COP.1_VERIFY, FDP_ITT.1, FDP_ITT.3) on the data and ensuring that it decrypts correctly (FCS_COP.1_DECRYPT).
GG_Create	**Create Authorization Group** These functions are used to create a group of PKI entities associated by a defined criteria based on their certificate DN or partial DN (FIA_USB.1). Groups can then be used to assign authorization or registration paths to policies. Only authorized persons are able to use the TOE to perform this function (FDP_ACC.1, FDP_ACF.1, FDP_IFF.1, FIA_UAU.2_CAO, FIA_UID.2_CAO, FIA_UAU.2_WebRAO, FIA_UID.2_WebRAO, FMT_MOF.1, FMT_MSA.1, FMT_MTD.1). Authorization group information is stored in the CA database.
GG_Modify	**Modify Group** These functions are used to modify a group of PKI entities associated by a defined criteria based on their certificate DN or partial DN. Only authorized persons are able to use the TOE to perform this function (FDP_ACC.1, FDP_ACF.1, FDP_IFF.1, FIA_UAU.2_CAO, FIA_UID.2_CAO, FIA_UAU.2_WebRAO, FIA_UID.2_WebRAO, FIA_USB.1, FMT_MTD.1).

Security Function	Description
GG_Retire	**Retire Group** These functions are used to retire a group of PKI entities associated by a defined criteria based on their certificate DN or partial DN. Groups cannot be deleted. Only authorized persons are able to use the TOE to perform this function (FDP_ACC.1, FDP_ACF.1, FDP_IFF.1, FIA_UAU.2_CAO, FIA_UID.2_CAO, FIA_UAU.2_WebRAO, FIA_UID.2_WebRAO, FMT_MTD.1, FMT_REV.1), and the function results in the database being updated.
IA_Authenticate	**Authenticate Entity** This function is executed after IA_Identify has identified the user and after PP_PKIVerify retrieved the PKI and verified its signature, and involves checking the PKI definition to determine if the entity is a valid and current member of the PKI community and if so, what permissions they have. The function is passed a certificate, and checks that: • It is associated with a member of the PKI community, and not retired • The current date/time falls within the validity period of the certificate • The certificate has the correct extensions for the function it is being used for If these checks are passed successfully, it obtains a list of the user's permissions from the PKI, which it uses to set the options available on the relevant screens. The identity, once authenticated, may be used in data generated by the TOE e.g., audit records (FAU_GEN.2), or to control access to TOE functionality and data (FAU_SAR.1, FAU_SAR.2, FAU_SAR.3 and FDP_ACC.1, FDP_ACF.1, FDP_IFF.1, FIA_UAU.1, FIA_UAU.2_CAO, FIA_UID.2_CAO, FIA_UAU.2_WebRAO, FIA_UID.2_WebRAO, FIA_UID.1, FMT_SAE.1, FMT_SMR.1).

Security Function	Description
IA_Identify	**Identify Entity** This function is used to identify a member of the PKI community. This is done by allowing the user to choose a key file and to enter their passphrase/PIN and then using this to attempt to open the key file (FCS_CKM.3). If it cannot be opened then an error is returned to the user. This function is not relevant to the Key Generator or Token Manager. The identity, once identified and authenticated, may be used in data generated by the TOE e.g., audit records (FAU_GEN.2), or to control access to TOE functionality and data (FAU_SAR.1, FAU_SAR.2, FAU_SAR.3 and FDP_ACC.1, FDP_ACF.1, FDP_IFF.1, FIA_UAU.2_CAO, FIA_UID.2_CAO, FIA_UAU.2_WebRAO, FIA_UID.2_WebRAO).
KG_Destroy	**Destroy Key** These functions are used to securely destroy key material, so that it cannot be recovered. This is done by the TOE (FCS_CKM.4, FDP_RIP.1) or via P11 interface to a Smart card or HSM. The ST requires that the P11 device is trusted and performs the appropriate key destruction function (FCS_CKM.4) – refer to OE.HardwareFunctions.
KG_Export	**Export Key Pair** These functions are used to export a key based on the current key policy (FDP_IFC.1). If this policy permits it, this can be done by any PKI entity or by the separate Key Gen Utility (FCS_CKM.2_PublicKey, FCS_CKM.2) or via the interface to a Smart card or HSM. The key will be encrypted using FCS_COP.1_ENCRYPT before being exported.
KG_Generate	**Generate Key Pair** These functions are used to specify a passphrase and generate a key based on the current key policy (FIA_SOS.1, FCS_CKM.1). Some control is exerted over the passphrase chosen to ensure that it is secure (FMT_MSA.2). This can be done using the CAO, WebRAO or by the Key Gen Utility.

Security Function	Description
KG_Split	**Split Key** These functions are used to split access to a key based on the user input. This operation can physically divide the key between more than one device if the key is in a PSE file (FCS_CKM.2_PublicKey, FIA_SOS.1). This can be initiated using the CAO, Token Manager or the Key Gen Utility.
KG_Update	**Update Key** These functions are used to update key properties, such as passphrase, based on user selection. They can also be used to physically move a key from one device to another (FCS_CKM.2_PublicKey, FIA_SOS.1). Some control is exerted over the passphrase chosen to ensure that it is secure (FMT_MSA.2). This can be done using the Token Manager.
PG_PolicyConfigure	**Configure Registration Policy.** These functions are used to create registration policies and assign registration policies to users, user groups, PHs and to create an authorization path for that policy. These functions can only be performed by authorized persons (FIA_UID.1, FIA_UAU.2_CAO, FIA_UID.2_CAO, FIA_UID.1, FMT_MOF.1, FMT_MSA.1, FMT_MTD.1, FMT_SAE.1, FMT_SMR.1), and some control is exerted over the choices available to ensure that they are secure (FMT_MSA.2). These functions allow an administrator to set the limits for certificate validity for certificates using this policy (FMT_MTD.2). All of these functions result in updating the database to save the results.
PG_PolicyDelete	**Delete Registration Policy.** These functions are used by authorized persons to delete a registration policy from the database (FIA_UAU.2_CAO, FIA_UID.2_CAO). Policies that have been used, or assigned, cannot be deleted, only retired (FMT_MSA.2).
PG_PolicyExport	**Export Registration Policy.** This set of functions is used to either export a policy to another PKI entity (signed, using FCS_COP.1_SIGN) or to save it to disk in order to create a backup. These functions are used to export the registration policy. (Note that signed policies are verified on receipt by a PKI entity using the function CP_Verify.)

Security Function	Description
PG_PolicyImport	**Import Registration Policy.** These functions are used to import a registration policy from a file. This function ensures that the policy is a valid policy, but the policy need not be created by an authorized PKI entity. These functions can only be performed by authorized persons (FIA_UID.1, FIA_UAU.2_CAO, FIA_UID.2_CAO).
PG_PolicyRetire	**Retire Registration Policy.** These functions are used by authorized persons to retire a registration policy by marking it as such in the database (FIA_UAU.2_CAO, FIA_UID.2_CAO, FMT_MTD.1). Policies that have been used, or assigned, cannot be deleted, only retired (FMT_MSA.2).
PP_EntityDelete	**Delete Entity** This set of functions is used to delete an entity from a PKI. This will not include end entities. Only authorized persons are able to use the TOE to perform this function (FDP_ACC.1, FDP_ACF.1, FDP_IFF.1, FIA_UAU.2_CAO, FIA_UID.2_CAO, FMT_MTD.1, FMT_REV.1).
PP_EntityModify	**Modify Entity** This set of functions is used to create and modify an entity in a PKI, resulting in its definition being stored or updated in the database. This will not include end entities. For other entities, it includes specifying configuration parameters such as key and certificate attributes and port, machine name, and timeout specifications and also includes working on the renewal of certificates and modifying permissions of entities (FIA_ATD.1, FIA_USB.1). This operation may include signing communications (FCS_COP.1_SIGN). Only authorized persons are able to use the TOE to perform this function (FDP_ACC.1, FDP_ACF.1, FDP_IFF.1, FIA_UAU.1, FIA_UID.1, FIA_UAU.2_CAO, FIA_UID.2_CAO, FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1), and some control is exerted over the configuration choices available to ensure that they are secure (FIA_SOS.1 and FMT_MSA.2).

Security Function	Description
PP_EntityRegister	**Register Entity** This set of functions is used to register an entity in a PKI, which includes creating users and administrators and storing information about them (FIA_ATD.1), but will not include registering end entities. Only authorized persons are able to use the TOE to perform this function (FDP_ACC.1, FDP_ACF.1, FDP_IFF.1, FIA_UAU.1, FIA_UAU.2_CAO, FIA_UID.2_CAO, FIA_UID.1, FMT_MTD.1), and some control is exerted over the configuration choices available to ensure that they are secure (FIA_SOS.1 and FMT_MSA.2). Entities will be given a default set of permissions on creation – this default set can be changed by an authorized administrator (FMT_MSA.3). If an attempt is made to register an entity with a certificate validity that is outside of the limits that have been set by an administrator, then this attempt will be rejected (FMT_MTD.2).
PP_PKICreate	**Create PKI** This set of functions is used to create a PKI, which will be stored in the CA database. The PKI at a minimum includes a CA and a CAO. Only authorized persons are able to use the TOE to perform this function (FDP_ACC.1, FDP_ACF.1, FDP_IFF.1, FIA_UAU.1, FIA_UID.1).
PP_PKIExport	**Export PKI** This set of functions is used to export the description of the PKI to another PKI entity (FDP_IFC.1).
PP_PKIModify	**Modify PKI** This set of functions is used to modify a PKI. Modifications include adding, deleting or modifying an entity, specifying renewals and permissions, and editing or the entities configuration parameters such as port, machine name and timeouts. Only authorized persons are able to use the TOE to perform this function (FDP_ACC.1, FDP_ACF.1, FDP_IFF.1).
PP_PKIProtect	**Protect PKI** These functions are used to protect the PKI from unauthorized modification. Signing the PKI with the CA key performs this (FCS_COP.1_SIGN, FDP_DAU.2, FDP_DAU.2_CAO). Only authorized persons are able to use the TOE to perform this function (FDP_ACC.1, FDP_ACF.1, FDP_IFF.1).

Security Function	Description
PP_PKIVerify	**Verify PKI** These functions are used to obtain the PKI and verify its integrity. The PKI will be either retrieved from a database or received in a communication (or both), along with its signature. The RA uses the PKI Version Number in its communication with the CA to ensure that it has the latest version of the PKI. Checking the hash (FCS_COP.1_HASH) and signature verification (FCS_COP.1_VERIFY) are used to verify the integrity of the PKI. Note that this function also provides the recipient with the latest CRL, ARL, and CA certificate.

Table 6-1 – IT Security Functions

6.2.2 Strength of Functions

Table 6.1 identifies all IT security functions that are realized by probabilistic or permutational mechanisms that are cryptographic in nature (i.e., those mapped to cryptographic SFRs). The assessment of the algorithmic strength used by these functions is out of scope of the evaluation, being assessed by the National Authority.

However one mechanism does require a strength of function assessment. This is the mechanism that protects the privacy and integrity of the ".pse" file. This is implemented by the functions IA_Identify, KG_Generate, KG_Split, KG_Update and KG_Export, and has a strength of function of SOF-Basic.

6.3 Assurance Measures

This section specifies the assurance measures of the TOE that are claimed to satisfy the stated assurance requirements. The assurance measures are traced to the assurance requirements so that it can be seen which measures contribute to the satisfaction of which requirements. This is done with reference to the appropriate documentation.

The assurance measures listed in Table 6.2 are required to be successfully evaluated in order for the TOE to be successfully certified.

Assurance Component	Assurance Measure	Justification that the assurance measure meets the TOE security assurance requirement
ASE_DES.1	Security Target document, i.e., this document	The security target contains a TOE description which contains relevant information to aid the understanding of the purpose of the TOE and its functionality which is complete and consistent.

Assurance Component	Assurance Measure	Justification that the assurance measure meets the TOE security assurance requirement
ASE_ENV.1	Security Target document, i.e., this document	The security target contains a statement of the TOE security environment which provides a clear and consistent definition of the security problem that the TOE and its environment is intended to address.
ASE_INT.1	Security Target document, i.e., this document	The security target contains an introduction which is complete and consistent with all other parts of the document and correctly identifies the ST.
ASE_OBJ.1	Security Target document, i.e., this document	The security target describes the security objectives completely and consistently, and these security objectives counter the identified threats, achieve the identified organizational security policies and are consistent with the stated assumptions.
ASE_PPC.1	Security Target document, i.e., this document	The security target makes no claims of protection profile conformance.
ASE_REQ.1	Security Target document, i.e., this document	The security target describes the TOE security requirements (both the TOE security functional requirements and the TOE security assurance requirements). The security requirements for the IT environment are described completely and consistently, and these provide an adequate basis for development of a TOE that will achieve its security objectives.
ASE_SRE.1	Security Target document, i.e., this document	The security target contains no security functional requirements or security assurance requirements that are stated without reference to the CC.
ASE_TSS.1	Security Target document, i.e., this document	The security target contains a TOE summary specification, which provides a clear and consistent high-level definition of the security functions and assurance measures, and demonstrates that these satisfy the specified TOE security requirements.
ACM_AUT.1	Configuration Management Plan as supplied to evaluators	As described in the configuration management plan, changes to the implementation representation are controlled with the support of the automated tool “Perforce”, making the CM system less susceptible to human error or negligence.
ACM_CAP.4	Configuration Management Plan as supplied to evaluators and Configuration Item List as supplied to evaluators	Configuration Management Plan and Configuration Item List clearly identify the TOE and its associated configuration items, and demonstrate that the ability to modify these items is properly controlled.

Assurance Component	Assurance Measure	Justification that the assurance measure meets the TOE security assurance requirement
ACM_SCP.2	Configuration Item List as supplied to evaluators	The Configuration Item List will demonstrate that the developer performs configuration management on the TOE implementation representation, design, tests, user and administrator guidance, the CM documentation and security flaws.
ADO_DEL.2	Delivery Procedures as supplied to evaluators	The Delivery Procedures describe all procedures used to maintain security and to detect modification or substitution of the TOE when distributing the TOE to the user's site.
ADO_IGS.1	Guidance Documents as supplied to evaluators	The Guidance Documents document the procedures and steps for the secure installation, generation, and startup of the TOE and result in a secure configuration.
ADV_FSP.2	Functional Specification as supplied to evaluators	The Functional Specification provides an adequate description of all security functions of the TOE and demonstrates that the security functions provided by the TOE are sufficient to satisfy the security functional requirements of the ST.
ADV_HLD.2	High-Level Design as supplied to evaluators	The High-Level Design provides a description of the TSF in terms of major structural units (i.e., subsystems), provides a description of the interfaces to these structural units, and is a correct realization of the functional specification.
ADV_IMP.1	Implementation Representation Sample as supplied to evaluators	The Implementation Representation is sufficient to satisfy the functional requirements of the ST and is a correct realization of the low-level design.
ADV_LLD.1	Low-Level Design as supplied to evaluators	The Low-Level Design satisfies the functional requirements of the ST, and is a correct and effective refinement of the high-level design.
ADV_RCR.1	Analysis of Correspondence as supplied to evaluators	The Analysis of Correspondence demonstrates that the developer has correctly and completely implemented the requirements of the ST, functional specification, high-level design and low-level design in the implementation representation.
ADV_SPM.1	Security Target Document as supplied to evaluators	The security policy model in the security target clearly and consistently describes the rules and characteristics of the security policies. This description corresponds with the description of security functions in the functional specification.
AGD_ADM.1	Guidance Documents as supplied to evaluators	The administrator guidance (part of the Guidance Documents) describes how to administer the TOE in a secure manner.

Assurance Component	**Assurance Measure**	**Justification that the assurance measure meets the TOE security assurance requirement**
AGD_USR.1	Guidance Documents as supplied to evaluators	The user guidance (i.e., The WebRAO guidance document, which forms part of the Guidance Documents) describes the security functions and interfaces provided by the TSF and provides instructions and guidelines for the secure use of the TOE.
ALC_DVS.1	Development Security Documentation as supplied to evaluators	The Development Security Documentation demonstrates that the developer's security controls on the development environment are adequate to provide the confidentiality and integrity of the TOE design and implementation that is necessary to ensure that secure operation of the TOE is not compromised.
ALC_FLR.2	Flaw Remediation Procedures Documentation as supplied to evaluators	The Flaw Remediation Procedures Documentation describes all flaw remediation procedures including the procedures for accepting and acting on all reports of flaws and requests to correct those flaws, tracking security flaws, describing the flaws, and recording the status of finding a correction to that flaw. It describes the means by which reports and enquires of suspected security flaws are reported and managed so that any reported flaws are corrected and the correction issued to TOE users.
ALC_LCD.1	Life-Cycle Definition Documentation as supplied to evaluators	The Life-Cycle Definition Documentation demonstrates that the developer has used a documented model of the TOE life-cycle.
ALC_TAT.1	Development Tools and Techniques Documentation as supplied to evaluators	The Development Tools and Techniques Documentation demonstrates that the developer has used well-defined development tools (e.g., programming languages or computer-aided design (CAD) systems) that yield consistent and predictable results.
ATE_COV.2	Analysis of Test Coverage (Test Documentation) as supplied to evaluators	The Analysis of Test Coverage (Test Documentation) shows that the testing is sufficient to establish that the TSF has been systematically tested against the functional specification.
ATE_DPT.1	Analysis of Depth of Testing (Test Documentation) as supplied to evaluators	The Analysis of Depth of Testing (Test Documentation) shows that the developer has tested the TSF against its high-level design.
ATE_FUN.1	Test documentation as supplied to evaluators	The test documentation demonstrates that security functions perform as specified.

Assurance Component	Assurance Measure	Justification that the assurance measure meets the TOE security assurance requirement
ATE_IND.2	Evaluator action	Evaluator action
AVA_MSU.2	Misuse Analysis Document as supplied to evaluators	The Misuse Analysis Document demonstrates that the guidance is neither misleading, unreasonable or conflicting, that secure procedures for all modes of operation have been addressed, and that use of the guidance will facilitate prevention and detection of insecure TOE states.
AVA_SOF.1	Strength of Function Analysis as supplied to evaluators	The Strength of Function Analysis will demonstrate that SOF claims have been made in the ST for all probabilistic or permutational mechanisms and that these claims supported by a correct analysis.
AVA_VLA.2	Vulnerability Analysis as supplied to evaluators	The Vulnerability Analysis will show that the TOE, in its intended environment, has no vulnerabilities exploitable by attackers possessing low attack potential.

Table 6-2 – Assurance Measures

7. Protection Profile Claims

This section contains the Protection Profile conformance claim statements.

7.1 Protection Profile Reference

No Protection Profile conformance claims are made.

7.2 Protection Profile Refinements

No Protection Profile conformance claims are made.

7.3 Protection Profile Additions

No Protection Profile conformance claims are made.

8. Rationale

8.1 Introduction

8.1.1 This section presents evidence that supports the claims that the Security Target is a complete and cohesive set of requirements, that a conformant TOE would provide an effective set of IT security countermeasures within the security environment, and that the TOE summary specification addresses the requirements. The rationale also demonstrates that any protection profile claims are valid.

8.2 Security Objectives Rationale

8.2.1 This section demonstrates that the stated security objectives are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them.

8.2.2 Table 8.1 below maps the threats, assumptions and organization security policies against the TOE security objectives that are intended to address them. Table 8.2 presents a similar mapping for the Environmental security objectives identified in Section 4.3. These tables show that each security objective covers at least one threat, assumption or policy and that each threat, assumption and policy (identified in Chapter 3) is covered by at least one security objective. All security objectives are thus shown to be necessary.

Security Objective	Threat/Assumption/Policy
O.AuditLogs	T.LossOfAuditData
	T.AdminErrCommit
	T.AdminErrOmit
	P.RoleSeparation
	P.Guidance
O.DisposalOfAuthenticationData	P.DisposalOfAuthenticationData
	T.PKIKeyCompromise
O.IndividualAccountability	T.AdminErrCommit
	T.AdminErrOmit
	T.NonRepudiation
	P.Accountability
	P.QualifiedTOEUsers
	P.RoleSeparation
O.Installation	P.Guidance
	P.QualifiedTOEUsers
	T.MaliciousCode
	P.RoleSeparation
O.CPS	T.AdminErrOmit

Security Objective	Threat/Assumption/Policy
O.CryptographicFunctions	T.Cryptography
	T.ExportKeyMaterial
	P.Cryptography
O.NonRepudiation	T.AdminErrCommit
	T.NonRepudiation
	T.MaliciousCode
	P.Accountability
O.Audit	T.LossOfAuditData
	T.AdminErrCommit
	T.AdminErrOmit
	T.NonRepudiation
	T.UnauthorizedConfigurationChange
	P.RoleSeparation
	P.Guidance
O.DataImportExport	T.ExportKeyMaterial
	T.MessageModification
O.FlawUnknownToUser	T.DevFlawedCode
	T.FlawDiscovery
O.Guidance	P.Guidance
O.IntegrityTOEData	T.MessageModification
	T.UnAuthorizedConfigurationChange
	T.PKIKeyCompromise
	T.MaliciousCode
	T.LossOfAuditData
O.IntegrityUserData	T.MessageModification
O.ConfidentialityTOEData	T.PKIKeyCompromise
	T.MessageModification
	T.ExportKeyMaterial
O.ConfidentialityUserData	T.ExportKeyMaterial
	T.PKIKeyCompromise
O.LifeCycleSecurity	T.DevFlawedCode
	T.FlawDiscovery
O.MaintainUserAttributes	T.UnAuthorizedConfigurationChange
	P.Accountability
	P.RoleSeparation
O.ProtectAuditRecords	T.PKIKeyCompromise
	T.LossOfAuditData
O.ProtectConfiguration	T.UnAuthorizedConfigurationChange T.UnTrustedEntity
O.ProvideEvidenceOfOrigin	T.NonRepudiation
O.Passphrase	T.NonRepudiation
	T.PKIKeyCompromise
	P.Guidance
O.ControlUnknownOriginComms	T.UnTrustedEntity
O.MaliciousCodeNotExecuted	T.MaliciousCode
O.FlawRemediation	P.Guidance
	T.DevFlawedCode
	T.FlawDiscovery
	P.ApplyFlawRemediation

Table 8-1 – TOE Security Objectives

Security Objective	Threat/Assumption/Policy
OE.BackupStorageRestoration	A.DisposalOfAuthenticationData.
	T.PKIKeyCompromise
	P.Guidance

Security Objective	Threat/Assumption/Policy
OE.Audit	T.LossOfAuditData
	A.AuditReview
	P.Guidance
OE.TamperNotify	P.Cryptography
	T.PKIKeyCompromise
	P.HardwareCryptography
	P.Guidance
OE.Cryptography	P.HardwareCryptography
	T.ExportKeyMaterial
	P.Cryptography
	T.Cryptography
OE.HardwareFunctions	P.HardwareCryptography
	T.ExportKeyMaterial
	T.Cryptography
	P.Cryptography
OE.CPS	A.CPS
OE.CompetentPKIUsers	A.CompetentPKIUsers
OE.MaliciousCodeNotExecuted	A.MaliciousCodeNotExecuted
OE.SecureInstallation	A.SecureInstallation
OE.Guidance	A.Guidance
OE.FlawRemediation	P.ApplyFlawRemediation
	T.FlawDiscovery
OE.Timesource	A.Timesource
OE.PassphrasePIN	T.PKIKeyCompromise
OE.Keys	T.PKIKeyCompromise
OE.Physical	A.PhysicalProtection
OE.DisposalOfAuthenticationData	A.DisposalOfAuthenticationData
	P.DisposalOfAuthenticationData
OE.Connectivity	A.CommunicationsProtection
	T.MessageModification

Table 8-2 – Environmental Security Objectives

8.2.3 The following sections demonstrate that the security objectives are sufficient to meet the security needs of the TOE. Each threat, assumption and policy is considered in turn.

8.2.4 Threats

T.AdminErrCommit	O.AuditLogs ensures that the audit logs created by the TOE are reviewed by an auditor. O.Audit ensures that the TOE records security related events, with evidence to allow the integrity of the audit logs to be verified. O.IndividualAccountability makes it more difficult for a user of the TOE to intentionally or unintentionally undermine the TOE's security objectives. O.NonRepudiation, by embedding the evidence of origin into TOE messages and/or other actions performed by users, makes it hard for someone to falsely argue that they

	did not perform an action.
T.AdminErrOmit	O.AuditLogs ensures that the audit logs created by the TOE are reviewed by an auditor. O.Audit ensures that the TOE records security related events, with evidence to allow the integrity of the audit logs to be verified. O.IndividualAccountability makes it more difficult for a user of the TOE to intentionally or unintentionally undermine the TOE's security objectives. O.CPS ensures that administrators and users of the TOE know their responsibilities when issuing certificates.
T.PKIKeyCompromise	O.DisposalOfAuthenticationData ensures that, when authentication data is no longer valid or required, the ability to use it can be withdrawn. O.ConfidentialityUserData ensures that secret user data such as secret keys will remain secret. O.Passphrase ensures that passphrases chosen meet specified complexity and length requirements and which makes them more difficult to break. O.IntegrityTOEData ensures that the data that is relevant to the secure operation of the TOE can only be changed by authorized persons. OE.BackupStorageRestoration ensures that procedures and facilities exist outside the TOE that allow the TOE owners to recover the TOE from any disaster while ensuring system integrity and the confidentiality private key material. OE.Keys secure storage of all keys used to operate or administer the TOE helps to prevent their compromise. OE.TamperNotify ensures that, if an HSM is used to store key material, that it will provide notification if someone attempts to tamper with it. O.ConfidentialityTOEData ensures that secret TOE data such as secret keys will remain secret. O.ProtectAuditRecords assists by ensuring that the TOE's audit trail is reliable. OE.PassphrasePIN ensures that secure choices will be made when specifying both passphrases and PINs, making them harder for an attacker to guess.

T.ExportKeyMaterial	O.ConfidentialityUserData ensures that secret user data such as secret keys will remain secret. O.ConfidentialityTOEData ensures that secret TOE data such as secret keys will remain secret. O.CryptographicFunctions ensures that correct algorithms are used, so as to provide reliable protection when required. OE.Cryptography ensures that correct algorithms are used, so as to provide reliable protection when required. OE.HardwareFunctions ensures that any HSMs used are able to perform the functions required reliably. O.DataImportExport ensures that keys are cryptographically protected when exported.
T.Cryptography	O.CryptographicFunctions ensures that correct algorithms are used, so as to provide reliable protection when required. OE.Cryptography ensures that correct algorithms are used, so as to provide reliable protection when required. OE.HardwareFunctions ensures that any HSMs used are able to perform the functions required reliably.
T.NonRepudiation	O.IndividualAccountability makes it more difficult for a user of the TOE to intentionally or unintentionally undermine the TOE's security objectives. O.NonRepudiation, by embedding the evidence of origin into TOE messages or and other actions performed by users makes it hard for someone to falsely argue that they did not perform an action. O.ProvideEvidenceOfOrigin ensures that the originator of messages can be established from the message itself. O.Passphrase ensures that passphrases chosen meet specified complexity and length requirements and which makes them more difficult to break. O.Audit ensures that the TOE records security related events, with evidence to allow the integrity of the audit logs to be verified.
T.DevFlawedCode	O.FlawUnknownToUser ensures that, if a security flaw is discovered, users can be made aware of the impact and any corrective action that they should undertake. O.LifecycleSecurity assists in preventing code

	with security flaws from being developed by using defined tools and techniques that are designed to prevent this. O.FlawRemediation ensures that there is a way to effectively address any flaws found.
T.FlawDiscovery	O.FlawUnknownToUser ensures that, if a security flaw is discovered, users can be made aware of the impact and any corrective action that they should undertake. O.FlawRemediation ensures that there is a way to effectively address any flaws found. O.LifeCycleSecurity assists in preventing code with security flaws from being developed by using defined tools and techniques that are designed to prevent this. OE.FlawRemediation ensures that any flaw remediation corrective action will be implemented by those responsible for the TOE.
T.LossOfAuditData	O.AuditLogs ensures that the audit logs created by the TOE are reviewed by an auditor. O.Audit ensures that the TOE records security related events, with evidence to allow the integrity of the audit logs to be verified. O.IntegrityTOEData ensures that the data that is relevant to the secure operation of the TOE can only be changed by authorized persons. O.ProtectAuditRecords assists by ensuring that the TOE's audit trail is reliable. OE.Audit ensures that no audit log records are lost due to lack of space.
T.MaliciousCode	O.IntegrityTOEData ensures that the data that is relevant to the secure operation of the TOE can only be changed by authorized persons. O.Installation ensures that the correct procedures will be followed at the time of installation to provide a secure TOE. O.NonRepudiation, by embedding the evidence of origin into TOE messages and/or other actions performed by users, makes it hard for someone to falsely argue that they did not perform an action. O.MaliciousCodeNotExecuted ensures that TOE users will not execute malicious code on the same platform as the TOE.
T.UnAuthorizedConfigurationChange	O.Audit ensures that the TOE records security related events, with evidence to allow the integrity of the audit logs to be verified. O.IntegrityTOEData ensures that the data that

	is relevant to the secure operation of the TOE can only be changed by authorized persons. O.MaintainUserAttributes ensures that the TOE correctly maintains user attributes associated with user identities. O.ProtectConfiguration provides a mechanism to protect the PKI configuration from unauthorized changes.
T.MessageModification	O.DataImportExport ensures that messages are cryptographically protected. O.IntegrityTOEData ensures that the data that is relevant to the secure operation of the TOE can only be changed by authorized persons. O.IntegrityUserData provides cryptographic measures to ensure the integrity of user data. O.ConfidentialityTOEData ensures that secret TOE data such as secret keys will remain secret. OE.Connectivity ensures that communications channels are logically and physically protected from unauthorized access.
T.UnTrustedEntity	O.ProtectConfiguration provides a mechanism to protect the PKI configuration from unauthorized changes. O.ControlUnknownOriginComms ensures that the TOE components only accept communications from known sources.

Table 8-3 – Threats

8.2.5 Assumptions

A.DisposalOfAuthenticationData	OE.BackupStorageRestoration ensures that procedures and facilities exist outside the TOE that allow the TOE owners to recover the TOE from any disaster while ensuring system integrity and the confidentiality private key material. OE.DisposalOfAuthenticationData makes the TOE owners responsible to ensure that this assumption is upheld.
A.AuditReview	OE.Audit ensures that the TOE owners are responsible to uphold the assumption.
A.CPS	OE.CPS ensures that the TOE owners are responsible to uphold the assumption.
A.CompetentPKIUsers	OE.CompetentPKIUsers ensures that the TOE owners are responsible to uphold the assumption.

A.MaliciousCodeNotExecuted	OE.MaliciousCodeNotExecuted ensures that the TOE owners are responsible to uphold the assumption.
A.SecureInstallation	OE.SecureInstallation ensures that the TOE owners are responsible to uphold the assumption.
A.Guidance	OE.Guidance ensures that the TOE owners are responsible to uphold the assumption.
A.CommunicationsProtection	OE.Connectivity ensures that the TOE owners are responsible to uphold the assumption.
A.Timesource	OE.Timesource ensures that the TOE owners are responsible to uphold the assumption.
A.PhysicalProtection	OE.Physical ensures that the TOE owners are responsible to uphold the assumption.

Table 8-4 – Assumptions

8.2.6 Organization Security Policies

P.Accountability	O.IndividualAccountability makes it more difficult for a user of the TOE to intentionally or unintentionally undermine the TOE’s security objectives. O.MaintainUserAttributes ensures that the TOE correctly maintains user attributes associated with user identities. O.NonRepudiation, by embedding the evidence of origin into TOE messages and/or other actions performed by users, makes it hard for someone to falsely argue that they did not perform an action.
P.DisposalOfAuthenticationData	O.DisposalOfAuthenticationData ensures that, when authentication data is no longer valid or required, the ability to use it can be withdrawn. OE.DisposalOfAuthenticationData makes the TOE owners responsible to ensure that this assumption is upheld.
P.Guidance	O.AuditLogs ensures that the audit logs created by the TOE are reviewed by an auditor. O.Installation ensures that the correct procedures will be followed at the time of installation to provide a secure TOE. O.Audit ensures that the TOE records security related events, with evidence to allow the

	integrity of the audit logs to be verified. O.Guidance provides enough information so that users and administrators can use the TOE securely. O.FlawRemediation ensures that there is a way to effectively address any flaws found. OE.BackupStorageRestoration ensures that procedures and facilities exist outside the TOE that allow the TOE owners to recover the TOE from any disaster while ensuring system integrity and the confidentiality private key material. OE.Audit ensures that the TOE records security related events, with evidence to allow the integrity of the audit logs to be verified. O.Passphrase ensures that passphrases chosen meet specified complexity and length requirements and which makes them more difficult to break. OE.TamperNotify ensures that, if an HSM is used to store key material, that it will provide notification if someone attempts to tamper with it.
P.QualifiedTOEUsers	O.IndividualAccountability makes it more difficult for a user of the TOE to intentionally or unintentionally undermine the TOE's security objectives. O.Installation ensures that the correct procedures will be followed at the time of installation to provide a secure TOE.
P.RoleSeparation	O.AuditLogs ensures that the audit logs created by the TOE are reviewed by an auditor. O.IndividualAccountability makes it more difficult for a user of the TOE to intentionally or unintentionally undermine the TOE's security objectives. O.Installation ensures that the correct procedures will be followed at the time of installation to provide a secure TOE. O.Audit ensures that the TOE records security related events, with evidence to allow the integrity of the audit logs to be verified. O.MaintainUserAttributes ensures that the TOE correctly maintains user attributes associated

	with user identities.
P.ApplyFlawRemediation	O.FlawRemediation ensures that there is a way to effectively address any flaws found. OE.FlawRemediation ensures that any flaw remediation corrective action will be implemented by those responsible for the TOE.
P.Cryptography	O.CryptographicFunctions ensures that correct algorithms are used, so as to provide reliable protection when required. OE.Cryptography ensures that correct algorithms are used, so as to provide reliable protection when required. OE.HardwareFunctions ensures that any HSMs used are able to perform the functions required reliably. OE.TamperNotify ensures that, if an HSM is used to store key material, that it will provide notification if someone attempts to tamper with it.
P.HardwareCryptography	OE.TamperNotify ensures that, if an HSM is used to store key material, that it will provide notification if someone attempts to tamper with it. OE.Cryptography ensures that correct algorithms are used, so as to provide reliable protection when required. OE.HardwareFunctions ensures that any HSMs used are able to perform the functions required reliably.

Table 8-5 – Organization Security Policies

8.3 Security Requirements Rationale

8.3.1 This section demonstrates that the set of security requirements for the TOE is suitable to meet and is traceable to the security objectives. Section 5.4 of the ST provides a tracing of security objectives for the IT environment to security requirements for the IT environment, with a justification for each one that the security requirements for the IT environment are suitable to meet that security objective for the IT environment.

8.3.2 It demonstrates the following:

a) That the combination of the individual functional and assurance requirements components for the TOE and its IT environment together meet the stated security objectives

b) That the set of security requirements together form a mutually supportive and internally consistent whole

c) That the choice of security requirements is justified (including non-satisfaction of dependencies)

d) That the selected strength of function level for the Security Target, together with any explicit strength of function claim, is consistent with the security objectives for the TOE.

8.3.3 Security Functional Requirements Rationale

8.3.3.1 The following table maps each TOE security objective against the corresponding security functional components. It demonstrates that each security objective for the TOE is addressed by at least one SFR and that each SFR addresses at least one security objective.

8.3.3.2 For each security objective, informal arguments are provided as to why the identified SFRs are sufficient to satisfy the objective.

O.AuditLogs	FAU_GEN.1 Identifies Auditable events for which the audit records should be generates and specifies the information to be provided in the audit records FAU_GEN.2 Associates each auditable event with the users that caused the event FAU_SAR.1 Provides that Authorized user the capability to read all or a selection of audit records from the audit trail in a manner that the user can interpret. FAU_SAR.2 Restricts the reading of the audit record to an Authorized user. FAU_SAR.3 Provides an authorized user the ability to sort, query and filter the audit records before displaying the log. FMT_MOF.1 This function supports this objective by ensuring that security functions can only be performed by authorized persons. FDP_ACC.1 and FDP_ACF.1 describe the access control policy that is enforced by the TOE to control who can perform controlled operations on specified objects such as the audit records. FAU_STG.1 Allows only an authorized user the ability to archive audit records, and provides a mechanism to detect modification to the audit record. FCS_COP.1_SIGN This function is used to sign the audit record and a representation of the entire log in order to allow for the detection of deletion and modification from the audit trail.

	FCS_COP.1_VERIFY This function is used to monitor the integrity of each audit record and the whole by verifying the signature. FCS_CKM.3 This specifies the mechanism used in acing the private key used for the protection of the audit records. FIA_UAU.1 This prevents the accessing of audit records without first ensuring that the user has the rights to access those audit records. FIA_UAU.2_CAO This prevents the accessing of audit records without first ensuring that the user has the rights to access the audit records. FMT_SAE.1 This function is used to ensure that the credentials of the auditor have not expired. FMT_SMR.1 This function is used to ensure that the TOE maintains the list of users associated with the TOE audit manager roles.
O.DisposalOfAuthenticationData	FCS_CKM.4 This function ensures that any private, secret or signing key that is used (in combination with a digital certificate) to identify and authenticate a user that is held in memory for the duration of the cryptographic operation is destroyed so that it cannot be re-used. FMT_REV.1 This function enables authorized users to revoke user privileges (by revoking or suspending their certificates or removing their attributes) for users who are no longer permitted to have those privileges. FMT_SAE.1 This function automatically revokes user privileges by invalidating authentication data (user certificates) when they have expired. FMT_MTD.2 limits the validity of certificates to reasonable amounts of time. FDP_RIP.1 This function ensures that authentication data that may reside in memory is securely deleted once used. This applies to passphrase, PINs and key material.

O.IndividualAccountability	FAU_GEN.1 This function ensures that all security relevant events are recorded in the audit log. FAU_GEN.2 This function supports this objective by ensuring, where possible, the user associated is identified with the event that is recorded in the audit log. FMT_MOF.1 This function supports this objective by ensuring that security functions can only be performed by authorized persons. FMT_MSA.1 This function ensures that only authorized persons are able to change security attributes, and, if they have been found to do so wrongly, that authorization can be withdrawn from them. FMT_MSA.2 and FIA_SOS.1 ensure that secure passphrases are used, so as to reduce the risk of private keys being discovered by someone other than the owner. FDP_ACC.1 and FDP_ACF.1 describe the access control policy that is enforced by the TOE to control who can perform controlled operations on specified objects such as the audit records. FCO_NRO.2 This function supports this objective by ensuring the user cannot deny their actions by using the digital signature of the user, which is cryptographically bound to the identity of the user. FIA_UID.1 This function ensures that any security relevant operation requires the user to be identified before initiating the function. FIA_UID.2_CAO This function ensures that any PKI Administration function cannot be initiated without the user being identified beforehand. FIA_UAU.2_WebRAO, FIA_UID.2_WebRAO ensure that only authenticated and identified persons can perform the WebRAO functions. Because of this, their actions can be linked to them via log records. FIA_USB.1 This function binds security attributes to the user associated with that attribute. This ensures that all operations involving a subject with attributes can be traced to an individual user. FMT_SMR.1 Ensures that all security roles can be associated to a user.
O.Installation	AGD_ADM.1 Ensures that the TOE Owners have sufficient information to install, maintain and operate the TOE in a secure manner.

	ADO_IGS.1 Ensures that the TOE is installed in a secure manner by providing guidance. ADO_DEL.2 Ensures that the TOE owner can distinguish between a genuine delivered TOE or a product masquerading as the TOE. This also ensures that the delivered product is the item identified in this security target as the TOE.
O.CPS	AGD_ADM.1 This ensures that the PKI administrators have sufficient information to allow them to operate the TOE in compliance to a defined Certificate Policy(ies) and Certification Practices Statement(s). AGD_USR.1 This ensures that TOE users have sufficient information to allow them to use the TOE in accordance with a defined Certificate Policy(ies) and Certification Practices Statement(s).
O.CryptographicFunctions	FCS_CKM.1 This functions ensures that cryptographic keys that are generated comply with the appropriate algorithm, key length and standards. FCS_CKM.2_PublicKey This function ensures that the public keys are distributed according the relevant standards and formats. FCS_CKM.2 This function ensures that when generated by the TSF the secret, private or signing keys are distributed securely according to the relevant standard and formats. FCS_CKM.3 Ensures that key load occurs according the relevant method and standards. FCS_CKM.4 This function ensures that key destruction is done correctly. FCS_COP.1_Sign This function ensures that signing functions use appropriate algorithms and hash functions according to the relevant standards. FCS_COP.1_Verify This function ensures that verification of a digital signature is in accordance to the relevant standards. FCS_COP.1_Hash This function ensures that cryptographic hash are generated with the appropriate algorithm and parameters. FCS_COP.1_Encrypt This function ensures that encryption operations are performed with the appropriate algorithm, key size and parameters. FCS_COP.1_Decrypt This function ensures that decryption operations are performed with the

	appropriate algorithms and parameters.
O.NonRepudiation	FCS_COP.1_Sign Contributes to meeting the objective by requiring that the TOE conforms to recognized digital signature standards. This function also contributes to meeting the objectives by associating and binding the signature with the user that produced it. The binding and association is performed by the contents of the message or data, which is protected by the digital signature. FCS_COP.1_Verify Contributes to this objective by ensuring that signatures on data can be checked. FAU_GEN.1 This function ensures that all security relevant events are recorded in the audit log, with the identity of the user that caused them and the date/time of the event. FCO_NRO.2 Contributes to satisfying this objective by ensuring that the user associated with a subject, message, or data cannot deny producing it by binding the user identity with the evidence in the form of a digital signature. FCS_CKM.3 Contributes to this objective by ensuring that the key loading for the signature operation conforms to the defined standards. FMT_SMR.1 Ensures that the TOE maintains the list that identifies the users associated with security relevant roles. FIA_UAU.2_CAO, FIA_UID.2_CAO ensure that only authenticated and identified persons can perform the CAO functions. Because of this, their actions can be linked to them via log records. FIA_UAU.2_WebRAO, FIA_UID.2_WebRAO ensure that only authenticated and identified persons can perform the WebRAO functions. Because of this, their actions can be linked to them via log records. FPT_SSP.1 Ensures that receipts can be generated to ensure that TSF data has not been modified when being passed to another part of the TSF. This contributes to this objective by guaranteeing the integrity of the evidence associated with the non-repudiation.
O.Audit	FAU_GEN.1 identifies the auditable events for which audit records should be generated and specifies the information to be provided in the audit records. FCS_CKM.3 specifies the mechanism(s) used in loading private keys used in the administration of the TOE.

	FAU_STG.1 Ensures that if evidence stored in the audit log is archived by an unauthorized person or modified then this can be detected. FCS_COP.1_Sign contributes to meeting the objective by requiring that the TOE conforms to recognized digital signature and hashing standards. FCS_COP.1_Verify contributes to meeting the objective by allowing auditors to verify the integrity of the audit logs FIA_USB.1 Ensures that the auditor role is bound to an authorized user. FMT_MOF.1 This function supports this objective by ensuring that security functions can only be performed by authorized persons.
O.DataImportExport	FCS_CKM.2_PublicKey Contributes to this objective by ensuring that public keys that are distributed are done so in compliance with standards and formats that ensure integrity by being transported inside X.509 digital certificates that are digitally signed using FCS_COP.1_Sign. FCS_CKM.2 Contributes to this objective by ensuring secret, private or signing key confidentiality is protected by FCS_COP.1_Encrypt that encrypts the keys and confidentiality by using FCS_COP.1_Sign that adds a signature to security relevant data that is transferred to the other parts of the TOE. FDP_IFC.1 Contributes to this objective by ensuring that information flow is controlled by specific SFPs, which ensure that confidential data is protected before being transmitted. FTP_ITC.1 Contributes to this objective by ensuring that information flow is controlled by specific SFPs, when importing user data. FCO_NRO.2 Contributes to this objective by ensuring that the list of security relevant transmitted information is generated with evidence of origin. Because of this, the originator can be checked by the TOE to be sure that they are allowed to communicate with the TOE – if not, the communications are not accepted. FDP_IFF.1 ensures that the TOE components only communicate with known entities. FDP_ITT.1 ensures that data that is received by TOE components is checked before FPT_ITI.1, FPT_ITT.1, FDP_ITT.1 and FDP_ITT.3

	Contributes to this objective by ensuring that TOE data integrity can be verified on receipt by TOE components, and discarded if modified.
O.FlawUnknownToUser	ALC_FLR.2 Enforces this objective by ensuring that the users and TOE owners are notified of any known flaw.
O.FlawRemediation	ALC_FLR.2 Contributes to this objective by ensuring that the users and TOE owners are notified of any known flaw and any remediation. ACM_SCP.2 Contributes to this object by ensuring that any reported flaws can be tracked to the point where the user and owner receive remediation information. AGD_USR.1 and AGD_ADM.1 ensures that the guidance documentation covers the correct way to respond to any flaws that have been found. ATE_COV.2 Contributes to this objective by ensuring that test coverage is sufficient to detect any potential security flaws. ATE_DPT.1 Contributes to this objective by ensuring that depth of testing is sufficient to detect any potential security flaws. ATE_FUN.1 Contributes to this objective by ensuring that the security functional design is adequately documented to prevent any inadvertent or deliberate potential security flaw being introduced into the TOE. ATE_IND.2 Contributes to this objective by introducing independent testing to verify that known security flaws are not part of the TOE.
O.Guidance	AGD_ADM.1 Contributes to this objective by ensuring that there is sufficient information for the owners, and administrators to operate and configure the TOE securely. ADO_IGS.1 Contributes to this objective by ensuring that there is sufficient information for the owners, and administrators to install the TOE securely. AGD_USR.1 Contributes to this objective by ensuring that there is sufficient information for the TOE users to operate the TOE and interact with the TOE securely.
O.IntegrityTOEData	FCS_COP.1_SIGN Contributes to this objective by ensuring that the data integrity can be verified by signing TOE data using standard algorithms and parameters. FCS_COP.1_VERIFY Contributes to this objective by

	using verification to check for data modification prior to using the data. FDP_ITT.3 Contributes to this objective by ensuring that TOE data integrity can be verified after transmitting between TOE components. FPT_ITI.1 Contributes to this objective by ensuring that TOE data integrity can be verified after transmitting between TOE components. FPT_ITT.1 Contributes to this objective by ensuring that TOE data integrity can be verified after transmitting between TOE components. FCS_CKM.3 Contributes to this objective by ensuring that the key loading for the signature operation conforms to the defined standards. FCS_CKM.2 Contributes to this objective by ensuring that TOE certificate integrity is assured by using FCS_COP.1_Sign and FCS_COP.1_Verify.
O.IntegrityUserData	FCS_COP.1_SIGN Contributes to this objective by ensuring that the data integrity can be verified by signing user data using standard algorithms and parameters. FCS_COP.1_VERIFY Contributes to this objective by using verification to check for data modification prior to using the data. FPT_SSP.1Contributes to this objective by ensuring that when requested by another part of the TSF, shall acknowledge the receipt of an unmodified TSF data. This occurs during the initial handshake between TOE modules and the CA/RA. FDP_ITT.3 Contributes to this objective by ensuring that user data integrity can be verified after transmitting between TOE components. FPT_ITT.1_WebRAO Contributes to this objective by ensuring that user data (certificates) integrity can be verified after transmitting between TOE components. FCS_CKM.3 Contributes to this objective by ensuring that the key loading for the signature operation conforms to the defined standards. FCS_CKM.2 Contributes to this objective by ensuring that TOE certificate integrity is assured by using FCS_COP.1_Sign and FCS_COP.1_Verify. FMT_MOF.1 and FMT_MTD.1 ensure that only authorized persons can perform specified operations on user data.

O.ConfidentialityTOEData	FCS_COP.1_ENCRYPT Contributes to this objective by ensuring that confidentiality is provided by secure cryptographic algorithms and parameters. FCS_COP.1_DECRYPT Contributes to this objective by ensuring that encrypted data is decrypted securely. FCS_CKM.3 Contributes to this objective by ensuring that the key loading for the signature operation conforms to the defined standards.
O.ConfidentialityUserData	FCS_COP.1_ENCRYPT Contributes to this objective by ensuring that confidentiality is provided by secure cryptographic algorithms and parameters. FCS_COP.1_DECRYPT Contributes to this objective by ensuring that encrypted data is decrypted securely. FCS_CKM.3 Contributes to this objective by ensuring that the key loading for the signature operation conforms to the defined standards. FPT_ITC.1_RA Contributes to this objective by ensuring that if the user private key needs to be exported outside the TSC the confidentiality is maintained by encryption as per FCS_COP.1_Encrypt FPT_ITT.1 ensures that key material handled by the TOE is protected from modification. FDP_ACC.1 and FDP_ACF.1 describe the access control policy that is enforced by the TOE to control who can perform controlled operations on specified objects such as user data. FCS_CKM.4 This function ensures that key destruction is done securely, to assist private keys to remain private.
O.LifeCycleSecurity	ACM_AUT.1 Contributes to this objective by ensuring that only authorized changes can be made to the TOE during development. ACM_CAP.4 Contributes to this objective along with ACM_AUT.1 by providing an automatic method to ensure that the TOE is generated from configuration items, and that any changes to configuration items are authorized. ACM_SCP.2 Contributes to this objective by ensuring that any flaws discovered during development can be tracked and reduces the likelihood of the flaws remaining in the TOE. ALC_DVS.1 Contributes to this objective by ensuring that the integrity and confidentiality of the TOE is maintained during development.

	ALC_LCD.1 Contributes to this objective by ensuring that there is a defined product development and maintenance lifecycle that will reduce the likelihood of deliberate or accidental flaws being introduced into the product, and ensures that remedial actions will be performed to eliminate flaws discovered during development. ALC_TAT.1 Contributes to this objective by ensuring that all tool options used in development are unambiguously defined to prevent the introduction of flaws. ADO_DEL.2 Ensures that the TOE is delivered securely. ADO_IGS.1 Ensures that the TOE is installed and started up securely.
O.MaintainUserAttributes	FMT_MOF.1 Contributes to this objective by ensuring that security functions can only be performed by authorized persons. FMT_MSA.1 Contributes to this objective by enforcing an access control SFP to prevent unauthorized changes to the user attributes. FMT_MSA.2 and FIA_SOS.1 Contributes to this objective by ensuring that only secure values for passphrases will be accepted. FMT_MSA.3 Contributes to this objective by ensuring that secure initial values are initialized for user attributes. FIA_ATD.1 Contributes to this objective by ensuring that the TOE maintains attributes belonging to individual users. FAU_STG.1 Allows only an Authorized user the ability to archive audit records, and provides a mechanism to detect modification to the audit record. Audit records will show who changed a user's attributes. FDP_ACC.1 and FDP_ACF.1 describe the access control policy that is enforced by the TOE to control who can perform controlled operations on specified objects such as user attributes. FIA_USB.1 ensures that the appropriate user security attributes are associated with the user, and not someone else's. FCS_COP.1_SIGN ensures that user attributes are

	signed when held by the TOE.
O.ProtectConfiguration	FAU_GEN.1 Contributes to this objective by deterring administrators from making unauthorized changes by recording all security relevant events, including changing the TOE configuration. FAU_GEN.2 Contributes to this objective by deterring administrators from making unauthorized changes by ensuring that users are accountable for their actions. FCS_COP.1_SIGN Contributes to this objective by protecting the PKI configuration by using cryptographic techniques that signing functions use appropriate algorithms and hash functions according to the relevant standards. FCS_COP.1_VERIFY Contributes to this objective by using verification to check for data modification prior to using the data. FIA_UAU.2_CAO Contributes to this objective by ensuring that users are successfully authenticated before being allowed to perform CAO mediated actions including changing the PKI configuration. FMT_SMR.1 Contributes to this objective by ensuring that the TOE associates users with roles. FDP_IFF.1 ensures that the TOE components only communicate with known entities. FDP_ACC.1 and FDP_ACF.1 describe the access control policy that is enforced by the TOE to control who can perform controlled operations on specified objects such as the TOE configuration. FMT_MOF.1 and FMT_MTD.1 ensure that only authorized persons can perform specified operations on configuration data. FMT_SMF.1 Contributes to this objective by providing a mechanism that will ensure that TOE administrators who can modify the PKI cannot delete the audit records. This is contingent on the policy P.RoleSeparation being enforced by the TOE owners.
O.ProtectAuditRecords	FAU_GEN.1 Contributes to this objective by deterring administrators from making unauthorized changes by recording all security relevant events, including deleting and archiving the audit records. FAU_GEN.2 Contributes to this objective by deterring administrators from making unauthorized changes by ensuring that users are accountable for their actions. The audit log records audit data archive events. FCS_COP.1_SIGN Contributes to this objective by

	protecting the audit record by using cryptographic techniques that signing functions use appropriate algorithms and hash functions according to the relevant standards. FCS_COP.1_VERIFY Contributes to this objective by using verification to check for audit date modification when initiated by the Audit Reviewer. FIA_UAU.2_CAO Contributes to this objective by ensuring that users are successfully authenticated before being allowed to perform CAO mediated actions including reviewing and deleting and archiving the audit records. FMT_SMR.1 Contributes to this objective by ensuring that the TOE associates users with roles. FDP_ACC.1 and FDP_ACF.1 describe the access control policy that is enforced by the TOE to control who can perform controlled operations on specified objects such as the audit records. FMT_SMF.1 Contributes to this objective by providing a mechanism that will ensure that TOE administrators who can modify the PKI cannot delete the audit records. This is contingent on the policy P.RoleSeparation being enforced by the TOE owners. FMT_MOF.1 and FMT_MTD.1 ensure that only authorized persons can perform specified operations on log data.
O.ProvideEvidenceOfOrigin	FCO_NRO.2 Contributes to this objective by ensuring that the list of security relevant transmitted information is generated with evidence of origin. FCS_COP.1_Sign Supports FCO_NRO.2 by using standard cryptographic techniques to add evidence of origin to the transmitted information. FDP_IFF.1 ensures that the TOE components only communicate with known entities. FCS_COP.1_Verify Supports FDP_DAU.2, FDP_DAU.2_CAO and FDP_DAU.2_WebRAO by using standard cryptographic techniques to verify the evidence of origin attached to the transmitted information. FDP_DAU.2 Contributes to this objective by ensuring the TSF has the capability to generate evidence of origin for transmitted security relevant information, and also ensures that the evidence of origin can be verified by using secure cryptographic algorithms and parameters in FCS_COP.1_Sign. The TSF can verify the evidence of origin by using FCS_COP.1_Verify.

	FDP_DAU.2_CAO contributes to this objective by ensuring the CAO has the capability to generate evidence of origin for transmitted security relevant information, and also ensures that the evidence of origin can be verified by using secure cryptographic algorithms and parameters in FCS_COP.1_Sign. The TSF can verify the evidence of origin by using FCS_COP.1_Verify. FDP_DAU.2_WebRAO contributes to this objective by ensuring the TSF has the capability to generate evidence of origin for transmitted security relevant information, and also ensures that the evidence of origin can be verified by using secure cryptographic algorithms and parameters in FCS_COP.1_Sign. The TSF can verify the evidence of origin by usingFCS_COP.1_Verify.
O.Passphrase	FMT_MSA.2 and FIA_SOS.1 ensure that passphrases conform to minimum length and complexity requirements.
O.ControlUnknownOriginComms	FCS_COP.1_VERIFY Contributes to this objective by using standard cryptographic algorithms and parameters for signature verification to check for subject identification before establishing a session with the subject. FDP_IFF.1 ensures that the TOE components only communicate with known entities. FDP_ITC.1 contributes to this objective by allowing the import of user data, but limiting the import to user data without security attributes when importing data from outside the TOE scope of control (TSC). FPT_SSP.1Contributes to this objective by ensuring that when requested by another part of the TSF, shall acknowledge the receipt of an unmodified TSF data. This occurs during the initial handshake between TOE modules and the CA/RA.
O.MaliciousCodeNotExecuted	AGD_USR.1 and AGD_AGD.1 Contributes to this objective by providing information to the user and administrator to identify valid and trusted downloadable code, to ensure that the user does not download and install malicious mobile code that is not signed or signed by an untrusted third party.

Table 8-6 – Security Objectives

8.3.4 Security Assurance Requirements Rationale

The target evaluation level of CC EAL 4 is sufficiently high given the identified threats and security objectives. In particular, it considers the vulnerabilities that may be exploited by external threat agents in the vulnerability analyses that are not included in lower assurance levels. The TOE has been developed in a manner to ensure that CC EAL 4 is attainable.

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices that, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOE and are prepared to incur additional security-specific engineering costs.

These are the circumstances applicable to UniCERT 5, and so, for these reasons, EAL4 is suitable.

8.3.5 Strength of Function Level Rationale

8.3.5.1 The Minimum Strength of Function Level of SOF-Basic is consistent with the security objectives of the TOE because of the Evaluation Assurance Level that is sought, and the likely expertise, resources, and motivation of attackers as described in the statement of TOE security environment.

8.3.5.2 As described in paragraph 511 of the CC part 2, in the description of AVA_VLA.2, it is necessary for the TOE to be resistant to penetration attacks by attackers of low attack potential only, in order to satisfy AVA_VLA.2. Furthermore, as described in the descriptions of threat sources in chapter 3 of this ST, the expertise, resources and motivation of attackers will never be high, due to the fact that the TOE will not be used to protect assets of any greater than low value. The minimum strength level for this TOE of SOF-Basic is therefore consistent with both of these because, according to Table B.2 in Annex B to the CEM, SOF-Basic provides adequate protection against attackers of low attack potential.

8.3.6 Dependency Rationale

8.3.6.1 The following table summarizes how the dependencies among SFRs are satisfied. The first column is used to identify individual rows. The second column lists all SFRs that contribute to the TOE security objectives. The next column contains the dependencies on each SFR. The last column references the row that refers to the dependency or states that it is not satisfied. For each unsatisfied dependency there is an explanation below the table, which shows why the dependency does not need to be satisfied.

ID	SFR	Dependency	Satisfied by
1	FAU_GEN.1	FPT_STM.1	Not satisfied

ID	SFR	Dependency	Satisfied by
2	FAU_GEN.2	FAU_GEN.1	1
		FIA_UID.1	34
3	FAU_SAR.1	FAU_GEN.1	1
4	FAU_SAR.2	FAU_SAR.1	3
5	FAU_SAR.3	FAU_SAR.1	3
6	FAU_STG.1	FAU_GEN.1	1
7	FCO_NRO.2	FIA_UID.1	34
8	FCS_CKM.1	FCS_COP.1	13,14,15,16 & 17
		FCS_CKM.4	12
		FMT_MSA.2	44
9	FCS_CKM.2_PublicKey	FCS_CKM.1	8
		FCS_CKM.4	12
		FMT_MSA.2	44
10	FCS_CKM.2	FCS_CKM.1	8
		FCS_CKM.4	12
		FMT_MSA.2	44
11	FCS_CKM.3	FCS_CKM.1	8
		FCS_CKM.4	12
		FMT_MSA.2	44
12	FCS_CKM.4	FDP_ITC.1	22
		FCS_CKM.1	8
		FMT_MSA.2	44
13	FCS_COP.1_SIGN	FCS_CKM.1	8
		FCS_CKM.4	12
		FMT_MSA.2	44
14	FCS_COP.1_VERIFY	FCS_CKM.1	8
		FCS_CKM.4	12
		FMT_MSA.2	44
15	FCS_COP.1_HASH	FCS_CKM.1	8
		FCS_CKM.4	12
		FMT_MSA.2	44
16	FCS_COP.1_ENCRYPT	FCS_CKM.1	8
		FCS_CKM.4	12

ID	SFR	Dependency	Satisfied by
		FMT_MSA.2	44
17	FCS_COP.1_DECRYPT	FCS_CKM.1	8
		FCS_CKM.4	12
		FMT_MSA.2	44
18	FDP_ACC.1	FDP_ACF.1	19
19	FDP_ACF.1	FDP_ACC.1	18
		FMT_MSA.3	45
20	FDP_IFC.1	FDP_IFF.1	21
21	FDP_IFF.1	FDP_IFC.1	20
		FMT_MSA.3	45
22	FDP_ITC.1	FDP_ACC.1	18
		FDP_IFC.1	20
		FMT_MSA.3	45
23	(deleted)	(deleted)	(deleted)
24	FDP_ITT.1	FDP_ACC.1	18
		FDP_IFC.1	20
25	FDP_ITT.3	FDP_ACC.1	18
		FDP_IFC.1	20
		FDP_ITT.1	24
26	FDP_RIP.1	NONE	
27	FDP_DAU.2	FIA_UID.1	34
28	FDP_DAU.2_CAO	FIA_UID.1	34
29	FDP_DAU.2_WebRAO	FIA_UID.1	34
30	FIA_ATD.1	NONE	
31	FIA_UAU.1	FIA_UID.1	34
32	FIA_UAU.2_CAO	FIA_UID.2_CAO	35
33	FIA_UAU.2_WebRAO	FIA_UID.2_WebRAO	36
34	FIA_UID.1	NONE	
35	FIA_UID.2_CAO	NONE	
36	FIA_UID.2_WebRAO	NONE	
37	FIA_USB.1	FIA_ATD.1	30
38	FIA_SOS.1	NONE	
39	(deleted)	(deleted)	

ID	SFR	Dependency	Satisfied by
40	(deleted)	(deleted)	
41	FMT_MOF.1	FMT_SMR.1	50
		FMT_SMF.1	49
42	(deleted)	(deleted)	
43	FMT_MSA.1	FDP_ACC.1	18
		FDP_IFC.1	20
		FMT_SMF.1	49
		FMT_SMR.1	50
44	FMT_MSA.2	ADV_SPM.1	Assurance Measure
		FDP_ACC.1	18
		FDP_IFC.1	20
		FMT_MSA.1	43
		FMT_SMR.1	50
45	FMT_MSA.3	FMT_MSA.1	43
		FMT_SMR.1	50
46	FMT_MTD.1	FMT_SMR.1	50
		FMT_SMF.1	49
47	FMT_REV.1	FMT_SMR.1	50
48	FMT_SAE.1	FMT_SMR.1	50
		FPT_STM.1	Not satisfied
49	FMT_SMF.1	NONE	
50	FMT_SMR.1	FIA_UID.1	34
51	FPT_ITC.1_RA	NONE	
52	FPT_ITI.1	NONE	
53	FPT_ITT.1_WebRAO	NONE	
54	FPT_ITT.1	NONE	
55	FPT_SSP.1	FPT_ITT.1	54
56	FMT_MTD.2	FMT_MTD.1	46
		FMT_SMR.1	50

Table 8-7 – SFR Dependency Analysis

8.3.6.2 The dependencies are not directly satisfied:

a) That of FAU_GEN.1 and FPT_SAE on FPT_STM.1

FAU_GEN.1 refers to the requirement of the TOE to have reliable timestamps for its own use, in order to put timing information in its audit logs. FMT_SAE has a similar requirement, in order to enforce time-limited authorization. In both cases the dependency is not required as the environmental security objective OE.TimeSource ensures that the administrator provides a reliable time source for both purposes.

8.3.7 Mutually Supportive Security Requirements Rationale

8.3.7.1 The security requirements are mutually supporting as all requirements are based purely on the CC part 2 and all dependencies have been addressed in some way. The set of SFRs are internally consistent and include SFRs that defend other SFRs against attacks such as bypassing or tampering.

8.3.7.2 The internal consistency of the security requirements is demonstrated by considering how they fall under the following categories:

a) **Security Audit (FAU)**. All of the audit SFRs relate to the same set of data, namely the auditable events. These events are recorded in an events log, associated with the identity of the entity that caused the event and time it occurred. Facilities are provided to review the events for selected users. The audit events are protected using cryptographic functions, with facilities provided to detect modifications to the audit records

b) **Communication (FCO).** The TSF enforces the generation of evidence of origin for its communications using its cryptographic functions, and provides facilities to check this evidence

c) **Cryptographic Support (FCS).** The cryptographic support SFRs (FCS_CKM.1, FCS_CKM.2, FCS_CKM.3, FCS_CKM.4 and FCS_COP.1) specify the requirements for generating, distributing, destroying, loading and using the cryptographic keys. These SFRs support the signing, encryption and decryption of communications and data. The cryptographic support SFRs support the other functions as shown under those functions elsewhere in this section. There are no potential conflicts with these SFRs.

d) **User Data Protection (FDP)**. The user data protection SFRs (FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1, FDP_ITC.1, FDP_ITT.1, FDP_ITT.3, FDP_RIP.1 and FDP_DAU.2) describe how the privacy and integrity of user data held by the TOE is preserved by access control to user data. FDP_ACC.1 defines the subjects, objects and operations allowed by the SFPs of the TOE. FDP_ACF.1, FDP_IFF.1, FDP_ITC.1, FDP_ITT.1, FDP_ITT.3 and FDP_IFC.1 define the SFPs and they way that the SFPs will be used. FDP_RIP.1 describes the protection applied to user data when it is no longer required. FDP_DAU.2, FDP_DAU.2_CAO, FDP_DAU.2_WebRAO define the evidence to be provided to guarantee the validity and origin of specified data. There are no potential conflicts with any other TOE SFR.

e) **Identification and Authentication (FIA).** The identification and authentication SFRs (FIA_ATD.1, FIA_UAU.1, FIA_UAU.2_CAO, FIA_UAU.2_WebRAO, FIA_UID.1, FIA_UID.2_CAO, FIA_UID.2_WebRAO, FIA_USB.1 and FIA_SOS.1) describe a number of rules for the identification and authentication of users by the TOE. These rules are specified in FIA_UAU.1, FIA_UAU.2_CAO, FIA_UAU.2_WebRAO, FIA_UID.1, FIA_UID.2_CAO, FIA_UID.2_WebRAO. FIA_ATD.1 and FIA_USB.1 describe the attributes of users who are managed by the TSF, and FIA_SOS.1 describes the rules on password choice. There are no instances where one of these identification and authentication SFRs applies to other SFRs in a way where potential conflicts may arise.

f) **Security Management (FMT).** The Security Management SFRs (FMT_MOF.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1, FMT_MTD.2, FMT_REV.1, FMT_SAE.1, FMT_SMF.1 and FMT_SMR.1) specify the security management functions, describe how the security attributes are managed, and specifies the security roles that can carry out this function. These SFRs depend on the Identification and Authentication SFRs to determine the identity and role of a user before allowing them to perform security management functions. There are no potential conflicts with any other TOE SFR.

g) **Protection of the TSF (FPT).** These SFRs (FPT_ITC.1_RA,FPT_ITI.1, FPT_ITT.1_WebRAO, FPT_ITT.1, FPT_SSP.1) describe how the TSF protects itself. It does this by using the cryptographic functions to ensure that data is protected during transmission between the parts of the TOE. There are no potential conflicts with any other TOE SFR.

8.3.7.3 Mutual support by SFRs that prevent bypassing of other SFRs is implemented by the identification and authentication (FIA) SFRs which identify and authenticate users and work to prevent the impersonation of a user. They require all users to be identified and authenticated before allowing them to perform any security-relevant actions on the TOE. As noted earlier, the Cryptographic Support and Protection of the TSF (FCS) SFRs assist the communication (FCO) SFRs and Protection of the TSF (FPT) SFRs in providing secure communications within the TOE, and in turn those secure communications assist the other SFRs by ensuring the integrity and privacy of communications. The remaining SFRs are always invoked when necessary and hence cannot be bypassed if the SFRs are satisfied by the TSF.

8.3.7.4 Mutual support by SFRs that prevent anyone tampering with other SFRs is, again, implemented by the identification and authentication (FIA) SFRs that ensure that only authorized users have access to the TOE functions, in conjunction with the cryptographic (FCS) SFRs which ensure that it is not possible for unauthorized persons to disrupt the functions of other SFRs. The FCS SFRs support the Security Management (FMT) SFRs and the Protection of the TSF (FPT) SFRs in managing the TOE functions and ensuring that TOE communications are not tampered with.

8.3.7.5 Mutual support by SFRs that prevent deactivation of other SFRs or of attack aimed at defeating another SFR is implemented by the same means as specified above for mutual support by SFRs that prevent anyone tampering with other SFRs.

8.3.7.6 Mutual support by SFRs that enable the detection of the misconfiguration of another SFR is implemented by the Security Management (FMT) SFRs that give authorized users access to the security functions of the TSF, enabling them to detect the configuration of the TOE, and therefore any misconfiguration of the TOE. The Security Audit (FAU) SFRs also assist in detecting misconfiguration of the TOE – these, again, are supported by the cryptographic (FCS) SFRs.

8.4 TOE Summary Specification Rationale

8.4.1 This section demonstrates that the TOE security functions and assurance measures are suitable to meet the TOE security requirements.

8.4.2 It demonstrates the following:

a) That the combination of specified TOE IT security functions work together so as to satisfy the TOE security functional requirements;

b) That the strength of TOE function claims made are valid, or that assertions that such claims are unnecessary are valid

c) That the claim is justified that the stated assurance measures are compliant with the assurance requirements.

8.4.3 IT Security Functions Rationale

A mapping of IT Security Functions onto SFRs is provided in Table 6.1. It demonstrates that each SFR is mapped onto at least one IT Security Function and that each IT Security Function is mapped onto at least one SFR. For a justification for each of these mappings, the reader is directed to the textual description of each function that is also provided in Table 6.1.

8.4.4 Strength of Function Claim Rationale

The strength of function claims for the IT security functions are consistent with the strength of functions for the TOE SFRs because they are the same: both are SOF-Low. The claims for the minimum strength of TOE SFRs and the minimum strength of the IT Security Functions are both made in the section on “Minimum Strength of Function Level” in Chapter 5.

8.4.5 Mutually Supportive IT Security Functions Rationale

The TOE Summary Specification does not introduce any changes to the dependency and mutual support argument presented for SFRs.

8.4.6 Security Assurance Measures Rationale

The security assurance requirements of EAL 4 are achievable for the following reasons:

d) All documentation and other resources required by this assurance level as shown in Table 6.2 will be made available

e) The documents have been produced to fulfill the criteria of this assurance level

f) The TOE has been developed to achieve a high degree of security

g) The TOE was developed in a secure manner.

8.5 PP Claims Rationale

No Protection Profile conformance claims have been made.

9. Security Policy Model

9.1 Introduction

9.1.1 This section details the security policy model that is enforced by the TOE security functions (TSP).

9.1.1.1 Security policy models

SPM_TOE_CONFIDENTIALITY	Private key material is encrypted for the receiver by using key exchange using the receiver's public key certificate. This applies to all end entity private/secret keys when being archived or recovered. The private key material is encrypted using the encrypt operations as specified in FCS_COP.1_ENCRYPT and can be decrypted using the decrypt operation as specified in FCS_COP.1_DECRYPT.
SPM_USER_CONFIDENTIALITY	Private key material is encrypted for the receiver by using key exchange using the receiver's public key certificate. This applies to all end entity private/secret keys when being archived or recovered. The private key material is encrypted using the encrypt operations as specified in FCS_COP.1_ENCRYPT and can be decrypted using the decrypt operation as specified in FCS_COP.1_DECRYPT.
SPM_TOE_INTEGRITY	Security relevant TOE data is protected from modification by use of digital signatures. The security relevant TOE data is stored in the database, signed by a valid PKI entity and when accessed the signature is checked according to SPM_SIGNATURE_VALIDITY. When transferred by TCP/IP communications the entity transferring the data will use digital signatures and the receiving entity will use SPM_MESSAGE_VALIDITY. The signing operation is as defined in FCS_COP.1_SIGN.
SPM_USER_INTEGRITY	Security relevant user data is protected from

	modification by use of digital signatures. The security relevant user data is stored in the database, signed by a valid PKI entity and when accessed the signature is checked according to SPM_SIGNATURE_VALIDITY. When transferred by TCP/IP communications the entity transferring the user data will use digital signatures the receiving entity will use SPM_MESSAGE_VALIDITY. The signing operation is as defined in FCS_COP.1_SIGN.
SPM_SIGNATURE_VALIDITY	In relation to authenticating signed data against a given identity (as described in FDP_DAU.2, FDP_DAU.2_CAO and FDP_DAU.2_WebRAO), as well detecting Inter TSF modification of data (as described in FPT_ITI.1), the signature is determined to be valid if: 1. The entity certificate is in the PKI (for PKI entities) 2. The signature is verified (FCS_COP.1_VERIFY) 3. Optionally checking for an appropriate extension 4. The certificate has not expired nor has been revoked or suspended. 🗎 TOE users and certificate attributes are defined in section 9.2.2
SPM_SECURE_HASH	Security relevant messages and data are hashed, and signed, for integrity checking. The receiver can verify that the message or data is unmodified by checking the hash of the message with the hash encrypted in the signature. The Hash operation is as defined in FCS_COP.1_HASH.
SPM_PASSWORD_METRIC	Enforced when PSE, P12s are generated by TOE components – the passphrase must be at least 8 characters with at least one alpha, one numeric, one upper, one lower, and one non alphanumeric character (FIA_SOS.1).
SPM_REVOKE_CERTIFICATE	An entity can request a revocation of their certificate, but only an authorized entity can Authorize the revocation (FMT_REV.1).
SPM_REMOVE_PKI	The CAO with PKI management attributes can remove an entity from the PKI directly

	(FMT_REV.1). A PKI entity can be untrusted (by other PKI entities) when their certificate has expired or has been revoked.
SPM_CHANGE_WEBRAO_GROUP	A WebRAO user may only authorize requests for certificates which have been requested using a registration policy to which they have been granted access. Likewise, a WebRAO user may only authorize requests to revoke certificates, where those certificates have been issued using a registration policy to which the WebRAO has been granted access for the purpose of revocation. Access to registration policies is controlled by a CAO user with the appropriate privileges. Refer to 9.2.2.10 and FMT_MOF.1.
SPM_CHANGE_CAO_ATTRIBUTE	The operations that a CAO can perform are controlled by their privileges. Only a CAO with appropriate privileges may change the privileges of another CAO. Refer to 9.2.2.2 and FMT_MOF.1.

Table 9-1 – Security Model

9.1.1.2 Security function policy

SFP_SIGNED_MESSAGES	As described through section 2.3 several of the components sign messages to other components within the TOE. Also, signed messages may be sent to users externally to the TOE (e.g., messages over the SCEP protocol and OCSP protocols). SPM_USER_INTEGRITY and SPM_TOE_INTEGRITY refer to the mechanism for signing and validating these messages. In addition to checks undertaken in SPM_SIGNATURE_VALIDITY, the following checks are also carried out: • Checking for Delayed Messages • Checking Replay Attacks
SFP_SIGNED_DATA	Certain TOE data and certain USER data is signed when being saved to the database. SPM_TOE_INTEGRITY and SPM_USER_INTEGRITY refer to the mechanisms for signing and validating the data.
SFP_AUDITOR	The Audit functions (FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1) can only be accessed by the

	roles with Auditor attributes (CAO Auditor, RA Auditor, CAO Audit Manager, RA Audit Manager) In addition, the archive functions of CA audit records is restricted to the CAO Audit Manager, the RA Audit Manager can archive RA audit records.

Table 9-2 – Security Function Policy

9.2 Definition of Users

This section lists the users, their required attributes and their roles as used in the document.

9.2.1 Users that are of relevance to the TOE, but do not act on it directly, and having attributes not controlled by the TOE.

CC Label	Common Label	Role	Identified	Authenticated	By OSP
Administrators	System Administrator	Network Admin	No	No	Yes
		OS Admin	No	No	Yes
		Database Admin	No	No	Yes
Operators	Backup Operator	Backup Operator	No	No	Yes
		Restore Operator	No	No	Yes

Table 9-3 – Users Relevant to the TOE

9.2.1.1 Administrators (Attributes not maintained by the TOE)

The following are IT administrator roles used to maintain the TOE environment that are created by the organizational security policies and not enforced or maintained by the TOE:

- Network administrator
- Operating system administrator
- Database administrator

9.2.1.2 Users (Attributes not maintained by the TOE)

The following are IT user roles that are used to maintain the TOE. These are created by the organization security policies, and not enforced by the TOE:

- Backup/restoration user

9.2.2 Subjects

The following subjects are defined for both Access_Control_SFP and Information_Flow_Control_SFP.

Common Label	Has Private Key	Has Certificate	Full DN	Partial DN	Has Cybertrust Defined OID= 1.2.372.980001.3.1
CA	✓	✓	✓	✗	✗
CAO user, CAO Audit Manager, CAO Auditor	✓	✓	✓	✓	.2
RA user	✓	✓	✓	✗	.1
RA Audit Manager RA Auditor	✓	✓	✓	✗	.22
CSS	✓	✓	✓	✗	✗
RA eXchange	✓	✓	✓	✗	.11
email PH	✓	✓	✓	✗	✗
Web PH	✗	✗	✓	✗	✗
WebRAO	✓	✓	✓	✗	.3 or .21
SCEP PH	✓	✓	✓	✗	✗

Table 9-4 – Summary of Subjects, and the Ways They Are Identified

A tick represents "yes", the entity possesses one, and a cross represents "No", the entity does not possess one.

9.2.2.1 CA

The CA is created on bootstrap, has an X.509 certificate with the following attributes:

- X.509 Basic Constraint: IsCA = TRUE.
- The CA key(s) usages should include: digital signature, non-repudiation, certificate signing and CRL signing. These may be part of the usage of one or more keys, but the CA requires key(s) that cover all these uses.
- The CA certificate is registered in the PKI, and must be valid and not expired.
- The CA is identified by its X.509 certificate DN, binding to its identity is by its private key.

9.2.2.2 CAO Users (including CAO Audit Manager and CAO Auditor)

The CAO users may have the ability to configure the PKI, add, modify policies, create certificates and manage PKI entity certificates when permitted.

The CAO user has an X.509 certificate with the following attributes:

- BTL Entity extension with OID=1.2.372.980001.3.1.2

- The CAO certificate is registered in the PKI, and must be valid and not expired.
- The CAO key(s) usages should include: digital signature and non-repudiation.
- The CAO is identified by its X.509 certificate DN, binding to its identity is by its private key.

The CAO users use the CAO GUI. They may have one or more of the following permissions (which are assigned by attributes within the PKI rather than in their certificate):

- View and Modify the PKI
- Manage Other Users
- Create and Manage Registration Policies
- Authorize CA Certificates
- Revoke CA Certificates
- Authorize PKI Entity Certificates
- Revoke PKI Entity Certificates
- Authorize End Entity Certificates
- Revoke End Entity Certificates
- Create and edit authorization groups
- Query the CA audit data (i.e., be a CAO Auditor)
- Archive the CA audit data (i.e., be a CAO Audit Manager).

CAO users are not able to edit their own permissions. Each CAO user (with permissions to manage other users) is able to create and assign permissions to other CAOs up to and including their own set of permissions. The CAO created at bootstrap has all permissions - this can later be changed by another authorized CAO.

CAO users who have been given CAO Audit Manager or CAO Auditor permissions (which are assigned by attributes within the PKI rather then in their certificates) may also act as RA Audit Managers or an RA Auditors, respectively. They will use the RA Event Viewer to perform the following tasks:

- Query the RA audit data (RA Auditor).
- Archive the RA audit data (RA Audit Manager).

9.2.2.3 RA

The RA is created by the CAO user with appropriate attributes after bootstrap. The RA has an X.509 certificate with the following attributes:

- X.509 BLT Entity extension with OID=1.2.372.980001.3.1.1
- The RA key usages should include: digital signature.
- The RA certificate is registered in the PKI, and must be valid and not expired.
- The RA is identified by its X.509 certificate's DN; binding to its identity is by its private key.
- The RA is identified by its X.509 DN, and authenticated by having its certificate registered in the PKI by the CAO user.

RA users have the following permission (which are assigned via attributes within the PKI rather than in their certificate).

- Query the RA audit data (i.e., be a RA Auditor) using the RA Event Viewer.

9.2.2.4 RA Auditor (including RA Audit Manager)

The RA Auditor is created by the CAO user with appropriate attributes after bootstrap. This entity has an X.509 certificate with the following attributes:

- X.509 BLT Entity extension with OID=1.2.372.980001.3.1.22
- The RA Auditor key usages should include: digital signature and non-repudiation
- The RA Auditor certificate is registered in the PKI, and must be valid and not expired.
- The RA Auditor is identified by its X.509 certificate's DN; binding to its identity is by its private key.
- The RA Auditor is identified by its X.509 DN, and authenticated by having its certificate registered in the PKI by the CAO user.

The RA Auditor has the following permissions (which are assigned via attributes within the PKI rather than in their certificate):

- Query the RA audit data (i.e., be a RA Auditor)
- Delete and archive the RA audit data (i.e., be a RA Audit Manager).

9.2.2.5 The CSS

The CSS is created by the CAO user with appropriate attributes after bootstrap. The CSS has an X.509 certificate with the following attributes:

- Extended key usage with X.509 OID= 1.3.6.1.5.5.7.3.9, equivalent to an OCSP certificate.

- The CSS key usages should include: digital signature.

- The CSS certificate is registered in the PKI, and must be valid and not expired.

- The CSS is identified by its X.509 certificate's DN, binding to its identity is by its private key.

- The CSS is identified by its X.509 DN, and authenticated by having its certificate registered in the PKI by the CAO user.

9.2.2.6 The RA eXchange

The RA eXchange is created by the CAO user with appropriate attributes after bootstrap. The RA eXchange has an X.509 certificate with the following attributes:

- BTL Entity extension with OID=1.2.372.980001.3.1.11

- The RA eXchange key(s) usages should include: digital signature.

- The RA eXchange certificate is registered in the PKI, and must be valid and not expired.

- The RA eXchange is identified by its X.509 certificate's DN, binding to its identity is by its private key.

- The RA eXchange is identified by its X.509 DN, and authenticated by having its certificate registered in the PKI by the CAO user.

9.2.2.7 The email PH

The email Handler is created by the CAO user with appropriate attributes after bootstrap. The email Handler has an X.509 certificate with the following attributes:

- The email Handler certificate is registered in the PKI, and must be valid and not expired.

- The email Handler is identified by its X 509 certificate's DN, binding to its identity is by its private key.

- The email Handler is identified by its X.509 DN, and authenticated by having its certificate registered in the PKI by the CAO user.

9.2.2.8 The Web Handler

The Web Handler is created by the CAO user with appropriate attributes after bootstrap. The Web Handler does not have X.509 certificate or a private key. The Web Handler is identified by a partial DN.

9.2.2.9 The SCEP PH

The SCEP Handler is created by the CAO user with appropriate attributes after bootstrap. The SCEP Handler has an X.509 certificate and a private key – these things are used to identify it.

Each SCEP PH must be associated with a certificate that is currently registered in the PKI for it to function.

9.2.2.10 WebRAO users

The WebRAO user grouping is based on DN or partial DN, and is configured by the CAO with permission to change the PKI. The CAO user has the ability to restrict the access to policy forms to a group or groups of WebRAO users.

WebRAO users, which are created by either the CAO user or by a WebRAO user with access to a WebRAO policy, have an X.509 certificate with the following attributes:

- BTL Entity extension with OID=1.2.372.980001.3.1.3 or OID=1.2.372.980001.3.1.21
- The WebRAO key(s) usages should include: digital signature.
- The WebRAO Certificate is not registered in the PKI, but must be valid and not expired.
- The WebRAO is identified by its X.509 certificate's DN, binding to its identity is by its private key.

9.2.3 End Entities

End entities are PKI users who have no role in the PKI, but have certificates issued by the PKI. Their activities are out of scope of the evaluation.

9.3 Information Flow Control Policy

This ST contains one information flow control policy (Information_Flow_Control_SFP), and one access control policy (Access_Control_SFP). This section contains the rules used to derive these policies.

For both policies:

- The subjects are defined in Section 9.2.2, which also describes how they are identified.

- The information and operations, and the rules regarding those operations, are as described in this section.
- The access control based on subject, object and permitted operations are as described in this section.

9.3.1 Access to CA

The CA will permit communications with an entity connecting to it if the entity (which will be an RA, CAO or KAS) is registered in the PKI and has a valid certificate.

If the connection receives messages that have been duplicated then the CA protects itself from replay attacks, delayed message attacks.

If the entity connecting to the CA is invalid, the CA will disconnect the entity.

9.3.1.1 Information passed from CA to CAO

The CA communicates with the CAO via the database. The CA does not respond to the CAO announce message. The following are valid communications:

- The CAO sends certificate request, cross certification request and revocation request messages by writing the request in the database. The CA verifies that the CAO user is a valid CAO user and has the attributes associated with certificate manager.
- The CAO sends CRL generation messages to the CA via the database. The CA verifies the CAO user is a valid CAO user with permission to change the PKI.
- The CAO sends PKI configuration information to the CA via the database. The CA verifies the CAO user is a valid CAO user with permission to change the PKI.
- The CA sends certificate response, and revocation response to the CAO via the database. The CAO verifies the signature on the responses against the CA certificate in the PKI data.

9.3.1.2 Information passed from the CA to the RA and from the RA to the CA.

The RA communicates with the CA via CMP over TCP. The RA needs to connect to the CA, the CA replies to the RA announce message with the PKI data. The following are valid communications:

- The RA sends an announce message to the CA. The CA verifies that the announce message has not been delayed, has not been replayed and has been signed by a valid RA;
- CA reads the PKI information from DB, packages up information, signs information and sends to RA in response to an Announce message, the RA verifies that the signature on the announce message is valid;

- The RA sends certificate request, renewal request and revocation request messages by writing the request in the database. The CA verifies that the RA is a valid RA in the PKI;
- The CA sends request responses, revocation response and renewal responses to the RA. The RA verifies the CA signature.

9.3.1.3 KAS to CA

The KAS communicates with the CA via CMP over TCP. The KAS needs to connect to the CA, the CA replies to the KAS announce message with the PKI data.

The announce message is the only valid communication between the KAS and the CA.

9.3.2 Access to CAO GUI

The CAO will permit a session with an entity connecting to it if:

- The user has a valid CAO certificate.

The CAO will enforce additional security roles as defined in the CAO user roles in section 9.2.2 to limit the CAO user's available functions.

9.3.2.1 Information exported from the CAO

The user logged into the CAO has the ability to delete audit events. The deletion of audit events is only permitted under the following conditions:

- The CAO user has the attributes associated with audit manager; and
- The CAO user has exported the archive data using the audit archive function.

The user logged into the CAO has the ability to archive audit events. The archive of audit events is only permitted under the following conditions:

- The CAO user and has the attributes associated with an audit manager.

The archived log integrity is protected by using a digital signature of the audit manager; however there is no restriction on accessing the archived data as it is exported out of the TOE scope of control.

9.3.3 Access to RA

The RA will permit a session with an entity connecting to it if:

- The entity, a CA, CSS or KAS, if the entity is registered in the PKI and has a valid certificate.

If the connection has been duplicated, the RA protects itself from replay attacks, delayed message attacks by disconnecting the entity.

If the entity connecting to the RA is invalid, the RA will disconnect the entity.

9.3.3.1 RA eXchange to RA

Communication between RA and RA eXchange takes place only through database as both share a common database.

The digital signature certificates of RA and RA eXchange (and other PKI entities) lie in the common database.

Message verification includes checking for:

- Delayed messages
- Anti-replay attack
- Signature verification and that the entity is part of the PKI.

The following are valid messages between the RA eXchange and RA:

- Certificate registration request, certificate revocation request, certificate renewal request.

The following are valid messages between the RA and RA eXchange:

- PKI data is sent by the CA to the RA, this data is a signed CMP message from the CA, the RA stores the PKI data in the database. The RA eXchange verifies the CA signature against the trust point in its PSE;
- The RA stores policy and authorization path data in the database, the RA eXchange obtains these from the database;
- The RA stores notification messages from the CA in to the database. The RA eXchange converts this information to a message that the protocol handler can obtain form the database and transmit the message.

9.3.3.2 CSS to RA

Communication between CSS and RA uses CMP over TCP. The RA uses the OCSP protocol to communicate to the CSS. The RA will connect to the CSS when it requires status information, on receiving status responses the RA will disconnect from the CSS. The RA verifies the signature on the CSS response. The CSS certificate is contained in the PKI data.

9.3.4 Access to RA Event Viewer

An RA user that is either an RA Auditor or an RA Audit Manager (section 9.2.2) may connect to the RA Event Viewer GUI to perform the tasks.

9.3.4.1 Information exported from the RA Event Viewer

The user logged into the RA Event Viewer has the ability to delete audit events. The deletion of audit events is only permitted under the following conditions:

- The RA Event Viewer user has the attributes associated with audit manager; and
- The RA Event Viewer user has exported the archive data using the audit archive function.

The user logged into the RA Event Viewer has the ability to archive audit events. The archive of audit events is only permitted under the following conditions:

- The RA Event Viewer user and has the attributes associated with an audit manager.

The archived log integrity is protected by using a digital signature of the audit manager; however there is no restriction on accessing the archived data as it is exported out of the TOE scope of control.

9.3.5 Access to the RA eXchange

The protocol handlers connect to the RA eXchange via BRSP messages. The protocol handler will indicate to the RA eXchange what type of protocol handler it is. The RA eXchange verifies the connection and responds with security irrelevant configuration information.

9.3.5.1 Access to the WebRAO

The WebRAO GUI can be accessed with a valid WebRAO certificate (refer to section 9.2.2). However any request signed by the WebRAO will be verified by the RA to ensure that WebRAO user is part of the authorization group and has access to the policy the certificate request was based on.

The WebRAO does not verify the data sent by the RA eXchange.

9.3.5.2 Access to the CSS

Communication between CSS and RA eXchange uses CMP over TCP. The RA eXchange uses the OCSP protocol to communicate to the CSS. The RA eXchange will connect to the CSS when it requires status information, on receiving status responses the RA eXchange will disconnect from the CSS. The RA eXchange verifies the signature on the CSS response. The CSS certificate is contained in the PKI data.

9.3.5.3 Access to the Web Handler

The Web Handler can be accessed by any end user. The CAO user will define the policies the Web Handler can access. The WebRAO user will authorize requests from the Web Handler.

9.3.5.4 Access to the email Handler

The email Handler can be accessed by any end user. The CAO user will define the policies the email Handler can access. The WebRAO user will authorize requests from the email Handler.

9.3.5.5 Access to the SCEP Handler

The SCEP Handler can be accessed by any end user. The CAO user will define the policies the SCEP Handler can access. The WebRAO user will authorize requests from the SCEP Handler.

Appendix A Documentation Contents on TOE CDs

A.1 UniCERT Core v5.2.1 for Windows

Filename	File size (bytes)
Files in D:\docs	
index.htm	955
readme.html	29,364
thirdpartylicense.txt	9,803
wwhelp3.cab	120,586
wwhelp3.jar	192,132
Files in D:\docs\admin	
admin.pdf	1,466,347
adminIX.xml	28,002
adminTOC.xml	5,358
catalog.css	16,757
dbw.html	3,366
dbw2.html	4,373
dbw3.html	11,766
dbw4.html	5,163
dbw5.html	10,270
dbw6.html	9,152
dbw7.html	10,874
dbw8.html	5,662
dbw9.html	5,469
document.css	561
introducing.html	3,663
introducing2.html	12,466
introducing3.html	15,009
keymgr.html	3,644
keymgr2.html	5,446
keymgr3.html	4,762
keymgr4.html	5,773
keymgr5.html	3,962
ralog.html	5,473
ralog10.html	7,580
ralog11.html	4,166
ralog12.html	4,105
ralog13.html	3,321
ralog14.html	3,728
ralog15.html	4,361
ralog2.html	6,216
ralog3.html	3,158
ralog4.html	2,883
ralog5.html	17,164
ralog6.html	3,315
ralog7.html	3,382
ralog8.html	3,344
ralog9.html	5,233
servicestr.html	5,551
servicestr2.html	8,360
servicestr3.html	6,105
servicestr4.html	6,475
servicestr5.html	5,159
servicestr6.html	6,625

Filename	File size (bytes)
servicestr7.html	4,416
servicestr8.html	4,412
servicestr9.html	3,133
tokenmgr.html	5,005
tokenmgr10.html	3,931
tokenmgr11.html	4,794
tokenmgr12.html	3,667
tokenmgr13.html	4,071
tokenmgr14.html	8,944
tokenmgr15.html	3,619
tokenmgr16.html	4,315
tokenmgr17.html	4,030
tokenmgr18.html	3,369
tokenmgr19.html	5,029
tokenmgr2.html	5,565
tokenmgr20.html	7,170
tokenmgr21.html	6,470
tokenmgr22.html	3,406
tokenmgr23.html	3,534
tokenmgr24.html	4,733
tokenmgr25.html	3,985
tokenmgr26.html	3,624
tokenmgr27.html	3,649
tokenmgr28.html	3,524
tokenmgr3.html	5,050
tokenmgr4.html	3,470
tokenmgr5.html	5,428
tokenmgr6.html	3,796
tokenmgr7.html	9,422
tokenmgr8.html	6,719
tokenmgr9.html	4,951
Files in D:\docs\admin\images	
ab.gif	881
auditarchive.gif	7,201
bullet.gif	822
caution.gif	1,533
dbw_1Logon.gif	8,097
dbw_2dbw.gif	11,087
dbw_APM1.gif	7,210
dbw_APM2.gif	13,373
dbw_APM3.gif	14,661
dbw_CA2.gif	13,104
dbw_CAO2.gif	13,751
dbw_UpPass1.gif	13,265
dbw_button_RefreshList.gif	1,567
dbw_button_create.gif	1,614
dbw_button_delete.gif	1,627
dbw_button_lock.gif	1,662
dbw_ca1.gif	6,976
dbw_ca3.gif	14,075
dbw_cao1.gif	7,270
delete.gif	862
filteringlog.gif	3,805
filteringlog2.gif	4,062
iconconfigure.gif	910
info.gif	1,155
keygen_01.gif	37,653
keygen_05.gif	34,323
keygen_06.gif	35,763
keygen_07.gif	7,785

Filename	**File size (bytes)**
logo.gif	2,524
new.gif	877
newquery2.gif	2,583
querylog.gif	5,189
querylog2.gif	13,626
querylogeg.gif	4,649
querylogview.gif	11,038
rev_dblogon.gif	11,230
rev_logresult.gif	14,726
rev_mainscr.gif	10,196
rev_open.gif	13,528
rev_pseopen.gif	4,227
servicestra5.gif	815
ss_01.gif	4,573
ss_03.gif	4,613
ss_04.gif	5,582
ss_05.gif	11,235
tm_01.gif	7,422
tm_02.gif	9,448
tm_03.gif	9,879
tm_04.gif	11,045
tm_05.gif	9,933
tm_06.gif	10,240
tm_08.gif	2,387
tm_09.gif	7,541
tm_10.gif	2,831
tm_11.gif	5,785
tm_12.gif	3,034
tm_13.gif	5,021
tm_14.gif	2,600
tm_17.gif	4,885
warn.gif	1,171
Files in D:\docs\admin\wwhdata\common	
context.js	74
files.js	4,195
popups.js	38
title.js	72
topics.js	67
towwhdir.js	54
wwhpagef.js	4,505
Files in D:\docs\admin\wwhdata\java	
files.xml	10,530
ix.xml	28,002
search.xml	49,308
toc.xml	5,358
Files in D:\docs\admin\wwhdata\js	
index.js	20,326
search.js	1,687
toc.js	4,231
Files in D:\docs\admin\wwhdata\js\search	
search0.js	16,013
search1.js	16,097
search2.js	16,150
search3.js	6,982
Files in D:\docs\config	
CRLs.html	3,750
CRLs2.html	3,937
CRLs3.html	5,229
app_whcustom.html	3,783
app_whcustom10.html	4,723

Filename	**File size (bytes)**
app_whcustom11.html	4,312
app_whcustom12.html	2,917
app_whcustom13.html	4,461
app_whcustom14.html	8,180
app_whcustom15.html	4,715
app_whcustom2.html	4,217
app_whcustom3.html	4,725
app_whcustom4.html	7,262
app_whcustom5.html	5,544
app_whcustom6.html	5,663
app_whcustom7.html	7,353
app_whcustom8.html	9,937
app_whcustom9.html	11,462
appendixa.html	28,613
arm.html	3,813
arm10.html	3,556
arm11.html	4,119
arm12.html	5,157
arm13.html	3,424
arm2.html	4,396
arm3.html	3,222
arm4.html	3,258
arm5.html	3,544
arm6.html	3,737
arm7.html	3,311
arm8.html	3,535
arm9.html	3,916
ca.html	7,871
ca10.html	3,931
ca11.html	4,890
ca12.html	3,375
ca13.html	9,556
ca14.html	2,954
ca15.html	3,806
ca16.html	3,788
ca17.html	3,383
ca18.html	3,753
ca19.html	3,653
ca2.html	4,479
ca20.html	5,986
ca21.html	3,953
ca22.html	3,530
ca23.html	4,311
ca24.html	3,064
ca25.html	3,686
ca3.html	3,994
ca4.html	4,420
ca5.html	4,485
ca6.html	5,794
ca7.html	4,513
ca8.html	4,850
ca9.html	3,777
cao.html	3,334
cao.pdf	4,674,222
cao2.html	7,492
cao3.html	3,242
cao4.html	3,932
cao5.html	3,008
cao6.html	3,332
caoIX.xml	91,133

Filename	File size (bytes)
caoTOC.xml	23,912
catalog.css	16,757
certificates.html	4,676
certificates10.html	4,348
certificates11.html	3,394
certificates12.html	4,158
certificates13.html	4,713
certificates14.html	6,317
certificates15.html	5,024
certificates16.html	7,905
certificates2.html	4,436
certificates3.html	14,454
certificates4.html	5,757
certificates5.html	3,095
certificates6.html	2,962
certificates7.html	3,702
certificates8.html	4,092
certificates9.html	4,530
clone.html	5,163
clone2.html	2,865
clone3.html	4,177
clone4.html	3,450
clone5.html	3,827
crosscert.html	6,227
crosscert2.html	4,247
crosscert3.html	4,384
css.html	4,640
css2.html	4,465
css3.html	3,471
definingrps.html	4,138
definingrps10.html	5,258
definingrps11.html	4,816
definingrps12.html	4,888
definingrps13.html	6,374
definingrps14.html	6,465
definingrps15.html	4,586
definingrps16.html	5,563
definingrps17.html	4,446
definingrps18.html	3,806
definingrps19.html	6,649
definingrps2.html	3,597
definingrps20.html	9,679
definingrps21.html	4,211
definingrps22.html	5,312
definingrps23.html	5,749
definingrps24.html	4,455
definingrps25.html	15,622
definingrps26.html	5,234
definingrps27.html	4,208
definingrps28.html	4,527
definingrps29.html	4,327
definingrps3.html	5,892
definingrps30.html	4,887
definingrps31.html	3,992
definingrps32.html	3,097
definingrps33.html	3,767
definingrps34.html	5,695
definingrps35.html	3,333
definingrps36.html	3,541
definingrps37.html	2,932

Filename	File size (bytes)
definingrps38.html	6,846
definingrps39.html	4,489
definingrps4.html	3,045
definingrps40.html	4,076
definingrps41.html	2,999
definingrps42.html	5,280
definingrps43.html	3,755
definingrps44.html	4,032
definingrps45.html	3,244
definingrps46.html	3,710
definingrps47.html	4,011
definingrps48.html	3,256
definingrps49.html	4,760
definingrps5.html	6,265
definingrps50.html	4,267
definingrps51.html	3,224
definingrps6.html	3,881
definingrps7.html	4,693
definingrps8.html	4,547
definingrps9.html	3,428
document.css	561
introduction.html	5,560
introduction2.html	6,761
introduction3.html	6,557
introduction4.html	3,841
kao.html	5,053
kao2.html	5,143
kao3.html	4,715
kao4.html	3,346
kao5.html	3,855
kas.html	5,986
kas2.html	3,996
kas3.html	10,220
kas4.html	5,294
kas5.html	4,277
kas6.html	3,575
kas7.html	4,253
logs.html	5,857
logs10.html	2,741
logs11.html	3,383
logs12.html	3,473
logs2.html	17,899
logs3.html	3,156
logs4.html	3,415
logs5.html	3,050
logs6.html	5,097
logs7.html	9,372
logs8.html	4,605
logs9.html	3,424
ph.html	7,522
ph10.html	5,253
ph11.html	7,824
ph12.html	3,994
ph13.html	4,696
ph14.html	3,837
ph15.html	4,720
ph16.html	4,429
ph17.html	3,684
ph18.html	3,953
ph19.html	5,546

Filename	File size (bytes)
ph2.html	3,513
ph20.html	5,901
ph21.html	6,293
ph22.html	5,630
ph23.html	6,849
ph24.html	5,896
ph3.html	2,892
ph4.html	2,787
ph5.html	8,346
ph6.html	4,302
ph7.html	4,380
ph8.html	3,681
ph9.html	10,162
pki.html	6,029
pki2.html	4,874
pki210.html	7,934
pki211.html	3,504
pki22.html	5,558
pki23.html	9,799
pki24.html	7,813
pki25.html	12,610
pki26.html	7,495
pki27.html	5,809
pki28.html	7,132
pki29.html	3,714
pki2a.html	3,722
pki3.html	9,228
pki4.html	6,752
pki5.html	9,272
pki6.html	9,203
pki7.html	12,405
pki8.html	3,592
pki9.html	6,256
ra.html	6,745
ra2.html	4,117
ra3.html	4,828
ra4.html	5,818
ra5.html	4,179
ra6.html	3,848
ra7.html	3,591
raa.html	5,759
raa2.html	5,170
raa3.html	2,773
rax.html	3,393
rax2.html	6,214
rax3.html	3,224
rax4.html	3,480
rax5.html	4,222
rax6.html	5,419
rax7.html	6,516
renew.html	6,499
renew10.html	8,321
renew11.html	10,121
renew12.html	6,005
renew13.html	8,967
renew14.html	9,776
renew15.html	6,034
renew16.html	9,077
renew17.html	10,679
renew18.html	10,514

Filename	File size (bytes)
renew19.html	13,090
renew2.html	3,751
renew20.html	7,943
renew21.html	4,018
renew22.html	6,957
renew23.html	18,409
renew24.html	4,959
renew25.html	3,968
renew26.html	3,574
renew27.html	3,991
renew28.html	9,776
renew29.html	7,437
renew3.html	5,249
renew30.html	11,661
renew31.html	4,546
renew4.html	4,805
renew5.html	4,548
renew6.html	6,840
renew7.html	5,876
renew8.html	4,382
renew9.html	3,317
rp.html	5,081
rp10.html	4,851
rp11.html	4,519
rp12.html	3,650
rp13.html	4,050
rp14.html	4,606
rp15.html	3,421
rp16.html	4,254
rp17.html	5,050
rp18.html	4,605
rp2.html	3,564
rp3.html	4,914
rp4.html	6,441
rp5.html	4,432
rp6.html	3,945
rp7.html	10,824
rp8.html	7,206
rp9.html	5,087
subCA.html	3,920
subCA2.html	3,897
subCA3.html	7,419
subCA4.html	4,331
subCA5.html	5,430
tasks.html	8,670
tasks2.html	4,013
tasks3.html	3,693
tasks4.html	3,183
tasks5.html	3,354
tasks6.html	3,212
tasks7.html	4,028
troubleshoot.html	3,846
troubleshoot2.html	2,829
troubleshoot3.html	3,309
troubleshoot4.html	3,506
troubleshoot5.html	2,888
troubleshoot6.html	4,223
troubleshoot7.html	3,686
troubleshoot8.html	3,476
troubleshoot9.html	3,207

Filename	File size (bytes)
webrao.html	4,056
webrao2.html	4,414
webrao3.html	5,143
webrao4.html	4,028
webrao5.html	3,764
webrao6.html	3,285
webrao7.html	3,403
webrao8.html	3,205
wh.html	5,478
wh10.html	3,080
wh11.html	6,207
wh12.html	12,560
wh13.html	6,415
wh14.html	4,493
wh15.html	4,822
wh16.html	6,280
wh2.html	5,038
wh3.html	4,942
wh4.html	3,427
wh5.html	4,935
wh6.html	4,399
wh7.html	3,481
wh8.html	7,650
wh9.html	3,022
Files in D:\docs\config\images	
ab.gif	881
addcdp.gif	5,981
addedcdp.gif	16,098
addentity.gif	5,420
alignspace.gif	6,850
apptype.gif	6,644
armlog.gif	8,853
armsda.gif	8,165
armtuning.gif	6,280
auditarchive.gif	7,201
auditdeletion.gif	35,700
authgroup.gif	3,652
authgrouptab.gif	3,701
bullet.gif	822
cacerts.gif	12,566
cacommunicate.gif	3,975
cacrl.gif	14,582
cadb.gif	2,891
caentityname.gif	12,725
cajob.gif	5,899
camiscellaneous.gif	7,690
caoaccess.gif	13,730
caotune.gif	23,511
caserverparam.gif	10,852
catune.gif	8,675
caution.gif	1,533
cert_request_ee.gif	18,108
certificate.gif	6,791
certificate_request_page.gif	8,991
certificateinstall.gif	9,081
certificatesa15.gif	1,117
certquery.gif	5,272
certtype.gif	2,305
choose.gif	37,081
choosepol.gif	34,026

Filename	File size (bytes)
choosepolicy.gif	26,030
cmpmode.gif	7,981
cmpreg.gif	16,551
cmprp.gif	12,762
cmptrust.gif	3,212
cmptune.gif	9,253
collection.gif	5,845
color.gif	2,834
columns.gif	6,086
combobox.gif	4,612
combobox2.gif	1,402
composequery.gif	13,335
connected.gif	1,166
cq_icon1.gif	157
cq_icon2.gif	166
crlgentime.gif	5,014
crosscerta.gif	8,150
cryptoprofile2.gif	11,045
csstune.gif	22,962
database.gif	3,758
delete.gif	862
deletiondetect.gif	4,819
dnelements.gif	24,623
dnorder.gif	4,034
dnvalue.gif	4,396
dnwindow.gif	4,523
dsapara.gif	4,893
editbox.gif	1,523
email.gif	13,648
emailadd.gif	9,606
emailnotification.gif	13,611
emailpemtags.gif	14,209
emailreg.gif	12,238
emailrp.gif	5,737
emailtemplate.gif	13,769
emailtemplate1.gif	11,187
emailtune.gif	15,086
entitiespki.gif	16,375
entityreq.gif	28,714
exportcrl.gif	7,987
exportcrl2.gif	8,550
filtering.gif	3,722
filtering2.gif	4,019
filteringlog.gif	3,805
filteringlog2.gif	4,062
fingeprint.gif	1,505
fingerprintalg.gif	4,574
form.gif	26,888
generateca.gif	28,249
genkeys.gif	38,427
grouptab.gif	5,348
iconcert.gif	928
iconconfigure.gif	910
iconerror.gif	890
iconrevoke.gif	935
icontask.gif	914
icontask2.gif	882
iddata.gif	13,847
importext.gif	12,420
info.gif	1,155

Filename	File size (bytes)
kaoaccess.gif	9,642
kaotuning.gif	6,092
kastuning.gif	10,891
keystore.gif	12,215
ldapuri.gif	3,364
ldapuriadv.gif	6,860
lisktuning.gif	4,903
lock.gif	940
logcolumns.gif	3,876
logo.gif	2,524
logoptions.gif	6,891
logresult.gif	12,520
logsa.gif	5,947
mainscreen.gif	10,939
mapped.gif	2,220
multkeys.gif	2,980
nested.gif	33,018
new.gif	877
newpolicy.gif	22,704
newquery.gif	5,775
newquery2.gif	2,583
newtemplate.gif	2,990
openpki.gif	4,571
openpki1.gif	5,650
pkia.gif	4,143
policyinfo.gif	21,255
policylife.gif	18,180
policymap.gif	14,351
policyscope.gif	3,987
policytab.gif	12,986
policytab1.gif	5,388
pselocate.gif	9,448
publication.gif	10,509
querylog.gif	5,189
querylog2.gif	13,626
querylogeg.gif	4,649
querylogview.gif	11,038
queryresult.gif	9,091
raaaccess.gif	7,961
ratasks.gif	22,092
ratune.gif	23,802
rax2eh.gif	8,853
rax2scepcmp.gif	11,440
rax2webrao.gif	20,911
rax2wh.gif	8,220
raxaccess.gif	18,259
raxaccess2.gif	18,597
raxtune.gif	13,216
received.gif	35,763
remote.gif	5,595
remove.gif	5,381
renewalrules.gif	5,323
renewcomplete.gif	10,922
renewcomplete2.gif	33,136
renewcomplete3.gif	11,105
renewcompletekeygen.gif	53,365
renewdecisions.gif	59,816
reneweditpolicy.gif	31,245
reneweditpolicya.gif	31,245
renewencrypt.gif	32,916

Filename	File size (bytes)
renewexport.gif	32,694
renewmulticert.gif	46,059
renewpkientity.gif	33,735
renewpolicy.gif	33,050
renewpse.gif	11,000
renewrootca1.gif	33,397
renewrootreuse.gif	33,121
renewsubCAdetails.gif	33,397
renewsubatroot1.gif	32,280
renewsubcaexport.gif	32,910
renewsubcaexport2.gif	32,753
renewsubcagrayout.gif	32,974
renewsubcaimport.gif	31,614
renewsubcapolicy.gif	33,555
renewsubcomplete.gif	10,978
renewsubkeygen.gif	5,900
renewsubmit.gif	33,097
renewsubp10.gif	9,415
renewsubreuse.gif	45,499
renewsubreuse2.gif	46,807
request.gif	21,847
requestnotify.gif	3,978
requestsum.gif	21,824
retire.gif	891
retire_unpub.gif	117
retirecdp.gif	3,531
retiregroup.gif	4,544
revoke.gif	5,715
revokentity.gif	5,546
rootcert.gif	7,177
rpproperties1.gif	9,313
rpproperties2.gif	12,204
rpproperties3.gif	10,472
rpproperties4.gif	9,500
rpproperties6.gif	10,782
rpproperties7.gif	11,437
ruleeg.gif	4,884
scep.gif	7,984
scepreg.gif	9,867
sceprp.gif	13,176
sceptune.gif	25,194
search_criteria_ee.gif	2,843
staticlist.gif	7,162
subca2.gif	34,309
subca3.gif	34,039
subca4.gif	28,052
submit.gif	35,171
suspend.gif	5,668
taborder.gif	3,592
tasksa.gif	17,832
tick.gif	882
titleurl.gif	1,201
unassigned.gif	915
unassigned2.gif	930
unsuspend.gif	5,838
viewevent.gif	5,749
warn.gif	1,171
Files in D:\docs\config\wwhdata\common	
context.js	72
files.js	18,571

Filename	**File size (bytes)**
popups.js	38
title.js	70
topics.js	67
towwhdir.js	54
wwhpagef.js	4,505
Files in D:\docs\config\wwhdata\java	
files.xml	30,257
ix.xml	91,133
search.xml	194,881
toc.xml	23,912
Files in D:\docs\config\wwhdata\js	
index.js	66,571
search.js	1,688
toc.js	19,305
Files in D:\docs\config\wwhdata\js\search	
search0.js	16,154
search1.js	16,125
search10.js	16,152
search11.js	15,839
search12.js	16,128
search13.js	1,137
search2.js	16,160
search3.js	16,139
search4.js	16,001
search5.js	16,141
search6.js	16,153
search7.js	16,145
search8.js	16,036
search9.js	15,710
Files in D:\docs\dbadmin	
catalog.css	16,757
dba_1b_changes.html	4,462
dba_1b_changes2.html	3,947
dba_1b_changes3.html	4,336
dba_1b_changes4.html	2,975
dba_1b_changes5.html	3,810
dba_1intro.html	2,891
dba_1intro2.html	6,384
dba_1intro3.html	4,618
dba_2ainstalloraclewindows.html	3,342
dba_2ainstalloraclewindows2.html	4,385
dba_2ainstalloraclewindows3.html	3,276
dba_2ainstalloraclewindows4.html	10,959
dba_2ainstalloraclewindows5.html	3,803
dba_2ainstalloraclewindows6.html	7,351
dba_2binstalloraclesolaris.html	3,341
dba_2binstalloraclesolaris2.html	4,394
dba_2binstalloraclesolaris3.html	3,422
dba_2binstalloraclesolaris4.html	9,108
dba_2binstalloraclesolaris5.html	10,350
dba_2binstalloraclesolaris6.html	3,803
dba_2binstalloraclesolaris7.html	7,418
dba_3acreate_dbwindows.html	3,828
dba_3acreate_dbwindows2.html	4,537
dba_3acreate_dbwindows3.html	18,907
dba_3acreate_dbwindows4.html	4,331
dba_3acreate_dbwindows5.html	6,363
dba_3bcreate_dbsolaris.html	3,549
dba_3bcreate_dbsolaris2.html	4,383
dba_3bcreate_dbsolaris3.html	18,896

Filename	File size (bytes)
dba_3bcreate_dbsolaris4.html	4,274
dba_4arunningoracle_windows.html	3,293
dba_4arunningoracle_windows2.html	6,207
dba_4arunningoracle_windows3.html	3,613
dba_4arunningoracle_windows4.html	4,270
dba_4arunningoracle_windows5.html	8,715
dba_4arunningoracle_windows6.html	5,347
dba_4brunningoracle_solaris.html	3,294
dba_4brunningoracle_solaris2.html	4,422
dba_4brunningoracle_solaris3.html	7,065
dba_4brunningoracle_solaris4.html	5,756
dba_4brunningoracle_solaris5.html	4,755
dba_4brunningoracle_solaris6.html	5,872
dba_4brunningoracle_solaris7.html	3,141
dba_4brunningoracle_solaris8.html	3,137
dba_4brunningoracle_solaris9.html	4,371
dba_5amorelisteners_windows.html	2,795
dba_5amorelisteners_windows2.html	7,781
dba_5bmorelisteners_solaris.html	2,797
dba_5bmorelisteners_solaris2.html	8,063
dba_6amorealiases_windows.html	3,275
dba_6amorealiases_windows2.html	9,137
dba_6bmorealiases_solaris.html	3,276
dba_6bmorealiases_solaris2.html	9,071
dba_7ahomeselector_windows.html	4,976
dba_8adbtranstion_windows.html	2,997
dba_8adbtranstion_windows2.html	4,452
dba_8adbtranstion_windows3.html	8,539
dba_8adbtranstion_windows4.html	8,191
dba_8bdbtranstion_solaris.html	2,984
dba_8bdbtranstion_solaris2.html	4,254
dba_8bdbtranstion_solaris3.html	8,967
dba_8bdbtranstion_solaris4.html	7,990
dba_appauto.html	3,025
dba_appauto2.html	2,557
dba_appauto3.html	3,797
dba_appauto4.html	7,431
dba_appbackup.html	3,419
dba_appbackup2.html	3,412
dba_appbackup3.html	3,569
dba_appbackup4.html	3,341
dba_appbackup5.html	3,286
dba_appbackup6.html	6,837
dba_appbackup7.html	4,983
dba_appbackup8.html	3,436
dba_appdbastudio_solaris.html	4,572
dba_appdbastudio_solaris2.html	3,513
dba_appdbastudio_solaris3.html	5,727
dba_appdbastudio_solaris4.html	3,526
dba_appdbastudio_windows.html	4,268
dba_appdbastudio_windows2.html	3,517
dba_appdbastudio_windows3.html	5,605
dba_appdbastudio_windows4.html	3,532
dba_appdelete.html	3,499
dba_appdelete2.html	4,216
dba_appdelete3.html	8,258
dba_apporadir.html	3,615
dba_apporadir2.html	3,084
dba_apporadir3.html	3,673
dba_apporadir4.html	4,489

Filename	File size (bytes)
dba_apporadir5.html	3,592
dba_apporadir6.html	3,347
dbadminguide.pdf	2,277,340
dbadminguideIX.xml	24,632
dbadminguideTOC.xml	8,366
document.css	561
Files in D:\docs\dbadmin\images	
099.summary.gif	33,520
099.summary_sol.gif	29,055
bullet.gif	822
caution.gif	1,533
db_config_ora_services.gif	15,241
db_upgrade_backup6_solaris.gif	39,047
db_upgrade_backup6_windows.gif	39,029
db_upgrade_database2.gif	42,242
db_upgrade_database2_sol.gif	42,266
db_upgrade_export_summary7_sol.gif	15,253
db_upgrade_export_summary7_wind.gif	15,060
db_upgrade_progress8.gif	42,122
db_upgrade_results9_sol.gif	21,658
db_upgrade_results9_win.gif	21,498
db_upgrade_rollback_issue4.gif	7,465
db_upgrade_temp.gif	5,579
db_upgrade_welcome1.gif	48,954
dbconfig92_archive_all_init_param.gif	11,201
dbconfig92_create_options.gif	7,315
dbconfig92_create_options_sol.gif	7,322
dbconfig92_db_storage_logs_gen.gif	13,815
dbconfig92_db_storage_logs_gen_sol.gif	13,828
dbconfig92_dbfeatures6.gif	6,212
dbconfig92_dbident4.gif	4,162
dbconfig92_dbtemplates3.gif	5,403
dbconfig92_init_param_archive.gif	9,428
dbconfig92_init_param_archive_sol.gif	9,486
dbconfig92_init_param_charset.gif	6,631
dbconfig92_init_param_dbsize.gif	5,549
dbconfig92_init_param_fileloc.gif	10,269
dbconfig92_init_param_fileloc_sol.gif	11,361
dbconfig92_initparam_mem9.gif	9,301
dbconfig92_messagefeatures7.gif	4,532
dbconfig92db_conoptions8.gif	5,830
dbconfig_passwords.gif	9,319
dbconfig_passwords_sol.gif	9,371
dbconfig_progress.gif	30,703
dbconfig_summary_92.gif	17,116
dbconfig_summary_92_sol.gif	17,121
delete_user.gif	28,698
home_selector1.gif	20,583
home_selector2.gif	20,594
home_selector3.gif	11,653
home_selector4.gif	7,978
info.gif	1,155
install92_avail_prod4.gif	79,097
install92_db_config7.gif	77,824
install92_file_loc3_sol.gif	78,552
install92_file_loc3_win.gif	77,135
install92_install_types4.gif	80,408
install92_install_types4_sol.gif	41,920
install92_mts8.gif	75,523
install92_progress10.gif	93,207

Filename	File size (bytes)
install92_rootsh_command_sol.gif	5,622
install92_rootsh_sol.gif	3,538
install_name.gif	2,059
logo.gif	2,524
lstnrctl.gif	9,549
net8asst_tns0008.gif	2,742
net8asst_tns0009.gif	6,212
netmgr_add_list_name.gif	2,216
netmgr_alias_protocol3.gif	8,723
netmgr_alias_protocol_settings4.gif	9,269
netmgr_alias_start1a.gif	15,727
netmgr_alias_test6.gif	10,388
netmgr_alias_test6a.gif	7,863
netmgr_alias_welcome2a.gif	7,739
netmgr_list_loc.gif	10,840
netmgr_lsnr_add_address3.gif	12,355
netmgr_lsnr_add_address3a.gif	8,070
netmgr_lsnr_add_database4.gif	9,492
netmgr_lsnr_add_database4_solaris.gif	9,479
netmgr_lsnr_start1.gif	13,141
oem_add_to_tree5.gif	6,043
oem_adding_uni6.gif	25,153
oem_check_db2.gif	17,055
oem_logged_in4_cropped.gif	21,670
oem_login1.gif	20,154
oem_password_login3.gif	21,010
ora_running.gif	8,150
oracledirectories.gif	4,501
regedit_04_nls_lang.gif	3,038
service_manager.gif	6,998
warn.gif	1,171
Files in D:\docs\dbadmin\wwhdata\common	
context.js	83
files.js	7,083
popups.js	38
title.js	81
topics.js	67
towwhdir.js	54
wwhpagef.js	4,505
Files in D:\docs\dbadmin\wwhdata\java	
files.xml	13,898
ix.xml	24,632
search.xml	62,572
toc.xml	8,366
Files in D:\docs\dbadmin\wwhdata\js	
index.js	14,425
search.js	1,687
toc.js	5,599
Files in D:\docs\dbadmin\wwhdata\js\search	
search0.js	16,125
search1.js	16,107
search2.js	16,144
search3.js	16,137
search4.js	5,320
Files in D:\docs\exts	
app_certext.html	24,236
app_crlext.html	8,386
app_dn.html	17,344
app_profiles.html	4,046
app_profiles2.html	4,251

Filename	File size (bytes)
app_profiles3.html	5,406
app_profiles4.html	3,824
app_profiles5.html	4,494
app_profiles6.html	5,511
app_profiles7.html	4,890
app_profiles8.html	3,905
catalog.css	16,757
document.css	561
extensions.pdf	1,165,967
extensionsIX.xml	28,932
extensionsTOC.html	4,737
extensionsTOC.xml	4,737
introx509.html	4,136
introx50910.html	9,826
introx50911.html	6,484
introx5092.html	4,471
introx5093.html	5,731
introx5094.html	6,879
introx5095.html	14,239
introx5096.html	6,305
introx5097.html	4,396
introx5098.html	5,496
introx5099.html	6,536
profile_rp.html	3,569
profile_rp10.html	10,248
profile_rp11.html	26,959
profile_rp2.html	4,550
profile_rp3.html	5,056
profile_rp4.html	4,674
profile_rp5.html	13,734
profile_rp6.html	3,062
profile_rp7.html	3,779
profile_rp8.html	4,350
profile_rp9.html	10,676
set_exts.html	3,007
set_exts10.html	4,646
set_exts11.html	5,644
set_exts12.html	5,634
set_exts13.html	5,709
set_exts14.html	5,109
set_exts15.html	5,231
set_exts16.html	5,357
set_exts17.html	4,097
set_exts18.html	5,165
set_exts19.html	5,019
set_exts2.html	8,079
set_exts20.html	4,366
set_exts21.html	4,627
set_exts22.html	4,364
set_exts23.html	4,469
set_exts24.html	2,546
set_exts25.html	3,806
set_exts26.html	10,601
set_exts27.html	9,923
set_exts28.html	4,197
set_exts29.html	3,506
set_exts3.html	5,208
set_exts30.html	4,416
set_exts31.html	3,875
set_exts32.html	4,116

Filename	File size (bytes)
set_exts33.html	3,387
set_exts4.html	8,459
set_exts5.html	4,210
set_exts6.html	5,357
set_exts7.html	5,236
set_exts8.html	4,308
set_exts9.html	4,470
Files in D:\docs\exts\images	
bullet.gif	822
caution.gif	1,533
certv3a.gif	54,197
info.gif	1,155
logo.gif	2,524
v2crl.gif	45,830
warn.gif	1,171
Files in D:\docs\exts\wwhdata\common	
context.js	69
files.js	3,648
popups.js	38
title.js	67
topics.js	67
towwhdir.js	54
wwhpagef.js	4,505
Files in D:\docs\exts\wwhdata\java	
files.xml	9,910
ix.xml	28,932
search.xml	55,882
toc.xml	4,737
Files in D:\docs\exts\wwhdata\js	
index.js	19,760
search.js	1,687
toc.js	3,516
Files in D:\docs\exts\wwhdata\js\search	
search0.js	16,164
search1.js	16,140
search2.js	16,138
search3.js	14,689
Files in D:\docs\index_topics	
arrow1.gif	1,022
arrow2.gif	1,282
arrow2big.gif	1,415
arrow3.gif	1,550
catalog.css	16,757
document.css	561
install.html	2,764
managing.html	3,127
planning.html	2,691
remarks.htm	699,714
running.html	3,274
search.html	688
testing.html	3,542
unicert1st.html	3,599
Files in D:\docs\install	
aboutdocs.html	4,231
aboutdocs10.html	3,187
aboutdocs11.html	3,106
aboutdocs12.html	7,207
aboutdocs13.html	3,922
aboutdocs14.html	3,560
aboutdocs15.html	8,642

Filename	**File size (bytes)**
aboutdocs2.html	4,583
aboutdocs3.html	6,571
aboutdocs4.html	3,007
aboutdocs5.html	3,031
aboutdocs6.html	8,478
aboutdocs7.html	3,014
aboutdocs8.html	2,994
aboutdocs9.html	3,191
catalog.css	16,757
document.css	561
install.pdf	1,332,178
installIX.xml	27,025
installTOC.xml	8,377
instructions.html	4,905
instructions10.html	2,977
instructions11.html	3,719
instructions12.html	3,591
instructions13.html	3,981
instructions14.html	8,269
instructions15.html	3,524
instructions16.html	4,568
instructions17.html	5,034
instructions18.html	3,843
instructions19.html	4,359
instructions2.html	4,579
instructions20.html	4,812
instructions3.html	3,824
instructions4.html	5,355
instructions5.html	4,116
instructions6.html	5,510
instructions7.html	3,964
instructions8.html	4,914
instructions9.html	8,291
plandeploy.html	5,204
plandeploy2.html	5,098
plandeploy3.html	6,371
plandeploy4.html	5,830
plandeploy5.html	4,123
plandeploy6.html	3,769
plandeploy7.html	3,603
plandeploy8.html	3,818
plandeploy9.html	3,744
prereqs.html	3,544
prereqs10.html	3,195
prereqs11.html	2,643
prereqs12.html	2,667
prereqs13.html	3,501
prereqs14.html	6,605
prereqs15.html	3,160
prereqs16.html	2,918
prereqs17.html	3,864
prereqs18.html	2,878
prereqs19.html	3,051
prereqs2.html	4,700
prereqs20.html	2,761
prereqs21.html	2,808
prereqs3.html	10,546
prereqs4.html	5,085
prereqs5.html	3,863
prereqs6.html	7,710

Filename	**File size (bytes)**
prereqs7.html	14,541
prereqs8.html	3,344
prereqs9.html	2,871
securepki.html	3,874
securepki10.html	3,852
securepki11.html	5,660
securepki12.html	6,720
securepki13.html	4,874
securepki14.html	3,258
securepki15.html	3,610
securepki16.html	4,350
securepki17.html	3,778
securepki18.html	4,150
securepki19.html	2,624
securepki2.html	6,172
securepki20.html	3,004
securepki21.html	6,957
securepki22.html	2,934
securepki23.html	4,848
securepki24.html	5,436
securepki25.html	5,630
securepki26.html	9,603
securepki3.html	3,606
securepki4.html	3,302
securepki5.html	2,664
securepki6.html	2,738
securepki7.html	3,178
securepki8.html	2,817
securepki9.html	3,701
webinstructions.html	4,373
webinstructions10.html	5,517
webinstructions11.html	5,613
webinstructions12.html	3,908
webinstructions13.html	3,309
webinstructions14.html	7,531
webinstructions15.html	3,349
webinstructions16.html	3,814
webinstructions17.html	3,646
webinstructions2.html	5,654
webinstructions3.html	3,885
webinstructions4.html	5,226
webinstructions5.html	7,387
webinstructions6.html	4,958
webinstructions7.html	6,433
webinstructions8.html	5,945
webinstructions9.html	3,748
Files in D:\docs\install\images	
bullet.gif	822
caution.gif	1,533
deployVPN2.gif	51,482
deploydemo.gif	11,473
docdiagram.gif	69,449
hostarchitect.gif	41,038
hostca.gif	47,288
info.gif	1,155
init_install.gif	80,923
installxp.gif	31,684
logo.gif	2,524
securepkia.gif	58,820
warn.gif	1,171

Filename	File size (bytes)
webinstructionsa.gif	110,567
Files in D:\docs\install\wwhdata\common	
context.js	71
files.js	6,510
popups.js	38
title.js	69
topics.js	67
towwhdir.js	54
wwhpagef.js	4,505
Files in D:\docs\install\wwhdata\java	
files.xml	13,658
ix.xml	27,025
search.xml	72,951
toc.xml	8,377
Files in D:\docs\install\wwhdata\js	
index.js	18,802
search.js	1,687
toc.js	6,245
Files in D:\docs\install\wwhdata\js\search	
search0.js	16,145
search1.js	16,158
search2.js	16,152
search3.js	16,127
search4.js	16,150
search5.js	1,277
Files in D:\docs\overview	
beginners.html	3,453
beginners10.html	3,966
beginners11.html	4,554
beginners12.html	5,187
beginners13.html	4,594
beginners14.html	5,055
beginners15.html	7,378
beginners16.html	9,843
beginners2.html	4,318
beginners3.html	6,150
beginners4.html	3,545
beginners5.html	3,428
beginners6.html	3,917
beginners7.html	6,088
beginners8.html	3,253
beginners9.html	5,005
catalog.css	16,757
certificates.html	3,077
certificates2.html	3,862
certificates3.html	6,074
certificates4.html	5,566
certificates5.html	4,622
certificates6.html	4,329
certificates7.html	4,097
certreq.html	3,692
certreq2.html	6,140
certreq3.html	5,708
certreq4.html	5,195
certreq5.html	5,652
certreq6.html	6,280
document.css	561
glossary.html	69,536
introduction.html	5,324
introduction10.html	5,776

Filename	**File size (bytes)**
introduction11.html	4,390
introduction12.html	4,103
introduction13.html	6,342
introduction14.html	4,227
introduction15.html	5,636
introduction16.html	7,064
introduction17.html	7,720
introduction18.html	4,480
introduction19.html	4,022
introduction2.html	3,828
introduction20.html	4,175
introduction3.html	6,366
introduction4.html	3,798
introduction5.html	3,623
introduction6.html	3,344
introduction7.html	4,023
introduction8.html	3,667
introduction9.html	4,122
overview.pdf	1,057,928
overviewIX.xml	23,697
overviewTOC.xml	5,722
pki_entities.html	3,689
pki_entities10.html	3,392
pki_entities11.html	3,419
pki_entities12.html	3,220
pki_entities13.html	3,277
pki_entities14.html	3,486
pki_entities15.html	4,097
pki_entities16.html	4,530
pki_entities17.html	5,158
pki_entities18.html	3,585
pki_entities19.html	3,042
pki_entities2.html	6,528
pki_entities20.html	3,584
pki_entities21.html	5,477
pki_entities22.html	4,777
pki_entities23.html	4,593
pki_entities24.html	3,747
pki_entities25.html	6,045
pki_entities26.html	3,908
pki_entities27.html	4,230
pki_entities28.html	3,819
pki_entities3.html	3,679
pki_entities4.html	3,462
pki_entities5.html	4,263
pki_entities6.html	3,590
pki_entities7.html	4,371
pki_entities8.html	3,322
pki_entities9.html	3,919
Files in D:\docs\overview\images	
bullet.gif	822
caution.gif	1,533
certprocess.gif	37,958
certtemplate.gif	21,953
gui_ex.gif	23,231
info.gif	1,155
laddertrust.gif	14,373
logo.gif	2,524
meetinmiddle.gif	15,845
pkiarch.gif	27,431

Filename	File size (bytes)
warn.gif	1,171
Files in D:\docs\overview\wwhdata\common	
context.js	69
files.js	4,378
popups.js	38
title.js	67
topics.js	67
towwhdir.js	54
wwhpagef.js	4,505
Files in D:\docs\overview\wwhdata\java	
files.xml	10,892
ix.xml	23,697
search.xml	84,226
toc.xml	5,722
Files in D:\docs\overview\wwhdata\js	
index.js	16,395
search.js	1,687
toc.js	4,125
Files in D:\docs\overview\wwhdata\js\search	
search0.js	16,072
search1.js	16,137
search2.js	16,138
search3.js	16,136
search4.js	16,156
search5.js	14,915
Files in D:\docs\overview\wwhelp	
books.xml	218
messages.xml	31,996
settings.xml	3,918
Files in D:\docs\overview\wwhelp\images	
altclose.gif	156
altopen.gif	173
caution.gif	1,533
info.gif	1,155
warn.gif	1,171
Files in D:\docs\overview\wwhelp\wwhimpl	
version.htm	868
Files in D:\docs\overview\wwhelp\wwhimpl\common\html	
blank.htm	336
bookmark.htm	339
content.htm	1,258
controll.htm	1,413
controlr.htm	1,454
default.css	553
default.htm	5,202
default10.htm	6,138
default11.htm	6,210
default2.htm	5,544
default3.htm	5,754
default4.htm	7,113
default5.htm	5,882
default6.htm	6,170
default7.htm	6,170
default8.htm	6,738
default9.htm	6,098
document.css	561
document.htm	1,056
init0.htm	935
init1.htm	1,400
init2.htm	1,098

Filename	File size (bytes)
init3.htm	935
pagenav.htm	1,338
switch.htm	1,379
title.htm	1,138
wwhelp.htm	3,620
Files in D:\docs\overview\wwhelp\wwhimpl\common\images	
bkmark.gif	250
bkmarkx.gif	99
close.gif	214
divider.gif	46
divider2.gif	46
doc.gif	150
email.gif	289
emailx.gif	93
fc.gif	235
fo.gif	174
frameset.gif	234
home.gif	287
logo.jpg	4,851
logocolor.gif	58
next.gif	248
nextx.gif	76
prev.gif	252
prevx.gif	76
print.gif	313
printx.gif	94
related.gif	440
relatedi.gif	95
relatedx.gif	95
spacer4.gif	51
spc1w2h.gif	43
spc1w7h.gif	44
spc2w1h.gif	43
spc5w1h.gif	43
sync.gif	270
syncx.gif	86
Files in D:\docs\overview\wwhelp\wwhimpl\common\private	
books.js	315
locale.js	12,224
options.js	1,594
popupf.js	3,024
title.js	133
Files in D:\docs\overview\wwhelp\wwhimpl\common\scripts	
bklist1s.js	422
bookgrps.js	5,006
booklist.js	7,909
browseri.js	3,482
controls.js	12,842
documt1s.js	190
filelist.js	1,710
handler.js	774
help.js	19,082
highlt.js	5,677
pophash.js	1,456
popup.js	12,897
related.js	13,393
strutils.js	12,383
switch.js	5,187
Files in D:\docs\overview\wwhelp\wwhimpl\java\html	
ie60win.htm	2,721

Filename	File size (bytes)
iemac.htm	1,820
iewindow.htm	2,296
netscape.htm	2,238
nosecie.htm	2,097
nosecie6.htm	2,522
nosecns.htm	2,237
wwhelp.htm	4,198
Files in D:\docs\overview\wwhelp\wwhimpl\java\private	
books.xml	230
locale.js	2,690
locale.xml	22,045
options.js	146
options.xml	1,086
Files in D:\docs\overview\wwhelp\wwhimpl\java\scripts	
handler.js	905
java.js	5,431
Files in D:\docs\overview\wwhelp\wwhimpl\js\html	
indexsel.htm	1,167
navigate.htm	1,353
panel.htm	1,568
panelini.htm	1,127
tabs.htm	1,149
wwhelp.htm	4,599
Files in D:\docs\overview\wwhelp\wwhimpl\js\images	
tabsbg.gif	45
Files in D:\docs\overview\wwhelp\wwhimpl\js\private	
locale.js	13,715
options.js	2,696
Files in D:\docs\overview\wwhelp\wwhimpl\js\scripts	
handler.js	475
index.js	44,486
index1s.js	171
javascpt.js	4,355
outlfast.js	6,502
outlin1s.js	167
outline.js	23,298
outlsafe.js	5,483
panels.js	6,663
search.js	33,500
search1s.js	341
search2s.js	147
search3s.js	142
search4s.js	142
tabs.js	3,713
Files in D:\docs\pubadmin	
addprofile.html	3,425
addprofile10.html	7,540
addprofile11.html	4,405
addprofile12.html	3,373
addprofile13.html	3,602
addprofile14.html	6,895
addprofile15.html	3,196
addprofile16.html	4,623
addprofile17.html	3,874
addprofile18.html	3,472
addprofile19.html	2,964
addprofile2.html	7,757
addprofile20.html	5,912
addprofile21.html	4,432
addprofile22.html	5,092

Filename	File size (bytes)
addprofile23.html	4,762
addprofile24.html	8,771
addprofile25.html	3,669
addprofile26.html	3,915
addprofile27.html	9,890
addprofile28.html	3,299
addprofile29.html	6,477
addprofile3.html	3,972
addprofile30.html	3,823
addprofile31.html	2,939
addprofile32.html	2,947
addprofile33.html	9,588
addprofile34.html	4,350
addprofile35.html	10,392
addprofile36.html	3,524
addprofile37.html	3,231
addprofile38.html	3,661
addprofile39.html	3,535
addprofile4.html	3,880
addprofile40.html	2,889
addprofile41.html	3,086
addprofile42.html	3,803
addprofile43.html	4,531
addprofile44.html	4,145
addprofile45.html	4,982
addprofile46.html	6,793
addprofile47.html	6,946
addprofile48.html	4,484
addprofile49.html	8,607
addprofile5.html	5,694
addprofile50.html	11,110
addprofile51.html	5,295
addprofile52.html	3,832
addprofile53.html	5,022
addprofile54.html	8,433
addprofile55.html	5,527
addprofile56.html	4,493
addprofile57.html	3,706
addprofile58.html	3,323
addprofile59.html	3,331
addprofile6.html	3,858
addprofile60.html	3,852
addprofile61.html	4,260
addprofile62.html	3,718
addprofile63.html	4,473
addprofile64.html	3,959
addprofile65.html	3,115
addprofile66.html	2,845
addprofile67.html	3,402
addprofile68.html	3,382
addprofile69.html	4,465
addprofile7.html	5,599
addprofile70.html	4,541
addprofile71.html	4,599
addprofile8.html	3,898
addprofile9.html	4,638
appx_aipa.html	6,025
appx_ldap.html	3,622
appx_ldap10.html	3,552
appx_ldap11.html	10,657

Filename	File size (bytes)
appx_ldap12.html	6,247
appx_ldap13.html	9,915
appx_ldap14.html	3,638
appx_ldap15.html	4,664
appx_ldap16.html	8,542
appx_ldap17.html	3,537
appx_ldap18.html	3,858
appx_ldap19.html	10,630
appx_ldap2.html	5,008
appx_ldap20.html	3,371
appx_ldap21.html	4,865
appx_ldap22.html	5,724
appx_ldap3.html	3,660
appx_ldap4.html	6,221
appx_ldap5.html	3,585
appx_ldap6.html	7,536
appx_ldap7.html	10,447
appx_ldap8.html	7,336
appx_ldap9.html	3,603
appx_ocsp.html	3,612
appx_ocsp2.html	7,145
appx_ocsp3.html	7,836
appx_trouble.html	4,029
appx_trouble2.html	3,979
appx_trouble3.html	2,888
appx_trouble4.html	4,161
appx_trouble5.html	13,589
catalog.css	16,757
crosscerts.html	3,500
crosscerts2.html	3,637
crosscerts3.html	5,930
document.css	561
emailtemplates.html	4,095
emailtemplates2.html	5,803
emailtemplates3.html	5,754
intro.html	4,194
intro10.html	3,415
intro11.html	4,478
intro12.html	3,728
intro13.html	3,337
intro14.html	3,290
intro15.html	3,545
intro16.html	3,143
intro17.html	3,357
intro18.html	5,030
intro19.html	4,616
intro2.html	3,993
intro20.html	4,386
intro21.html	4,031
intro22.html	5,172
intro23.html	4,815
intro24.html	7,308
intro25.html	3,592
intro3.html	5,854
intro4.html	6,352
intro5.html	3,964
intro6.html	3,317
intro7.html	3,410
intro8.html	3,512
intro9.html	3,395

Filename	**File size (bytes)**
ix.xml	43,350
modify.html	3,956
modify2.html	5,429
modify3.html	4,672
modify4.html	4,399
modify5.html	4,820
modify6.html	5,710
modify7.html	4,289
modify8.html	5,449
modify9.html	3,913
preconfig.html	3,862
preconfig2.html	8,956
preconfig3.html	4,143
preconfig4.html	5,660
preconfig5.html	7,144
preconfig6.html	6,676
preconfig7.html	7,707
pubad.pdf	2,024,414
sysconfig.html	3,252
sysconfig2.html	4,792
sysconfig3.html	5,214
sysconfig4.html	3,955
sysconfig5.html	3,381
sysconfig6.html	6,017
sysconfig7.html	5,203
sysconfig8.html	3,660
sysconfig9.html	3,651
testing.html	3,454
testing2.html	3,844
testing3.html	3,634
testing4.html	3,576
toc.xml	12,338
Files in D:\docs\pubadmin\images	
apm_cainfo.gif	9,317
apm_casourcepubretries.gif	12,030
apm_config_main.gif	32,385
apm_config_main_completed.gif	19,561
apm_directories.gif	3,475
apm_directoryentryattr.gif	15,350
apm_eecertadd.gif	15,049
apm_eecertmodify.gif	15,118
apm_flowchart.gif	50,052
apm_leafnode.gif	11,627
apm_postingpreferences.gif	14,986
apm_pubfilterconfig.gif	11,556
apm_pubfiltercrls_rip.gif	6,076
apm_pubinstance.gif	5,093
apm_pubnoticesrecords.gif	13,954
apm_sysconfigtab.gif	14,541
apm_upcertfile.gif	5,850
bullet.gif	822
caution.gif	1,533
connconfigmgr.gif	12,376
dbconnconfig.gif	8,847
dbconnconfig_full.gif	9,308
info.gif	1,155
ldapserverconfigdsam.gif	9,221
logo.gif	2,524
ocspconfigmgr.gif	30,614
ocspsvrconfig.gif	26,634

Filename	File size (bytes)
pubconfigselect.gif	8,823
pubinstanceunicert.gif	5,075
pubnoticesrecordsdcc.gif	16,932
tsconfigmgr.gif	13,656
tssvrconfig.gif	15,634
warn.gif	1,171
Files in D:\docs\pubadmin\wwhdata\common	
context.js	84
files.js	9,618
popups.js	38
title.js	82
topics.js	1,401
towwhdir.js	54
wwhpagef.js	4,505
Files in D:\docs\pubadmin\wwhdata\java	
files.xml	20,157
ix.xml	43,350
search.xml	89,826
toc.xml	12,338
Files in D:\docs\pubadmin\wwhdata\js	
index.js	30,684
search.js	1,687
toc.js	9,413
Files in D:\docs\pubadmin\wwhdata\js\search	
search0.js	16,160
search1.js	16,153
search2.js	16,143
search3.js	16,160
search4.js	16,149
search5.js	15,712
search6.js	2,084
Files in D:\docs\relnotes	
catalog.css	16,757
copyright.html	5,388
document.css	561
introduction.html	3,751
introduction2.html	2,878
introduction3.html	2,864
introduction4.html	3,338
introduction5.html	3,254
issuesresolved.html	2,387
issuesresolved10.html	2,189
issuesresolved11.html	2,480
issuesresolved12.html	2,409
issuesresolved13.html	2,563
issuesresolved14.html	2,635
issuesresolved15.html	2,192
issuesresolved16.html	2,418
issuesresolved17.html	2,986
issuesresolved18.html	2,463
issuesresolved19.html	2,480
issuesresolved2.html	2,659
issuesresolved20.html	2,554
issuesresolved21.html	2,360
issuesresolved22.html	2,533
issuesresolved23.html	3,046
issuesresolved24.html	2,723
issuesresolved25.html	2,508
issuesresolved26.html	2,632
issuesresolved27.html	2,554

Filename	File size (bytes)
issuesresolved28.html	2,424
issuesresolved29.html	2,415
issuesresolved3.html	2,495
issuesresolved30.html	2,216
issuesresolved31.html	2,956
issuesresolved32.html	2,537
issuesresolved33.html	2,408
issuesresolved34.html	2,326
issuesresolved35.html	2,358
issuesresolved36.html	2,425
issuesresolved37.html	2,459
issuesresolved38.html	2,892
issuesresolved39.html	2,360
issuesresolved4.html	2,820
issuesresolved40.html	2,556
issuesresolved41.html	2,404
issuesresolved42.html	2,428
issuesresolved43.html	2,466
issuesresolved44.html	2,694
issuesresolved45.html	2,415
issuesresolved46.html	2,565
issuesresolved47.html	2,210
issuesresolved48.html	2,426
issuesresolved49.html	2,419
issuesresolved5.html	2,396
issuesresolved50.html	2,588
issuesresolved51.html	2,482
issuesresolved52.html	2,442
issuesresolved53.html	2,429
issuesresolved54.html	2,541
issuesresolved55.html	2,363
issuesresolved56.html	2,222
issuesresolved57.html	2,531
issuesresolved58.html	2,403
issuesresolved59.html	2,228
issuesresolved6.html	2,382
issuesresolved60.html	2,428
issuesresolved61.html	2,216
issuesresolved62.html	2,471
issuesresolved63.html	2,219
issuesresolved64.html	2,473
issuesresolved65.html	2,432
issuesresolved66.html	2,590
issuesresolved7.html	2,663
issuesresolved8.html	2,559
issuesresolved9.html	2,624
newfeatures.html	2,286
newfeatures2.html	3,763
newfeatures3.html	2,306
newfeatures4.html	2,378
newfeatures5.html	2,371
newfeatures6.html	2,562
newfeatures7.html	2,614
newfeatures8.html	2,533
newfeatures9.html	2,533
relnotes.pdf	342,191
relnotesIX.xml	4,889
relnotesTOC.xml	6,349
Files in D:\docs\relnotes\images	
bullet.gif	822

Filename	File size (bytes)
caution.gif	1,533
info.gif	1,155
logo.gif	2,524
warn.gif	1,171
Files in D:\docs\relnotes\wwhdata\common	
context.js	66
files.js	4,880
popups.js	38
title.js	64
topics.js	67
towwhdir.js	54
wwhpagef.js	4,505
Files in D:\docs\relnotes\wwhdata\java	
files.xml	11,409
ix.xml	4,889
search.xml	25,336
toc.xml	6,349
Files in D:\docs\relnotes\wwhdata\js	
index.js	3,392
search.js	1,687
toc.js	4,460
Files in D:\docs\relnotes\wwhdata\js\search	
search0.js	16,153
search1.js	12,913
Files in D:\docs\webrao	
about.html	3,392
about10.html	7,146
about11.html	3,492
about12.html	3,437
about2.html	3,287
about3.html	3,809
about4.html	4,186
about5.html	3,949
about6.html	3,636
about7.html	4,148
about8.html	3,192
about9.html	4,236
appendix_identrus.html	2,864
appendix_identrus10.html	5,765
appendix_identrus2.html	3,033
appendix_identrus3.html	6,745
appendix_identrus4.html	7,642
appendix_identrus5.html	3,375
appendix_identrus6.html	5,396
appendix_identrus7.html	5,025
appendix_identrus8.html	4,931
appendix_identrus9.html	10,632
appendix_passphrase.html	3,125
appendixb.html	3,075
appendixb2.html	5,067
appendixb3.html	4,160
appendixc.html	6,682
authorizingrequests.html	3,948
authorizingrequests2.html	12,326
authorizingrequests3.html	10,790
authorizingrequests4.html	10,388
catalog.css	16,757
collecting.html	3,340
collecting10.html	8,648
collecting2.html	3,338

Filename	**File size (bytes)**
collecting3.html	5,733
collecting4.html	5,702
collecting5.html	6,882
collecting6.html	10,322
collecting7.html	5,730
collecting8.html	5,898
collecting9.html	5,259
document.css	561
facetoface.html	4,480
facetoface10.html	7,829
facetoface11.html	3,586
facetoface12.html	4,086
facetoface13.html	8,862
facetoface14.html	4,202
facetoface15.html	3,547
facetoface16.html	4,097
facetoface17.html	3,875
facetoface18.html	8,449
facetoface19.html	4,945
facetoface2.html	3,402
facetoface20.html	5,045
facetoface21.html	4,264
facetoface22.html	4,318
facetoface23.html	7,874
facetoface24.html	4,106
facetoface25.html	4,259
facetoface26.html	7,244
facetoface27.html	4,607
facetoface28.html	5,296
facetoface29.html	3,922
facetoface3.html	7,832
facetoface30.html	3,889
facetoface31.html	8,703
facetoface32.html	5,301
facetoface33.html	4,717
facetoface34.html	4,640
facetoface35.html	5,285
facetoface36.html	4,123
facetoface37.html	3,860
facetoface38.html	4,237
facetoface39.html	6,054
facetoface4.html	3,717
facetoface5.html	5,060
facetoface6.html	5,270
facetoface7.html	4,269
facetoface8.html	4,000
facetoface9.html	4,266
gettingstarted.html	3,700
gettingstarted2.html	4,260
gettingstarted3.html	12,313
gettingstarted4.html	11,240
gettingstarted5.html	3,639
gettingstarted6.html	3,992
installing.html	4,675
installing10.html	4,243
installing11.html	6,820
installing12.html	3,486
installing13.html	4,996
installing14.html	6,201
installing15.html	5,203

Filename	File size (bytes)
installing2.html	4,708
installing3.html	3,790
installing4.html	3,972
installing5.html	5,822
installing6.html	3,115
installing7.html	5,180
installing8.html	6,018
installing9.html	3,795
introduction.html	3,324
introduction2.html	3,659
introduction3.html	4,253
introduction4.html	5,155
introduction5.html	6,394
introduction6.html	3,489
introduction7.html	3,097
introduction8.html	3,138
introduction9.html	4,143
keepingyoursystemsecure.html	3,932
keepingyoursystemsecure2.html	4,386
keepingyoursystemsecure3.html	4,022
keepingyoursystemsecure4.html	3,090
keepingyoursystemsecure5.html	4,889
keepingyoursystemsecure6.html	3,485
recover.html	2,944
recover2.html	3,268
recover3.html	10,521
recover4.html	3,201
suspendingandrevoking.html	3,895
suspendingandrevoking2.html	8,438
suspendingandrevoking3.html	6,358
suspendingandrevoking4.html	3,412
suspendingandrevoking5.html	9,254
suspendingandrevoking6.html	6,520
suspendingandrevoking7.html	5,733
troubleshooting.html	3,817
troubleshooting2.html	3,430
troubleshooting3.html	4,642
troubleshooting4.html	11,919
troubleshooting5.html	3,818
troubleshooting6.html	5,018
troubleshooting7.html	4,195
troubleshooting8.html	3,788
troubleshooting9.html	3,231
webraoguide.pdf	1,786,892
webraoguideIX.xml	36,204
webraoguideTOC.xml	11,499
Files in D:\docs\webrao\images	
appendix_identrusa.gif	46,643
bullet.gif	822
caution.gif	1,533
cert_req_dual_ke_PKCS11.gif	11,409
cert_req_dual_key.gif	11,132
cert_request_sub_authorize.gif	2,466
cert_request_sub_authorize2.gif	2,047
cert_status.gif	5,601
certificate_request_page.gif	8,140
certificate_request_page_PKCS11.gif	8,680
certificate_request_page_import.gif	8,709
certificate_request_recover.gif	5,529
certificate_request_submitted_page.gif	7,457

Filename	File size (bytes)
certificate_request_submitted_page_PKCS11.gif	2,485
certificate_request_submitted_page_authorize.gif	8,683
certificate_request_submitted_page_import.gif	2,523
collect_rro.gif	6,165
export_certificate_screen2.gif	10,022
export_certificate_screen_key1.gif	10,063
facetofacea26.gif	11,888
friendly_name2.gif	7,864
import_certificate_request_page.gif	2,339
import_certificate_request_screen.gif	10,298
info.gif	1,155
install.gif	64,385
key_recov_submitted.gif	2,477
key_recov_submitted_auth.gif	2,537
login_page.gif	6,084
logo.gif	2,524
menu_krowrao.gif	4,446
multi_cert_friendly.gif	9,877
pkcs12_options.gif	15,729
random_data_screen.gif	9,204
recov_key.gif	8,441
recov_key_auth.gif	8,550
recov_request2.gif	6,862
recovery_reasons.gif	2,262
registration_officer_logon_screen.gif	8,347
registration_officer_logon_screen_pkcs11.gif	8,080
request_details.gif	6,017
revocation_dropdown.gif	2,477
revoke_cert_revoke.gif	9,142
revoke_certificate_page.gif	9,504
revoke_certificate_page_suspend.gif	8,825
revoke_certificate_page_unsuspend.gif	10,072
save_cert_p12_drop-down.gif	3,629
save_certificate_page_import.gif	5,811
save_certificate_page_multiple.gif	10,305
save_certificate_page_multiple_PKCS11.gif	15,606
save_certificate_page_p12.gif	11,978
save_certificate_page_pem.gif	12,137
save_certificate_page_smartcard3.gif	8,402
save_key_cert.gif	5,900
saving_keys_and_certificates_screen.gif	13,379
saving_keys_and_certificates_screen_multiple_certificates .gif	8,985
saving_keys_and_certificates_screen_p7c_file.gif	10,049
saving_keys_and_certs_collect.gif	5,866
saving_keys_and_certs_key1.gif	13,655
saving_keys_and_certs_key2.gif	13,794
saving_keys_and_certs_key2_diff_file.gif	13,750
saving_keys_and_certs_recover.gif	13,538
search_criteria_page_authorize.gif	10,585
search_criteria_page_ch_cert_status.gif	10,768
search_criteria_page_collect.gif	9,888
search_criteria_page_collect_keys.gif	9,865
search_criteria_page_recover.gif	9,394
search_criteria_page_revoke.gif	3,743
search_criteria_page_status.gif	3,781
select_certificate_screen_collect.gif	10,793
select_certificate_screen_collect_key.gif	5,324
select_certificate_screen_recover.gif	7,800
select_certificate_screen_status.gif	9,233

Filename	File size (bytes)
select_registration_policy_page.gif	9,686
select_request_page2.gif	7,335
select_request_page3.gif	5,474
select_request_page4.gif	5,456
select_request_status.gif	5,436
smartcard2_ro_screen.gif	7,460
smartcard2_screen.gif	10,225
smartcard3_ro_screen.gif	6,783
smartcard3_screen.gif	6,973
smartcard4_ro_screen.gif	7,305
smartcard4_screen.gif	7,391
status.gif	6,738
warn.gif	1,171
welcome_rro.gif	9,985
Files in D:\docs\webrao\wwhdata\common	
context.js	72
files.js	9,395
popups.js	38
title.js	70
topics.js	67
towwhdir.js	54
wwhpagef.js	4,505
Files in D:\docs\webrao\wwhdata\java	
files.xml	17,133
ix.xml	36,204
search.xml	84,686
toc.xml	11,499
Files in D:\docs\webrao\wwhdata\js	
index.js	23,203
search.js	1,687
toc.js	8,618
Files in D:\docs\webrao\wwhdata\js\search	
search0.js	16,155
search1.js	16,162
search2.js	16,131
search3.js	16,112
search4.js	16,146
search5.js	12,308
Files in D:\docs\wwhelp	
books.xml	698
messages.xml	31,996
settings.xml	3,918
Files in D:\docs\wwhelp\images	
altclose.gif	156
altopen.gif	173
caution.gif	1,533
info.gif	1,155
warn.gif	1,171
Files in D:\docs\wwhelp\wwhimpl	
version.htm	868
Files in D:\docs\wwhelp\wwhimpl\common\html	
blank.htm	336
bookmark.htm	339
catalog.css	16,757
content.htm	1,258
controll.htm	1,413
controlr.htm	1,454
default.htm	4,539
document.css	561
document.htm	1,056

Filename	File size (bytes)
init0.htm	935
init1.htm	1,400
init2.htm	1,098
init3.htm	935
pagenav.htm	1,338
switch.htm	1,379
title.htm	1,138
wwhelp.htm	3,620
Files in D:\docs\wwhelp\wwhimpl\common\images	
bkmark.gif	250
bkmarkx.gif	99
close.gif	214
divider.gif	46
divider2.gif	46
doc.gif	150
email.gif	289
emailx.gif	93
fc.gif	235
fo.gif	174
frameset.gif	234
home.gif	287
logo.jpg	4,851
logocolor.gif	58
next.gif	248
nextx.gif	76
prev.gif	252
prevx.gif	76
print.gif	313
printx.gif	94
related.gif	440
relatedi.gif	95
relatedx.gif	95
spacer4.gif	51
spc1w2h.gif	43
spc1w7h.gif	44
spc2w1h.gif	43
spc5w1h.gif	43
sync.gif	270
syncx.gif	86
Files in D:\docs\wwhelp\wwhimpl\common\private	
books.js	812
locale.js	12,224
options.js	1,594
popupf.js	3,024
title.js	162
Files in D:\docs\wwhelp\wwhimpl\common\scripts	
bklist1s.js	422
bookgrps.js	5,006
booklist.js	7,909
browseri.js	3,482
controls.js	12,842
documt1s.js	190
filelist.js	1,710
handler.js	774
help.js	19,082
highlt.js	5,677
pophash.js	1,456
popup.js	12,897
related.js	13,393
strutils.js	12,383

Filename	**File size (bytes)**
switch.js	5,187
Files in D:\docs\wwhelp\wwhimpl\java\html	
ie60win.htm	2,721
iemac.htm	1,820
iewindow.htm	2,296
netscape.htm	2,238
nosecie.htm	2,097
nosecie6.htm	2,522
nosecns.htm	2,237
wwhelp.htm	4,198
Files in D:\docs\wwhelp\wwhimpl\java\private	
books.xml	776
locale.js	2,690
locale.xml	22,045
options.js	146
options.xml	1,085
Files in D:\docs\wwhelp\wwhimpl\java\scripts	
handler.js	905
java.js	5,431
Files in D:\docs\wwhelp\wwhimpl\js\html	
indexsel.htm	1,167
navigate.htm	1,353
panel.htm	1,568
panelini.htm	1,127
tabs.htm	1,149
wwhelp.htm	4,599
Files in D:\docs\wwhelp\wwhimpl\js\images	
tabsbg.gif	45
Files in D:\docs\wwhelp\wwhimpl\js\private	
locale.js	13,715
options.js	2,696
Files in D:\docs\wwhelp\wwhimpl\js\scripts	
handler.js	475
index.js	44,486
index1s.js	171
javascpt.js	4,355
outlfast.js	6,502
outlin1s.js	167
outline.js	23,298
outlsafe.js	5,483
panels.js	6,663
search.js	33,500
search1s.js	341
search2s.js	147
search3s.js	142
search4s.js	142
tabs.js	3,713

Table A-1 – UniCERT Core v5.2.1 Documentation Files for Windows

A.2 UniCERT WebRAO Client v5.2.1 for Windows

Filename	**File size (bytes)**
Files in D:\docs	
webraoindex.htm	955
webraoreadme.html	6,913
wwhelp3.cab	120,586
wwhelp3.jar	192,132
Files in D:\docs\users	

Filename	File size (bytes)
about.html	3,392
about10.html	7,146
about11.html	3,492
about12.html	3,437
about2.html	3,287
about3.html	3,809
about4.html	4,186
about5.html	3,949
about6.html	3,636
about7.html	4,148
about8.html	3,192
about9.html	4,236
appendix_identrus.html	2,864
appendix_identrus10.html	5,765
appendix_identrus2.html	3,033
appendix_identrus3.html	6,745
appendix_identrus4.html	7,642
appendix_identrus5.html	3,375
appendix_identrus6.html	5,396
appendix_identrus7.html	5,025
appendix_identrus8.html	4,931
appendix_identrus9.html	10,632
appendix_passphrase.html	3,125
appendixb.html	3,075
appendixb2.html	5,067
appendixb3.html	4,160
appendixc.html	6,682
authorizingrequests.html	3,948
authorizingrequests2.html	12,326
authorizingrequests3.html	10,790
authorizingrequests4.html	10,388
catalog.css	16,757
collecting.html	3,340
collecting10.html	8,648
collecting2.html	3,338
collecting3.html	5,733
collecting4.html	5,702
collecting5.html	6,882
collecting6.html	10,322
collecting7.html	5,730
collecting8.html	5,898
collecting9.html	5,259
copyright.html	5,363
document.css	561
facetoface.html	4,480
facetoface10.html	7,829
facetoface11.html	3,586
facetoface12.html	4,086
facetoface13.html	8,862
facetoface14.html	4,202
facetoface15.html	3,547
facetoface16.html	4,097
facetoface17.html	3,875
facetoface18.html	8,449
facetoface19.html	4,945
facetoface2.html	3,402
facetoface20.html	5,045
facetoface21.html	4,264
facetoface22.html	4,318
facetoface23.html	7,874
facetoface24.html	4,106
facetoface25.html	4,259

Filename	File size (bytes)
facetoface26.html	7,244
facetoface27.html	4,607
facetoface28.html	5,296
facetoface29.html	3,922
facetoface3.html	7,832
facetoface30.html	3,889
facetoface31.html	8,703
facetoface32.html	5,301
facetoface33.html	4,717
facetoface34.html	4,640
facetoface35.html	5,285
facetoface36.html	4,123
facetoface37.html	3,860
facetoface38.html	4,237
facetoface39.html	6,054
facetoface4.html	3,717
facetoface5.html	5,060
facetoface6.html	5,270
facetoface7.html	4,269
facetoface8.html	4,000
facetoface9.html	4,266
gettingstarted.html	3,700
gettingstarted2.html	4,260
gettingstarted3.html	12,313
gettingstarted4.html	11,240
gettingstarted5.html	3,639
gettingstarted6.html	3,992
installing.html	4,675
installing10.html	4,243
installing11.html	6,820
installing12.html	3,486
installing13.html	4,996
installing14.html	6,201
installing15.html	5,203
installing2.html	4,200
installing3.html	3,790
installing4.html	3,729
installing5.html	5,580
installing6.html	3,115
installing7.html	5,180
installing8.html	6,018
installing9.html	3,795
introduction.html	3,324
introduction2.html	3,659
introduction3.html	4,252
introduction4.html	5,155
introduction5.html	6,394
introduction6.html	3,489
introduction7.html	3,097
introduction8.html	3,138
introduction9.html	4,143
keepingyoursystemsecure.html	3,932
keepingyoursystemsecure2.html	4,386
keepingyoursystemsecure3.html	4,022
keepingyoursystemsecure4.html	3,090
keepingyoursystemsecure5.html	4,889
keepingyoursystemsecure6.html	3,485
recover.html	2,944
recover2.html	3,268
recover3.html	10,521
recover4.html	3,201
suspendingandrevoking.html	3,895

Filename	File size (bytes)
suspendingandrevoking2.html	8,438
suspendingandrevoking3.html	6,358
suspendingandrevoking4.html	3,412
suspendingandrevoking5.html	9,254
suspendingandrevoking6.html	6,520
suspendingandrevoking7.html	5,733
troubleshooting.html	3,817
troubleshooting2.html	3,430
troubleshooting3.html	4,642
troubleshooting4.html	11,919
troubleshooting5.html	3,818
troubleshooting6.html	5,018
troubleshooting7.html	4,195
troubleshooting8.html	3,788
troubleshooting9.html	3,231
webraoguide.pdf	1,811,916
webraoguideIX.xml	36,204
webraoguideTOC.xml	11,499
Files in D:\docs\users\images	
appendix_identrusa.gif	46,643
bullet.gif	822
caution.gif	1,533
cert_req_dual_ke_PKCS11.gif	11,409
cert_req_dual_key.gif	11,132
cert_request_sub_authorize.gif	2,466
cert_request_sub_authorize2.gif	2,047
cert_status.gif	5,601
certificate_request_page.gif	8,140
certificate_request_page_PKCS11.gif	8,680
certificate_request_page_import.gif	8,709
certificate_request_recover.gif	5,529
certificate_request_submitted_page.gif	7,457
certificate_request_submitted_page_PKCS11.gif	2,485
certificate_request_submitted_page_authorize.gif	8,683
certificate_request_submitted_page_import.gif	2,523
collect_rro.gif	6,165
export_certificate_screen2.gif	10,022
export_certificate_screen_key1.gif	10,063
facetofacea26.gif	11,888
friendly_name2.gif	7,864
import_certificate_request_page.gif	2,339
import_certificate_request_screen.gif	10,298
info.gif	1,155
install.gif	64,385
key_recov_submitted.gif	2,477
key_recov_submitted_auth.gif	2,537
login_page.gif	6,084
logo.gif	2,524
menu_krowrao.gif	4,446
multi_cert_friendly.gif	9,877
pkcs12_options.gif	15,729
random_data_screen.gif	9,204
recov_key.gif	8,441
recov_key_auth.gif	8,550
recov_request2.gif	6,862
recovery_reasons.gif	2,262
registration_officer_logon_screen.gif	8,347
registration_officer_logon_screen_pkcs11.gif	8,080
request_details.gif	6,017
revocation_dropdown.gif	2,477
revoke_cert_revoke.gif	9,142
revoke_certificate_page.gif	9,504

Filename	File size (bytes)
revoke_certificate_page_suspend.gif	8,825
revoke_certificate_page_unsuspend.gif	10,072
save_cert_p12_drop-down.gif	3,629
save_certificate_page_import.gif	5,811
save_certificate_page_multiple.gif	10,305
save_certificate_page_multiple_PKCS11.gif	15,606
save_certificate_page_p12.gif	11,978
save_certificate_page_pem.gif	12,137
save_certificate_page_smartcard3.gif	8,402
save_key_cert.gif	5,900
saving_keys_and_certificates_screen.gif	13,379
saving_keys_and_certificates_screen_multiple_certificates.gif	8,985
saving_keys_and_certificates_screen_p7c_file.gif	10,049
saving_keys_and_certs_collect.gif	5,866
saving_keys_and_certs_key1.gif	13,655
saving_keys_and_certs_key2.gif	13,794
saving_keys_and_certs_key2_diff_file.gif	13,750
saving_keys_and_certs_recover.gif	13,538
search_criteria_page_authorize.gif	10,585
search_criteria_page_ch_cert_status.gif	10,768
search_criteria_page_collect.gif	9,888
search_criteria_page_collect_keys.gif	9,865
search_criteria_page_recover.gif	9,394
search_criteria_page_revoke.gif	3,743
search_criteria_page_status.gif	3,781
select_certificate_screen_collect.gif	10,793
select_certificate_screen_collect_key.gif	5,324
select_certificate_screen_recover.gif	7,800
select_certificate_screen_status.gif	9,233
select_registration_policy_page.gif	9,686
select_request_page2.gif	7,335
select_request_page3.gif	5,474
select_request_page4.gif	5,456
select_request_status.gif	5,436
smartcard2_ro_screen.gif	7,460
smartcard2_screen.gif	10,225
smartcard3_ro_screen.gif	6,783
smartcard3_screen.gif	6,973
smartcard4_ro_screen.gif	7,305
smartcard4_screen.gif	7,391
status.gif	6,738
warn.gif	1,171
welcome_rro.gif	9,985
Files in D:\docs\users\wwhdata\common	
context.js	72
files.js	9,328
popups.js	38
title.js	70
topics.js	67
towwhdir.js	54
wwhpagef.js	4,505
Files in D:\docs\users\wwhdata\java	
files.xml	17,045
ix.xml	36,204
search.xml	84,207
toc.xml	11,499
Files in D:\docs\users\wwhdata\js	
index.js	23,203
search.js	1,687
toc.js	8,618
Files in D:\docs\users\wwhdata\js\search	
search0.js	16,142

Filename	**File size (bytes)**
search1.js	16,152
search2.js	16,151
search3.js	16,125
search4.js	16,149
search5.js	11,781
Files in D:\docs\wwhelp	
books.xml	246
messages.xml	31,996
settings.xml	3,918
Files in D:\docs\wwhelp\images	
altclose.gif	156
altopen.gif	173
caution.gif	1,533
info.gif	1,155
warn.gif	1,171
Files in D:\docs\wwhelp\wwhimpl	
version.htm	868
Files in D:\docs\wwhelp\wwhimpl\common\html	
blank.htm	336
bookmark.htm	339
catalog.css	16,757
content.htm	1,258
controll.htm	1,413
controlr.htm	1,454
default.htm	4,602
document.css	561
document.htm	1,056
init0.htm	935
init1.htm	1,400
init2.htm	1,098
init3.htm	935
pagenav.htm	1,338
switch.htm	1,379
title.htm	1,138
wwhelp.htm	3,620
Files in D:\docs\wwhelp\wwhimpl\common\images	
bkmark.gif	250
bkmarkx.gif	99
close.gif	214
divider.gif	46
divider2.gif	46
doc.gif	150
email.gif	289
emailx.gif	93
fc.gif	235
fo.gif	174
frameset.gif	234
home.gif	287
logo.jpg	4,851
next.gif	248
nextx.gif	76
prev.gif	252
prevx.gif	76
print.gif	313
printx.gif	94
related.gif	440
relatedi.gif	95
relatedx.gif	95
spacer4.gif	51
spc1w2h.gif	43
spc1w7h.gif	44
spc2w1h.gif	43

Filename	File size (bytes)
spc5w1h.gif	43
sync.gif	270
syncx.gif	86
Files in D:\docs\wwhelp\wwhimpl\common\private	
books.js	318
locale.js	12,224
options.js	1,589
popupf.js	3,024
title.js	158
Files in D:\docs\wwhelp\wwhimpl\common\scripts	
bklist1s.js	422
bookgrps.js	5,006
booklist.js	7,909
browseri.js	3,482
controls.js	12,842
documt1s.js	190
filelist.js	1,710
handler.js	774
help.js	19,082
highlt.js	5,677
pophash.js	1,456
popup.js	12,897
related.js	13,393
strutils.js	12,383
switch.js	5,187
Files in D:\docs\wwhelp\wwhimpl\java\html	
ie60win.htm	2,721
iemac.htm	1,820
iewindow.htm	2,296
netscape.htm	2,238
nosecie.htm	2,097
nosecie6.htm	2,522
nosecns.htm	2,237
wwhelp.htm	4,198
Files in D:\docs\wwhelp\wwhimpl\java\private	
books.xml	234
locale.js	2,690
locale.xml	22,045
options.js	146
options.xml	1,085
Files in D:\docs\wwhelp\wwhimpl\java\scripts	
handler.js	905
java.js	5,431
Files in D:\docs\wwhelp\wwhimpl\js\html	
indexsel.htm	1,167
navigate.htm	1,353
panel.htm	1,568
panelini.htm	1,127
tabs.htm	1,149
wwhelp.htm	4,599
Files in D:\docs\wwhelp\wwhimpl\js\images	
tabsbg.gif	45
Files in D:\docs\wwhelp\wwhimpl\js\private	
locale.js	13,715
options.js	2,696
Files in D:\docs\wwhelp\wwhimpl\js\scripts	
handler.js	475
index.js	44,486
index1s.js	171
javascpt.js	4,355
outlfast.js	6,502
outlin1s.js	167

Filename	File size (bytes)
outline.js	23,298
outlsafe.js	5,483
panels.js	6,663
search.js	33,500
search1s.js	341
search2s.js	147
search3s.js	142
search4s.js	142
tabs.js	3,713

Table A-2 – UniCERT WebRAO Client v5.2.1 Documentation Files for Windows

A.3 UniCERT Core v5.2.1 for Solaris

Filename	File size (bytes)
Files in /docs	
index.htm	920
readme.html	38,513
thirdpartylicense.txt	9,615
wwhelp3.cab	120,586
wwhelp3.jar	192,132
Files in /docs/admin	
admin.pdf	1,297,569
adminIX.xml	25,120
adminTOC.xml	5,398
catalog.css	15,962
dbw.html	3,298
dbw2.html	4,271
dbw3.html	10,784
dbw4.html	5,058
dbw5.html	8,859
dbw6.html	8,249
dbw7.html	9,276
dbw8.html	5,555
dbw9.html	5,361
document.css	534
introducing.html	3,533
introducing2.html	3,422
introducing3.html	14,658
keymgr.html	3,566
keymgr2.html	5,356
keymgr3.html	4,013
keymgr4.html	5,661
keymgr5.html	4,057
ralog.html	5,827
ralog10.html	7,418
ralog11.html	4,064
ralog12.html	4,009
ralog13.html	3,296
ralog14.html	3,650
ralog15.html	4,256
ralog2.html	6,025
ralog3.html	3,083
ralog4.html	2,810
ralog5.html	16,730
ralog6.html	3,240
ralog7.html	3,306
ralog8.html	3,263
ralog9.html	5,092
servicestr.html	5,315

Filename	File size (bytes)
servicestr10.html	3,833
servicestr11.html	2,952
servicestr2.html	4,614
servicestr3.html	10,512
servicestr4.html	4,258
servicestr5.html	3,270
servicestr6.html	2,380
servicestr7.html	4,377
servicestr8.html	4,807
servicestr9.html	4,320
tokenmgr.html	4,527
tokenmgr10.html	4,704
tokenmgr11.html	5,529
tokenmgr12.html	3,855
tokenmgr13.html	3,953
tokenmgr14.html	6,230
tokenmgr15.html	4,193
tokenmgr16.html	4,713
tokenmgr17.html	4,205
tokenmgr18.html	3,745
tokenmgr19.html	4,471
tokenmgr2.html	5,384
tokenmgr20.html	4,275
tokenmgr21.html	3,577
tokenmgr22.html	3,034
tokenmgr23.html	3,949
tokenmgr24.html	3,019
tokenmgr25.html	2,809
tokenmgr26.html	2,918
tokenmgr27.html	3,754
tokenmgr28.html	2,980
tokenmgr3.html	4,811
tokenmgr4.html	3,930
tokenmgr5.html	4,526
tokenmgr6.html	3,999
tokenmgr7.html	8,760
tokenmgr8.html	6,448
tokenmgr9.html	5,480
Files in /docs/admin/images	
ab.gif	881
auditarchive.gif	7,201
bullet.gif	822
caution.gif	1,533
dbw_1Logon.gif	8,097
dbw_2dbw.gif	11,087
dbw_APM1.gif	7,210
dbw_APM2.gif	13,373
dbw_APM3.gif	14,661
dbw_CA2.gif	13,104
dbw_CAO2.gif	13,751
dbw_UpPass1.gif	13,265
dbw_button_RefreshList.gif	1,567
dbw_button_create.gif	1,614
dbw_button_delete.gif	1,627
dbw_button_lock.gif	1,662
dbw_ca1.gif	6,976
dbw_ca3.gif	14,075
dbw_cao1.gif	7,270
delete.gif	862
filteringlog.gif	3,805
filteringlog2.gif	4,062
iconconfigure.gif	910

Filename	File size (bytes)
info.gif	1,155
keygen_01.gif	37,653
keygen_05.gif	34,323
keygen_06.gif	35,763
keygen_07.gif	7,785
logo.gif	2,524
new.gif	877
newquery2.gif	2,583
querylog.gif	5,189
querylog2.gif	13,626
querylogeg.gif	4,649
querylogview.gif	11,038
rev_dblogon.gif	11,230
rev_logresult.gif	14,726
rev_mainscr.gif	10,196
rev_open.gif	13,528
rev_pseopen.gif	4,227
warn.gif	1,171
Files in /docs/admin/wwhdata/common	
context.js	70
files.js	4,212
popups.js	35
title.js	68
topics.js	62
towwhdir.js	50
wwhpagef.js	4,299
Files in /docs/admin/wwhdata/java	
files.xml	10,458
ix.xml	25,120
search.xml	46,367
toc.xml	5,398
Files in /docs/admin/wwhdata/js	
index.js	18,719
search.js	1,575
toc.js	4,243
Files in /docs/admin/wwhdata/js/search	
search0.js	15,797
search1.js	15,799
search2.js	15,830
search3.js	4,725
Files in /docs/config	
CRLs.html	3,656
CRLs2.html	3,839
CRLs3.html	5,106
app_whcustom.html	3,703
app_whcustom10.html	4,630
app_whcustom11.html	4,230
app_whcustom12.html	2,844
app_whcustom13.html	4,363
app_whcustom14.html	8,016
app_whcustom15.html	4,615
app_whcustom2.html	4,033
app_whcustom3.html	4,622
app_whcustom4.html	7,103
app_whcustom5.html	5,435
app_whcustom6.html	5,532
app_whcustom7.html	7,237
app_whcustom8.html	9,690
app_whcustom9.html	11,712
appendixa.html	27,583
arm.html	3,736
arm10.html	3,470

Filename	File size (bytes)
arm11.html	4,038
arm12.html	5,057
arm13.html	3,342
arm2.html	4,304
arm3.html	3,145
arm4.html	3,181
arm5.html	3,467
arm6.html	3,660
arm7.html	3,234
arm8.html	3,458
arm9.html	3,827
ca.html	7,733
ca10.html	3,838
ca11.html	4,787
ca12.html	3,298
ca13.html	8,716
ca14.html	2,879
ca15.html	3,716
ca16.html	3,705
ca17.html	3,306
ca18.html	3,675
ca19.html	3,569
ca2.html	4,391
ca20.html	5,867
ca21.html	3,863
ca22.html	3,444
ca23.html	4,207
ca24.html	2,988
ca25.html	3,597
ca3.html	3,908
ca4.html	3,765
ca5.html	4,382
ca6.html	5,674
ca7.html	4,408
ca8.html	4,754
ca9.html	3,692
cao.html	3,258
cao.pdf	4,622,060
cao2.html	7,359
cao3.html	3,160
cao4.html	3,836
cao5.html	2,934
cao6.html	3,251
caoIX.xml	86,248
caoTOC.xml	23,509
catalog.css	15,962
certificates.html	4,571
certificates10.html	4,263
certificates11.html	3,315
certificates12.html	4,071
certificates13.html	4,611
certificates14.html	6,179
certificates15.html	4,912
certificates16.html	7,742
certificates2.html	3,965
certificates3.html	14,091
certificates4.html	5,624
certificates5.html	3,021
certificates6.html	2,888
certificates7.html	3,615
certificates8.html	4,006
certificates9.html	4,434

Filename	File size (bytes)
clone.html	5,048
clone2.html	2,791
clone3.html	4,096
clone4.html	3,373
clone5.html	3,731
crosscert.html	6,093
crosscert2.html	4,142
crosscert3.html	4,297
css.html	4,543
css2.html	4,370
css3.html	3,385
definingrps.html	4,058
definingrps10.html	5,163
definingrps11.html	4,713
definingrps12.html	4,804
definingrps13.html	6,264
definingrps14.html	6,339
definingrps15.html	4,492
definingrps16.html	5,459
definingrps17.html	4,345
definingrps18.html	3,726
definingrps19.html	5,955
definingrps2.html	3,519
definingrps20.html	9,448
definingrps21.html	4,124
definingrps22.html	5,041
definingrps23.html	5,645
definingrps24.html	4,364
definingrps25.html	15,320
definingrps26.html	5,119
definingrps27.html	4,122
definingrps28.html	4,434
definingrps29.html	4,233
definingrps3.html	5,782
definingrps30.html	4,765
definingrps31.html	3,907
definingrps32.html	3,020
definingrps33.html	3,682
definingrps34.html	5,452
definingrps35.html	3,256
definingrps36.html	3,462
definingrps37.html	2,859
definingrps38.html	6,712
definingrps39.html	4,392
definingrps4.html	2,972
definingrps40.html	3,973
definingrps41.html	2,924
definingrps42.html	5,045
definingrps43.html	3,670
definingrps44.html	3,929
definingrps45.html	3,167
definingrps46.html	3,629
definingrps47.html	3,926
definingrps48.html	3,179
definingrps49.html	4,657
definingrps5.html	5,767
definingrps50.html	4,168
definingrps51.html	3,144
definingrps6.html	3,803
definingrps7.html	4,595
definingrps8.html	4,452
definingrps9.html	3,350

Filename	File size (bytes)
document.css	534
introduction.html	5,467
introduction2.html	6,675
introduction3.html	6,275
introduction4.html	3,635
kao.html	4,957
kao2.html	5,031
kao3.html	4,610
kao4.html	3,267
kao5.html	3,772
kas.html	5,872
kas2.html	3,898
kas3.html	10,017
kas4.html	5,186
kas5.html	4,195
kas6.html	3,494
kas7.html	4,161
logs.html	5,730
logs10.html	2,679
logs11.html	3,310
logs12.html	3,380
logs2.html	17,082
logs3.html	3,082
logs4.html	3,330
logs5.html	2,977
logs6.html	4,987
logs7.html	9,173
logs8.html	4,499
logs9.html	3,341
ph.html	7,388
ph10.html	5,148
ph11.html	7,690
ph12.html	3,907
ph13.html	4,605
ph14.html	3,741
ph15.html	4,623
ph16.html	4,342
ph17.html	3,606
ph18.html	3,856
ph19.html	5,432
ph2.html	3,436
ph20.html	5,762
ph21.html	6,177
ph22.html	5,497
ph23.html	6,675
ph24.html	5,744
ph3.html	2,823
ph4.html	2,718
ph5.html	8,170
ph6.html	4,202
ph7.html	4,290
ph8.html	3,598
ph9.html	10,000
pki.html	5,915
pki2.html	4,780
pki210.html	7,767
pki211.html	3,423
pki22.html	5,451
pki23.html	9,618
pki24.html	7,360
pki25.html	11,062
pki26.html	7,376

Filename	File size (bytes)
pki27.html	5,689
pki28.html	7,013
pki29.html	3,636
pki2a.html	3,640
pki3.html	9,087
pki4.html	5,947
pki5.html	8,764
pki6.html	8,886
pki7.html	12,167
pki8.html	3,507
pki9.html	6,147
ra.html	6,633
ra2.html	4,026
ra3.html	4,721
ra4.html	5,722
ra5.html	4,097
ra6.html	3,765
ra7.html	3,507
raa.html	6,464
raa2.html	5,059
raa3.html	2,698
rax.html	3,316
rax2.html	6,102
rax3.html	3,148
rax4.html	3,404
rax5.html	4,141
rax6.html	5,300
rax7.html	6,400
renew.html	6,369
renew10.html	7,999
renew11.html	9,766
renew12.html	4,873
renew13.html	8,827
renew14.html	9,439
renew15.html	4,902
renew16.html	8,937
renew17.html	10,322
renew18.html	9,246
renew19.html	12,463
renew2.html	3,670
renew20.html	7,824
renew21.html	3,923
renew22.html	6,851
renew23.html	16,830
renew24.html	4,876
renew25.html	3,872
renew26.html	3,495
renew27.html	3,911
renew28.html	9,629
renew29.html	6,296
renew3.html	5,142
renew30.html	11,183
renew31.html	4,464
renew4.html	4,692
renew5.html	4,453
renew6.html	6,708
renew7.html	5,778
renew8.html	4,284
renew9.html	3,236
rp.html	4,973
rp10.html	4,744
rp11.html	4,431

Filename	File size (bytes)
rp12.html	3,577
rp13.html	3,957
rp14.html	4,520
rp15.html	3,342
rp16.html	4,166
rp17.html	4,953
rp18.html	4,499
rp2.html	3,486
rp3.html	4,790
rp4.html	6,319
rp5.html	4,325
rp6.html	3,856
rp7.html	10,556
rp8.html	7,077
rp9.html	4,976
subCA.html	3,836
subCA2.html	3,801
subCA3.html	7,287
subCA4.html	4,246
subCA5.html	5,338
tasks.html	8,448
tasks2.html	3,923
tasks3.html	3,613
tasks4.html	3,106
tasks5.html	3,282
tasks6.html	3,135
tasks7.html	3,945
troubleshoot.html	3,814
troubleshoot2.html	2,755
troubleshoot3.html	3,236
troubleshoot4.html	3,428
troubleshoot5.html	2,814
troubleshoot6.html	4,145
troubleshoot7.html	3,612
troubleshoot8.html	3,394
troubleshoot9.html	3,131
webrao.html	3,972
webrao2.html	4,328
webrao3.html	5,035
webrao4.html	3,945
webrao5.html	3,686
webrao6.html	3,210
webrao7.html	3,328
webrao8.html	3,127
wh.html	5,358
wh10.html	3,004
wh11.html	5,875
wh12.html	12,368
wh13.html	6,276
wh14.html	4,391
wh15.html	4,719
wh16.html	6,163
wh2.html	4,954
wh3.html	4,801
wh4.html	3,350
wh5.html	4,836
wh6.html	4,296
wh7.html	3,396
wh8.html	7,505
wh9.html	2,946
Files in /docs/config/images	
ab.gif	881

Filename	File size (bytes)
addcdp.gif	5,981
addedcdp.gif	16,098
addentity.gif	5,420
alignspace.gif	6,850
apptype.gif	6,644
armlog.gif	8,853
armsda.gif	8,165
armtuning.gif	6,280
auditarchive.gif	7,201
auditdeletion.gif	35,700
authgroup.gif	3,652
authgrouptab.gif	3,701
bullet.gif	822
cacerts.gif	12,566
cacommunicate.gif	3,975
cacrl.gif	14,582
cadb.gif	2,891
caentityname.gif	12,725
cajob.gif	5,899
camiscellaneous.gif	7,690
caoaccess.gif	13,730
caotune.gif	23,511
caserverparam.gif	10,852
catune.gif	8,675
caution.gif	1,533
cert_request_ee.gif	18,108
certificate.gif	6,791
certificate_request_page.gif	8,991
certificateinstall.gif	9,081
certificatesa15.gif	1,115
certquery.gif	5,272
certtype.gif	2,305
choose.gif	37,081
choosepol.gif	34,026
choosepolicy.gif	26,030
cmpmode.gif	7,981
cmpreg.gif	16,551
cmprp.gif	12,762
cmptrust.gif	3,212
cmptune.gif	9,253
collection.gif	5,845
color.gif	2,834
columns.gif	6,086
combobox.gif	4,612
combobox2.gif	1,402
composequery.gif	13,335
connected.gif	1,166
cq_icon1.gif	157
cq_icon2.gif	166
crlgentime.gif	5,014
crosscerta.gif	8,150
cryptoprofile2.gif	11,045
csstune.gif	22,962
database.gif	3,758
delete.gif	862
deletiondetect.gif	4,819
dnelements.gif	24,623
dnorder.gif	4,034
dnvalue.gif	4,396
dnwindow.gif	4,523
dsapara.gif	4,893
editbox.gif	1,523

Filename	File size (bytes)
email.gif	13,648
emailadd.gif	9,606
emailnotification.gif	13,611
emailpemtags.gif	14,209
emailreg.gif	12,238
emailrp.gif	5,737
emailtemplate.gif	13,769
emailtemplate1.gif	11,187
emailtune.gif	15,086
entitiespki.gif	16,375
entityreq.gif	28,719
exportcrl.gif	7,987
exportcrl2.gif	8,550
filtering.gif	3,722
filtering2.gif	4,019
filteringlog.gif	3,805
filteringlog2.gif	4,062
fingeprint.gif	1,505
fingerprintalg.gif	4,574
form.gif	26,888
generateca.gif	28,249
genkeys.gif	38,427
grouptab.gif	5,348
iconcert.gif	928
iconconfigure.gif	910
iconerror.gif	890
iconrevoke.gif	935
icontask.gif	914
icontask2.gif	882
iddata.gif	13,847
importext.gif	12,420
info.gif	1,155
kaoaccess.gif	9,642
kaotuning.gif	6,092
kastuning.gif	10,891
keystore.gif	12,215
ldapuri.gif	3,364
ldapuriadv.gif	6,860
lisktuning.gif	4,903
lock.gif	940
logcolumns.gif	3,876
logo.gif	2,524
logoptions.gif	6,891
logresult.gif	12,520
logsa.gif	5,947
mainscreen.gif	10,939
mapped.gif	2,220
multkeys.gif	2,980
nested.gif	33,159
new.gif	877
newpolicy.gif	22,704
newquery.gif	5,775
newquery2.gif	2,583
newtemplate.gif	2,990
openpki.gif	4,571
openpki1.gif	5,650
pkia.gif	4,143
policyinfo.gif	21,255
policylife.gif	18,149
policymap.gif	14,351
policyscope.gif	3,987
policytab.gif	12,986

Filename	File size (bytes)
policytab1.gif	5,388
pselocate.gif	9,448
publication.gif	10,509
querylog.gif	5,189
querylog2.gif	13,626
querylogeg.gif	4,649
querylogview.gif	11,038
queryresult.gif	9,091
raaaccess.gif	7,961
ratasks.gif	22,092
ratune.gif	23,802
rax2eh.gif	8,853
rax2scepcmp.gif	11,440
rax2webrao.gif	21,115
rax2wh.gif	8,220
raxaccess.gif	18,259
raxaccess2.gif	18,597
raxtune.gif	13,216
received.gif	35,763
remote.gif	5,595
remove.gif	5,381
renewalrules.gif	5,323
renewcomplete.gif	10,922
renewcomplete2.gif	33,136
renewcomplete3.gif	11,105
renewcompletekeygen.gif	53,365
renewdecisions.gif	59,915
reneweditpolicy.gif	31,245
renewencrypt.gif	32,916
renewexport.gif	32,694
renewmulticert.gif	46,059
renewpkientity.gif	33,735
renewpolicy.gif	33,050
renewpse.gif	11,000
renewrootca1.gif	33,397
renewrootreuse.gif	33,121
renewsubCAdetails.gif	33,397
renewsubatroot1.gif	32,280
renewsubcaexport.gif	32,910
renewsubcaexport2.gif	32,753
renewsubcagrayout.gif	32,974
renewsubcaimport.gif	31,614
renewsubcapolicy.gif	33,555
renewsubcomplete.gif	10,978
renewsubkeygen.gif	5,900
renewsubmit.gif	33,097
renewsubp10.gif	9,415
renewsubreuse.gif	45,499
renewsubreuse2.gif	46,807
request.gif	21,847
requestnotify.gif	3,978
requestsum.gif	21,824
retire.gif	891
retire_unpub.gif	117
retirecdp.gif	3,531
retiregroup.gif	4,544
revoke.gif	5,715
revokentity.gif	5,546
rootcert.gif	7,177
rpproperties1.gif	9,313
rpproperties2.gif	12,204
rpproperties3.gif	10,472

Filename	**File size (bytes)**
rpproperties4.gif	9,500
rpproperties6.gif	10,782
rpproperties7.gif	11,437
ruleeg.gif	4,884
scep.gif	7,997
scepreg.gif	9,867
sceprp.gif	13,176
sceptune.gif	25,194
search_criteria_ee.gif	2,843
staticlist.gif	7,162
subca2.gif	34,309
subca3.gif	34,039
subca4.gif	28,052
submit.gif	35,171
suspend.gif	5,668
taborder.gif	3,592
tasksa.gif	17,832
tick.gif	882
titleurl.gif	1,201
unassigned.gif	915
unassigned2.gif	930
unsuspend.gif	5,838
viewevent.gif	5,749
warn.gif	1,171
Files in /docs/config/wwhdata/common	
context.js	68
files.js	18,244
popups.js	35
title.js	66
topics.js	62
towwhdir.js	50
wwhpagef.js	4,299
Files in /docs/config/wwhdata/java	
files.xml	29,799
ix.xml	86,248
search.xml	191,535
toc.xml	23,509
Files in /docs/config/wwhdata/js	
index.js	64,630
search.js	1,576
toc.js	18,978
Files in /docs/config/wwhdata/js/search	
search0.js	15,879
search1.js	15,900
search10.js	15,953
search11.js	15,504
search12.js	15,949
search13.js	1,055
search2.js	15,913
search3.js	15,900
search4.js	15,856
search5.js	15,938
search6.js	15,950
search7.js	15,857
search8.js	15,759
search9.js	15,216
Files in /docs/dbadmin	
catalog.css	15,962
dba_1b_changes.html	4,207
dba_1b_changes2.html	3,565
dba_1b_changes3.html	3,952
dba_1b_changes4.html	2,901

Filename	File size (bytes)
dba_1b_changes5.html	3,727
dba_1intro.html	2,818
dba_1intro2.html	6,089
dba_1intro3.html	4,536
dba_2ainstalloraclewindows.html	3,267
dba_2ainstalloraclewindows2.html	4,619
dba_2ainstalloraclewindows3.html	3,624
dba_2ainstalloraclewindows4.html	10,595
dba_2ainstalloraclewindows5.html	3,718
dba_2ainstalloraclewindows6.html	7,227
dba_2binstalloraclesolaris.html	3,266
dba_2binstalloraclesolaris2.html	4,619
dba_2binstalloraclesolaris3.html	3,399
dba_2binstalloraclesolaris4.html	8,983
dba_2binstalloraclesolaris5.html	9,981
dba_2binstalloraclesolaris6.html	3,718
dba_2binstalloraclesolaris7.html	7,297
dba_3acreate_dbwindows.html	3,747
dba_3acreate_dbwindows2.html	4,448
dba_3acreate_dbwindows3.html	18,627
dba_3acreate_dbwindows4.html	4,244
dba_3acreate_dbwindows5.html	6,227
dba_3bcreate_dbsolaris.html	3,470
dba_3bcreate_dbsolaris2.html	4,295
dba_3bcreate_dbsolaris3.html	18,617
dba_3bcreate_dbsolaris4.html	4,177
dba_4arunningoracle_windows.html	3,220
dba_4arunningoracle_windows2.html	6,087
dba_4arunningoracle_windows3.html	3,538
dba_4arunningoracle_windows4.html	4,178
dba_4arunningoracle_windows5.html	8,568
dba_4arunningoracle_windows6.html	5,249
dba_4brunningoracle_solaris.html	3,221
dba_4brunningoracle_solaris2.html	4,331
dba_4brunningoracle_solaris3.html	6,636
dba_4brunningoracle_solaris4.html	5,351
dba_4brunningoracle_solaris5.html	4,059
dba_4brunningoracle_solaris6.html	5,466
dba_4brunningoracle_solaris7.html	3,067
dba_4brunningoracle_solaris8.html	3,061
dba_4brunningoracle_solaris9.html	4,280
dba_5amorelisteners_windows.html	2,723
dba_5amorelisteners_windows2.html	7,660
dba_5bmorelisteners_solaris.html	2,725
dba_5bmorelisteners_solaris2.html	7,932
dba_6amorealiases_windows.html	3,200
dba_6amorealiases_windows2.html	8,997
dba_6bmorealiases_solaris.html	3,201
dba_6bmorealiases_solaris2.html	8,926
dba_7ahomeselector_windows.html	4,873
dba_8adbtranstion_windows.html	2,907
dba_8adbtranstion_windows2.html	4,180
dba_8adbtranstion_windows3.html	8,358
dba_8adbtranstion_windows4.html	8,031
dba_8bdbtranstion_solaris.html	2,904
dba_8bdbtranstion_solaris2.html	3,983
dba_8bdbtranstion_solaris3.html	8,782
dba_8bdbtranstion_solaris4.html	7,845
dba_appauto.html	2,952
dba_appauto2.html	2,485
dba_appauto3.html	3,721
dba_appauto4.html	7,299

Filename	File size (bytes)
dba_appbackup.html	3,158
dba_appbackup2.html	3,335
dba_appbackup3.html	3,492
dba_appbackup4.html	3,264
dba_appbackup5.html	3,212
dba_appbackup6.html	6,651
dba_appbackup7.html	4,877
dba_appbackup8.html	3,354
dba_appdbastudio_solaris.html	4,187
dba_appdbastudio_solaris2.html	3,430
dba_appdbastudio_solaris3.html	5,683
dba_appdbastudio_solaris4.html	3,444
dba_appdbastudio_windows.html	4,187
dba_appdbastudio_windows2.html	3,434
dba_appdbastudio_windows3.html	5,567
dba_appdbastudio_windows4.html	3,450
dba_appdelete.html	3,404
dba_appdelete2.html	4,124
dba_appdelete3.html	8,115
dba_apporadir.html	3,536
dba_apporadir2.html	3,009
dba_apporadir3.html	3,598
dba_apporadir4.html	4,380
dba_apporadir5.html	3,517
dba_apporadir6.html	3,262
dbadminguide.pdf	2,338,682
dbadminguideIX.xml	24,243
dbadminguideTOC.xml	8,235
document.css	534
Files in /docs/dbadmin/images	
099.summary.gif	33,520
099.summary_sol.gif	29,055
bullet.gif	822
caution.gif	1,533
db_config_ora_services.gif	15,241
db_upgrade_backup6_solaris.gif	39,047
db_upgrade_backup6_windows.gif	39,029
db_upgrade_database2.gif	42,242
db_upgrade_database2_sol.gif	42,266
db_upgrade_export_summary7_sol.gif	15,253
db_upgrade_export_summary7_wind.gif	15,060
db_upgrade_progress8.gif	42,122
db_upgrade_results9_sol.gif	21,658
db_upgrade_results9_win.gif	21,498
db_upgrade_rollback_issue4.gif	7,465
db_upgrade_temp.gif	5,579
db_upgrade_welcome1.gif	48,954
dbconfig92_archive_all_init_param.gif	11,201
dbconfig92_create_options.gif	7,315
dbconfig92_create_options_sol.gif	7,322
dbconfig92_db_storage_logs_gen.gif	13,815
dbconfig92_db_storage_logs_gen_sol.gif	13,828
dbconfig92_dbfeatures6.gif	6,212
dbconfig92_dbident4.gif	4,162
dbconfig92_dbtemplates3.gif	5,403
dbconfig92_init_param_archive.gif	9,428
dbconfig92_init_param_archive_sol.gif	9,486
dbconfig92_init_param_charset.gif	6,631
dbconfig92_init_param_dbsize.gif	5,549
dbconfig92_init_param_fileloc.gif	10,269
dbconfig92_init_param_fileloc_sol.gif	11,361
dbconfig92_initparam_mem9.gif	9,301

Filename	File size (bytes)
dbconfig92_messagefeatures7.gif	4,532
dbconfig92db_conoptions8.gif	5,830
dbconfig_passwords.gif	9,319
dbconfig_passwords_sol.gif	9,371
dbconfig_progress.gif	30,703
dbconfig_summary_92.gif	17,116
dbconfig_summary_92_sol.gif	17,121
delete_user.gif	28,698
home_selector1.gif	20,583
home_selector2.gif	20,594
home_selector3.gif	11,653
home_selector4.gif	7,978
info.gif	1,155
install92_avail_prod4.gif	79,097
install92_db_config7.gif	77,824
install92_file_loc3_sol.gif	78,552
install92_file_loc3_win.gif	77,135
install92_install_types4.gif	80,408
install92_install_types4_sol.gif	41,920
install92_mts8.gif	75,523
install92_progress10.gif	93,207
install92_rootsh_command_sol.gif	5,622
install92_rootsh_sol.gif	3,538
install_name.gif	2,059
logo.gif	2,524
lstnrctl.gif	9,549
net8asst_tns0008.gif	2,742
net8asst_tns0009.gif	6,212
netmgr_add_list_name.gif	2,216
netmgr_alias_protocol3.gif	8,723
netmgr_alias_protocol_settings4.gif	9,269
netmgr_alias_start1a.gif	15,727
netmgr_alias_test6.gif	10,388
netmgr_alias_test6a.gif	7,863
netmgr_alias_welcome2a.gif	7,739
netmgr_list_loc.gif	10,840
netmgr_lsnr_add_address3.gif	12,355
netmgr_lsnr_add_address3a.gif	8,070
netmgr_lsnr_add_database4.gif	9,492
netmgr_lsnr_add_database4_solaris.gif	9,479
netmgr_lsnr_start1.gif	13,141
oem_add_to_tree5.gif	6,043
oem_adding_uni6.gif	25,153
oem_check_db2.gif	17,055
oem_logged_in4_cropped.gif	21,670
oem_login1.gif	20,154
oem_password_login3.gif	21,010
ora_running.gif	8,150
oracledirectories.gif	4,501
regedit_04_nls_lang.gif	3,038
service_manager.gif	6,998
warn.gif	1,171
Files in D:/docs/dbadmin/wwhdata/common	
context.js	79
files.js	6,984
popups.js	35
title.js	77
topics.js	62
towwhdir.js	50
wwhpagef.js	4,299
Files in /docs/dbadmin/wwhdata/java	
files.xml	13,668

Filename	File size (bytes)
ix.xml	24,243
search.xml	61,358
toc.xml	8,235
Files in /docs/dbadmin/wwhdata/js	
index.js	14,211
search.js	1,575
toc.js	5,500
Files in /docs/dbadmin/wwhdata/js/search	
search0.js	15,817
search1.js	15,798
search2.js	15,817
search3.js	15,843
search4.js	5,361
Files in /docs/exts	
app_certext.html	25,769
app_crlext.html	8,102
app_dn.html	16,806
app_profiles.html	3,956
app_profiles2.html	4,130
app_profiles3.html	5,280
app_profiles4.html	3,721
app_profiles5.html	4,373
app_profiles6.html	5,365
app_profiles7.html	4,751
app_profiles8.html	3,799
catalog.css	15,962
document.css	534
extensions.pdf	1,134,998
extensionsIX.xml	27,777
extensionsTOC.xml	4,659
introx509.html	4,048
introx50910.html	9,578
introx50911.html	6,318
introx5092.html	4,393
introx5093.html	5,622
introx5094.html	6,698
introx5095.html	13,902
introx5096.html	6,136
introx5097.html	4,318
introx5098.html	5,390
introx5099.html	6,186
profile_rp.html	3,491
profile_rp10.html	9,952
profile_rp11.html	26,239
profile_rp2.html	4,470
profile_rp3.html	4,968
profile_rp4.html	4,576
profile_rp5.html	13,463
profile_rp6.html	2,988
profile_rp7.html	3,687
profile_rp8.html	4,263
profile_rp9.html	10,407
set_exts.html	2,933
set_exts10.html	4,552
set_exts11.html	5,544
set_exts12.html	5,535
set_exts13.html	5,624
set_exts14.html	4,631
set_exts15.html	5,120
set_exts16.html	5,250
set_exts17.html	4,014
set_exts18.html	4,690

Filename	File size (bytes)
set_exts19.html	4,928
set_exts2.html	7,742
set_exts20.html	4,266
set_exts21.html	4,524
set_exts22.html	4,275
set_exts23.html	4,379
set_exts24.html	2,484
set_exts25.html	3,712
set_exts26.html	10,321
set_exts27.html	9,433
set_exts28.html	4,101
set_exts29.html	3,427
set_exts3.html	5,113
set_exts30.html	4,317
set_exts31.html	3,781
set_exts32.html	4,022
set_exts33.html	3,308
set_exts4.html	7,805
set_exts5.html	4,109
set_exts6.html	5,244
set_exts7.html	4,756
set_exts8.html	4,209
set_exts9.html	4,370
Files in /docs/exts/images	
bullet.gif	822
caution.gif	1,533
certv3a.gif	54,672
info.gif	1,155
logo.gif	2,524
v2crl.gif	45,662
warn.gif	1,171
Files in /docs/exts/wwhdata/common	
context.js	65
files.js	3,579
popups.js	35
title.js	63
topics.js	62
towwhdir.js	50
wwhpagef.js	4,299
Files in /docs/exts/wwhdata/java	
files.xml	9,710
ix.xml	27,777
search.xml	54,418
toc.xml	4,659
Files in /docs/exts/wwhdata/js	
index.js	19,378
search.js	1,575
toc.js	3,449
Files in /docs/exts/wwhdata/js/search	
search0.js	15,754
search1.js	15,766
search2.js	15,788
search3.js	14,339
Files in /docs/index_topics	
arrow1.gif	1,022
arrow2.gif	1,282
arrow2big.gif	1,415
arrow3.gif	1,550
catalog.css	15,962
document.css	534
install.html	2,688
managing.html	3,054

Filename	**File size (bytes)**
planning.html	2,621
remarks.htm	686,920
running.html	3,201
search.html	1,613
testing.html	3,388
unicert1st.html	3,514
Files in /docs/install	
aboutdocs.html	4,149
aboutdocs10.html	3,221
aboutdocs11.html	3,035
aboutdocs12.html	3,053
aboutdocs13.html	6,978
aboutdocs14.html	3,837
aboutdocs15.html	3,482
aboutdocs16.html	8,390
aboutdocs2.html	4,515
aboutdocs3.html	6,581
aboutdocs4.html	2,918
aboutdocs5.html	2,965
aboutdocs6.html	9,675
aboutdocs7.html	2,941
aboutdocs8.html	2,921
aboutdocs9.html	3,229
catalog.css	15,962
document.css	534
install.pdf	1,364,781
installIX.xml	27,181
installTOC.xml	8,875
instructions.html	5,058
instructions10.html	3,330
instructions11.html	5,039
instructions12.html	4,759
instructions13.html	5,296
instructions14.html	3,922
instructions15.html	3,029
instructions16.html	2,896
instructions17.html	2,853
instructions18.html	2,847
instructions19.html	3,668
instructions2.html	4,482
instructions20.html	6,154
instructions21.html	7,395
instructions22.html	5,186
instructions23.html	3,592
instructions24.html	5,298
instructions25.html	5,147
instructions3.html	3,737
instructions4.html	5,330
instructions5.html	3,932
instructions6.html	5,601
instructions7.html	3,834
instructions8.html	4,971
instructions9.html	7,643
plandeploy.html	5,082
plandeploy2.html	5,490
plandeploy3.html	6,052
plandeploy4.html	5,714
plandeploy5.html	4,027
plandeploy6.html	3,687
plandeploy7.html	3,519
plandeploy8.html	3,779
plandeploy9.html	3,225

Filename	File size (bytes)
prereqs.html	3,466
prereqs10.html	3,116
prereqs11.html	2,571
prereqs12.html	2,595
prereqs13.html	3,420
prereqs14.html	6,850
prereqs15.html	3,065
prereqs16.html	2,845
prereqs17.html	3,749
prereqs18.html	2,803
prereqs19.html	2,972
prereqs2.html	4,608
prereqs20.html	2,687
prereqs21.html	2,731
prereqs3.html	10,654
prereqs4.html	8,265
prereqs5.html	3,781
prereqs6.html	7,760
prereqs7.html	13,812
prereqs8.html	3,296
prereqs9.html	2,798
securepki.html	4,744
securepki10.html	5,570
securepki11.html	6,204
securepki12.html	4,787
securepki13.html	3,180
securepki14.html	3,517
securepki15.html	4,251
securepki16.html	3,688
securepki17.html	4,049
securepki18.html	2,552
securepki19.html	2,929
securepki2.html	6,081
securepki20.html	6,860
securepki21.html	2,871
securepki22.html	4,788
securepki23.html	5,332
securepki24.html	5,520
securepki25.html	9,477
securepki3.html	3,418
securepki4.html	3,230
securepki5.html	3,210
securepki6.html	2,666
securepki7.html	3,106
securepki8.html	2,745
securepki9.html	3,773
webinstructions.html	4,302
webinstructions10.html	6,635
webinstructions11.html	5,879
webinstructions12.html	4,416
webinstructions13.html	5,317
webinstructions14.html	5,501
webinstructions15.html	3,812
webinstructions16.html	3,231
webinstructions17.html	7,191
webinstructions18.html	3,602
webinstructions19.html	3,457
webinstructions2.html	5,599
webinstructions20.html	3,829
webinstructions3.html	3,878
webinstructions4.html	5,124
webinstructions5.html	3,563

Filename	**File size (bytes)**
webinstructions6.html	4,981
webinstructions7.html	3,967
webinstructions8.html	5,986
webinstructions9.html	5,027
Files in /docs/install/images	
bullet.gif	822
caution.gif	1,533
deployVPN2.gif	55,428
deploydemo_unix.gif	13,354
docdiagram.gif	69,368
hostarchitect.gif	41,193
hostca.gif	47,556
info.gif	1,155
init_install.gif	80,923
installxp.gif	31,684
logo.gif	2,524
securepkia.gif	59,063
warn.gif	1,171
webcomps.gif	17,576
Files in /docs/install/wwhdata/common	
context.js	67
files.js	6,885
popups.js	35
title.js	65
topics.js	62
towwhdir.js	50
wwhpagef.js	4,299
Files in /docs/install/wwhdata/java	
files.xml	14,070
ix.xml	27,181
search.xml	75,128
toc.xml	8,875
Files in /docs/install/wwhdata/js	
index.js	19,342
search.js	1,575
toc.js	6,587
Files in /docs/install/wwhdata/js/search	
search0.js	15,793
search1.js	15,780
search2.js	15,793
search3.js	15,804
search4.js	15,817
search5.js	5,448
Files in /docs/overview	
beginners.html	3,376
beginners10.html	3,884
beginners11.html	4,283
beginners12.html	5,083
beginners13.html	4,499
beginners14.html	4,786
beginners15.html	7,221
beginners16.html	8,932
beginners2.html	4,234
beginners3.html	6,051
beginners4.html	3,467
beginners5.html	3,340
beginners6.html	3,646
beginners7.html	5,979
beginners8.html	3,171
beginners9.html	4,523
catalog.css	15,962
certificates.html	3,002

Filename	File size (bytes)
certificates2.html	3,783
certificates3.html	5,960
certificates4.html	5,461
certificates5.html	4,529
certificates6.html	4,249
certificates7.html	4,002
certreq.html	3,609
certreq2.html	5,999
certreq3.html	5,585
certreq4.html	5,092
certreq5.html	5,541
certreq6.html	6,165
document.css	534
glossary.html	64,904
introduction.html	5,222
introduction10.html	5,684
introduction11.html	4,309
introduction12.html	4,016
introduction13.html	6,246
introduction14.html	4,143
introduction15.html	5,543
introduction16.html	6,937
introduction17.html	7,578
introduction18.html	4,391
introduction19.html	3,943
introduction2.html	3,748
introduction20.html	4,096
introduction3.html	6,268
introduction4.html	3,719
introduction5.html	3,545
introduction6.html	3,266
introduction7.html	3,944
introduction8.html	3,589
introduction9.html	4,043
overview.pdf	1,025,625
overviewIX.xml	22,719
overviewTOC.xml	5,627
pki_entities.html	3,598
pki_entities10.html	3,316
pki_entities11.html	3,340
pki_entities12.html	3,142
pki_entities13.html	3,198
pki_entities14.html	3,408
pki_entities15.html	4,003
pki_entities16.html	4,428
pki_entities17.html	5,053
pki_entities18.html	3,504
pki_entities19.html	2,969
pki_entities2.html	6,402
pki_entities20.html	3,505
pki_entities21.html	5,387
pki_entities22.html	4,680
pki_entities23.html	4,501
pki_entities24.html	3,668
pki_entities25.html	5,946
pki_entities26.html	3,826
pki_entities27.html	4,148
pki_entities28.html	3,734
pki_entities3.html	3,596
pki_entities4.html	3,386
pki_entities5.html	4,180
pki_entities6.html	3,510

Filename	File size (bytes)
pki_entities7.html	4,263
pki_entities8.html	3,242
pki_entities9.html	3,837
Files in /docs/overview/images	
bullet.gif	822
caution.gif	1,533
certprocess.gif	37,841
certtemplate.gif	21,953
gui_ex.gif	23,231
info.gif	1,155
laddertrust.gif	14,553
logo.gif	2,524
meetinmiddle.gif	16,070
pkiarch.gif	27,456
warn.gif	1,171
Files in /docs/overview/wwhdata/common	
context.js	65
files.js	4,297
popups.js	35
title.js	63
topics.js	62
towwhdir.js	50
wwhpagef.js	4,299
Files in /docs/overview/wwhdata/java	
files.xml	10,680
ix.xml	22,719
search.xml	82,119
toc.xml	5,627
Files in /docs/overview/wwhdata/js	
index.js	16,058
search.js	1,575
toc.js	4,044
Files in /docs/overview/wwhdata/js/search	
search0.js	15,746
search1.js	15,757
search2.js	15,740
search3.js	15,755
search4.js	15,779
search5.js	14,674
Files in /docs/pubadmin	
addprofile.html	3,351
addprofile10.html	7,392
addprofile11.html	4,134
addprofile12.html	3,297
addprofile13.html	3,526
addprofile14.html	6,594
addprofile15.html	3,120
addprofile16.html	4,156
addprofile17.html	3,790
addprofile18.html	3,398
addprofile19.html	2,890
addprofile2.html	7,591
addprofile20.html	5,819
addprofile21.html	4,339
addprofile22.html	5,000
addprofile23.html	4,674
addprofile24.html	8,621
addprofile25.html	3,589
addprofile26.html	3,831
addprofile27.html	8,766
addprofile28.html	3,222
addprofile29.html	6,336

Filename	File size (bytes)
addprofile3.html	3,892
addprofile30.html	3,739
addprofile31.html	2,865
addprofile32.html	2,873
addprofile33.html	9,353
addprofile34.html	4,248
addprofile35.html	10,031
addprofile36.html	3,443
addprofile37.html	3,156
addprofile38.html	3,583
addprofile39.html	3,453
addprofile4.html	3,794
addprofile40.html	2,816
addprofile41.html	3,012
addprofile42.html	3,722
addprofile43.html	4,443
addprofile44.html	4,063
addprofile45.html	4,888
addprofile46.html	6,137
addprofile47.html	6,637
addprofile48.html	4,212
addprofile49.html	8,430
addprofile5.html	5,589
addprofile50.html	10,619
addprofile51.html	5,203
addprofile52.html	3,749
addprofile53.html	4,742
addprofile54.html	8,214
addprofile55.html	5,061
addprofile56.html	4,389
addprofile57.html	3,628
addprofile58.html	3,245
addprofile59.html	3,253
addprofile6.html	3,780
addprofile60.html	3,774
addprofile61.html	4,164
addprofile62.html	3,637
addprofile63.html	4,388
addprofile64.html	3,858
addprofile65.html	3,041
addprofile66.html	2,771
addprofile67.html	3,324
addprofile68.html	3,306
addprofile69.html	4,200
addprofile7.html	5,487
addprofile70.html	4,277
addprofile71.html	4,515
addprofile8.html	3,817
addprofile9.html	4,549
appx_aipa.html	5,544
appx_ldap.html	3,540
appx_ldap10.html	3,474
appx_ldap11.html	10,452
appx_ldap12.html	6,135
appx_ldap13.html	8,850
appx_ldap14.html	3,561
appx_ldap15.html	4,564
appx_ldap16.html	8,217
appx_ldap17.html	3,461
appx_ldap18.html	3,597
appx_ldap19.html	9,005
appx_ldap2.html	4,919

Filename	File size (bytes)
appx_ldap20.html	3,294
appx_ldap21.html	4,781
appx_ldap22.html	5,610
appx_ldap3.html	3,581
appx_ldap4.html	6,059
appx_ldap5.html	3,507
appx_ldap6.html	7,266
appx_ldap7.html	10,303
appx_ldap8.html	7,023
appx_ldap9.html	3,524
appx_ocsp.html	3,518
appx_ocsp2.html	6,112
appx_ocsp3.html	6,391
appx_trouble.html	3,587
appx_trouble2.html	2,679
appx_trouble3.html	4,040
appx_trouble4.html	13,372
catalog.css	15,962
crosscerts.html	3,424
crosscerts2.html	3,374
crosscerts3.html	5,801
document.css	534
emailtemplates.html	4,021
emailtemplates2.html	5,687
emailtemplates3.html	5,584
intro.html	4,098
intro10.html	3,338
intro11.html	4,390
intro12.html	3,651
intro13.html	3,260
intro14.html	3,209
intro15.html	3,468
intro16.html	3,066
intro17.html	3,280
intro18.html	4,860
intro19.html	5,532
intro2.html	3,913
intro20.html	4,511
intro21.html	4,248
intro22.html	5,332
intro23.html	3,690
intro24.html	6,801
intro25.html	3,512
intro3.html	5,754
intro4.html	6,247
intro5.html	3,868
intro6.html	3,241
intro7.html	3,334
intro8.html	3,436
intro9.html	3,319
ix.xml	41,294
modify.html	3,873
modify2.html	5,327
modify3.html	4,582
modify4.html	4,315
modify5.html	4,737
modify6.html	5,618
modify7.html	4,205
modify8.html	5,353
modify9.html	3,829
preconfig.html	3,775
preconfig2.html	8,191

Filename	File size (bytes)
preconfig3.html	4,061
preconfig4.html	5,578
preconfig5.html	7,023
preconfig6.html	6,450
preconfig7.html	4,236
pubad.pdf	1,961,650
sysconfig.html	3,176
sysconfig2.html	4,426
sysconfig3.html	5,121
sysconfig4.html	3,868
sysconfig5.html	3,288
sysconfig6.html	5,459
sysconfig7.html	5,106
sysconfig8.html	3,582
sysconfig9.html	3,573
testing.html	3,379
testing2.html	3,749
testing3.html	3,540
testing4.html	3,479
toc.xml	12,060
Files in /docs/pubadmin/images	
apm_cainfo.gif	9,317
apm_casourcepubretries.gif	12,030
apm_config_main.gif	32,385
apm_config_main_completed.gif	19,561
apm_directories.gif	3,475
apm_directoryentryattr.gif	15,350
apm_eecertadd.gif	15,049
apm_eecertmodify.gif	15,118
apm_flowchart.gif	49,937
apm_leafnode.gif	11,634
apm_postingpreferences.gif	14,986
apm_pubfilterconfig.gif	11,556
apm_pubfiltercrls_rip.gif	6,076
apm_pubinstance.gif	5,093
apm_pubnoticesrecords.gif	13,954
apm_sysconfigtab.gif	14,541
apm_upcertfile.gif	5,850
bullet.gif	822
caution.gif	1,533
connconfigmgr.gif	12,376
dbconnconfig.gif	8,847
dbconnconfig_full.gif	9,308
info.gif	1,155
ldapserverconfigdsam.gif	9,221
logo.gif	2,524
mainmenu.gif	7,644
ocspconfigmgr.gif	30,614
ocspsvrconfig.gif	26,634
pubconfigselect.gif	8,823
pubinstanceunicert.gif	5,075
pubnoticesrecordsdcc.gif	16,932
tsconfigmgr.gif	13,656
tssvrconfig.gif	15,634
warn.gif	1,171
Files in /docs/pubadmin/wwhdata/common	
context.js	80
files.js	9,393
popups.js	35
title.js	78
topics.js	1,374
towwhdir.js	50

Filename	File size (bytes)
wwhpagef.js	4,299
Files in /docs/pubadmin/wwhdata/java	
files.xml	19,758
ix.xml	41,294
search.xml	87,610
toc.xml	12,060
Files in /docs/pubadmin/wwhdata/js	
index.js	30,021
search.js	1,575
toc.js	9,190
Files in /docs/pubadmin/wwhdata/js/search	
search0.js	15,842
search1.js	15,831
search2.js	15,837
search3.js	15,850
search4.js	15,864
search5.js	15,895
search6.js	1,252
Files in /docs/relnotes	
catalog.css	15,962
copyright.html	5,289
document.css	534
introduction.html	3,670
introduction2.html	2,804
introduction3.html	2,790
introduction4.html	3,264
introduction5.html	3,177
issuesresolved.html	3,236
issuesresolved10.html	2,559
issuesresolved11.html	2,410
issuesresolved12.html	2,127
issuesresolved13.html	2,415
issuesresolved14.html	2,344
issuesresolved15.html	2,498
issuesresolved16.html	2,582
issuesresolved17.html	2,130
issuesresolved18.html	2,353
issuesresolved19.html	2,917
issuesresolved2.html	2,181
issuesresolved20.html	2,410
issuesresolved21.html	2,415
issuesresolved22.html	2,489
issuesresolved23.html	2,295
issuesresolved24.html	2,480
issuesresolved25.html	2,976
issuesresolved26.html	2,670
issuesresolved27.html	2,443
issuesresolved28.html	2,575
issuesresolved29.html	2,489
issuesresolved3.html	2,547
issuesresolved30.html	2,371
issuesresolved31.html	2,350
issuesresolved32.html	2,154
issuesresolved33.html	2,517
issuesresolved34.html	2,472
issuesresolved35.html	2,355
issuesresolved36.html	2,264
issuesresolved37.html	2,305
issuesresolved38.html	2,360
issuesresolved39.html	2,406
issuesresolved4.html	2,430
issuesresolved40.html	2,821

Filename	File size (bytes)
issuesresolved41.html	2,307
issuesresolved42.html	2,491
issuesresolved43.html	2,351
issuesresolved44.html	2,363
issuesresolved45.html	2,626
issuesresolved46.html	2,350
issuesresolved47.html	2,500
issuesresolved48.html	2,148
issuesresolved49.html	2,373
issuesresolved5.html	2,807
issuesresolved50.html	2,366
issuesresolved51.html	2,531
issuesresolved52.html	2,417
issuesresolved53.html	2,377
issuesresolved54.html	2,377
issuesresolved55.html	2,546
issuesresolved56.html	2,499
issuesresolved57.html	2,298
issuesresolved58.html	2,774
issuesresolved59.html	2,466
issuesresolved6.html	2,331
issuesresolved60.html	2,338
issuesresolved61.html	2,414
issuesresolved62.html	2,166
issuesresolved63.html	2,363
issuesresolved64.html	2,154
issuesresolved65.html	2,406
issuesresolved66.html	2,157
issuesresolved67.html	2,377
issuesresolved68.html	2,408
issuesresolved69.html	2,365
issuesresolved7.html	2,317
issuesresolved70.html	2,838
issuesresolved8.html	2,598
issuesresolved9.html	2,510
newfeatures.html	3,134
newfeatures2.html	3,693
newfeatures3.html	2,244
newfeatures4.html	2,634
newfeatures5.html	2,620
newfeatures6.html	2,497
newfeatures7.html	2,549
newfeatures8.html	2,362
newfeatures9.html	2,468
relnotes.pdf	313,019
relnotesIX.xml	4,677
relnotesTOC.xml	6,582
Files in /docs/relnotes/images	
bullet.gif	822
caution.gif	1,533
info.gif	1,155
logo.gif	2,524
warn.gif	1,171
Files in /docs/relnotes/wwhdata/common	
context.js	62
files.js	5,116
popups.js	35
title.js	60
topics.js	62
towwhdir.js	50
wwhpagef.js	4,299
Files in /docs/relnotes/wwhdata/java	

Filename	**File size (bytes)**
files.xml	11,619
ix.xml	4,677
search.xml	26,350
toc.xml	6,582
Files in /docs/relnotes/wwhdata/js	
index.js	3,311
search.js	1,575
toc.js	4,621
Files in /docs/relnotes/wwhdata/js/search	
search0.js	15,535
search1.js	14,796
Files in /docs/webrao	
about.html	3,314
about10.html	6,917
about11.html	3,426
about12.html	3,357
about2.html	3,210
about3.html	3,727
about4.html	4,106
about5.html	3,865
about6.html	3,557
about7.html	4,068
about8.html	3,116
about9.html	4,153
appendix_identrus.html	2,791
appendix_identrus10.html	4,905
appendix_identrus2.html	2,959
appendix_identrus3.html	6,557
appendix_identrus4.html	7,497
appendix_identrus5.html	3,298
appendix_identrus6.html	5,290
appendix_identrus7.html	4,938
appendix_identrus8.html	4,834
appendix_identrus9.html	10,237
appendix_passphrase.html	3,055
appendixb.html	3,006
appendixb2.html	4,979
appendixb3.html	4,079
appendixc.html	6,538
authorizingrequests.html	3,868
authorizingrequests2.html	12,131
authorizingrequests3.html	10,626
authorizingrequests4.html	10,218
catalog.css	15,962
collecting.html	3,264
collecting10.html	8,513
collecting2.html	3,260
collecting3.html	5,631
collecting4.html	5,604
collecting5.html	6,773
collecting6.html	10,127
collecting7.html	5,614
collecting8.html	5,782
collecting9.html	5,130
document.css	534
facetoface.html	4,395
facetoface10.html	7,700
facetoface11.html	3,503
facetoface12.html	4,007
facetoface13.html	8,707
facetoface14.html	4,122
facetoface15.html	3,469

Filename	File size (bytes)
facetoface16.html	4,017
facetoface17.html	3,791
facetoface18.html	8,326
facetoface19.html	4,856
facetoface2.html	3,327
facetoface20.html	4,929
facetoface21.html	4,176
facetoface22.html	4,214
facetoface23.html	7,728
facetoface24.html	4,019
facetoface25.html	4,179
facetoface26.html	7,110
facetoface27.html	4,517
facetoface28.html	5,200
facetoface29.html	3,843
facetoface3.html	7,713
facetoface30.html	3,805
facetoface31.html	8,549
facetoface32.html	5,206
facetoface33.html	4,245
facetoface34.html	4,544
facetoface35.html	5,178
facetoface36.html	4,035
facetoface37.html	3,776
facetoface38.html	4,156
facetoface39.html	5,950
facetoface4.html	3,638
facetoface5.html	4,973
facetoface6.html	5,149
facetoface7.html	4,171
facetoface8.html	3,914
facetoface9.html	4,162
gettingstarted.html	3,617
gettingstarted2.html	4,174
gettingstarted3.html	11,705
gettingstarted4.html	10,676
gettingstarted5.html	3,561
gettingstarted6.html	3,889
installing.html	4,574
installing10.html	4,144
installing11.html	6,495
installing12.html	3,410
installing13.html	4,891
installing14.html	6,102
installing15.html	5,109
installing2.html	4,623
installing3.html	3,716
installing4.html	3,894
installing5.html	5,694
installing6.html	3,028
installing7.html	5,078
installing8.html	5,919
installing9.html	3,700
introduction.html	3,248
introduction2.html	3,584
introduction3.html	4,170
introduction4.html	5,069
introduction5.html	6,090
introduction6.html	3,409
introduction7.html	3,024
introduction8.html	3,065
introduction9.html	4,054

Filename	File size (bytes)
keepingyoursystemsecure.html	3,850
keepingyoursystemsecure2.html	4,300
keepingyoursystemsecure3.html	3,943
keepingyoursystemsecure4.html	3,018
keepingyoursystemsecure5.html	4,790
keepingyoursystemsecure6.html	3,406
recover.html	2,871
recover2.html	3,193
recover3.html	10,335
recover4.html	3,136
suspendingandrevoking.html	3,810
suspendingandrevoking2.html	8,299
suspendingandrevoking3.html	6,238
suspendingandrevoking4.html	3,336
suspendingandrevoking5.html	9,078
suspendingandrevoking6.html	6,402
suspendingandrevoking7.html	5,620
troubleshooting.html	3,740
troubleshooting2.html	3,352
troubleshooting3.html	4,550
troubleshooting4.html	11,380
troubleshooting5.html	3,732
troubleshooting6.html	4,920
troubleshooting7.html	4,103
troubleshooting8.html	3,708
troubleshooting9.html	3,157
webraoguide.pdf	1,769,920
webraoguideIX.xml	35,201
webraoguideTOC.xml	11,326
Files in /docs/webrao/images	
appendix_identrusa.gif	46,643
bullet.gif	822
caution.gif	1,533
cert_req_dual_ke_PKCS11.gif	11,409
cert_req_dual_key.gif	11,132
cert_request_sub_authorize.gif	2,466
cert_request_sub_authorize2.gif	2,047
cert_status.gif	5,601
certificate_request_page.gif	8,140
certificate_request_page_PKCS11.gif	8,680
certificate_request_page_import.gif	8,709
certificate_request_recover.gif	5,529
certificate_request_submitted_page.gif	7,457
certificate_request_submitted_page_PKCS11.gif	2,485
certificate_request_submitted_page_authorize.gif	8,683
certificate_request_submitted_page_import.gif	2,523
collect_rro.gif	6,165
export_certificate_screen2.gif	10,022
export_certificate_screen_key1.gif	10,063
facetofacea26.gif	11,301
friendly_name2.gif	7,864
import_certificate_request_page.gif	2,339
import_certificate_request_screen.gif	10,298
info.gif	1,155
install.gif	64,385
key_recov_submitted.gif	2,477
key_recov_submitted_auth.gif	2,537
login_page.gif	6,084
logo.gif	2,524
menu_krowrao.gif	4,446
multi_cert_friendly.gif	9,877
pkcs12_options.gif	15,729

Filename	File size (bytes)
random_data_screen.gif	9,204
recov_key.gif	8,441
recov_key_auth.gif	8,550
recov_request2.gif	6,862
recovery_reasons.gif	2,262
registration_officer_logon_screen.gif	8,347
registration_officer_logon_screen_pkcs11.gif	8,080
request_details.gif	6,017
revocation_dropdown.gif	2,477
revoke_cert_revoke.gif	9,142
revoke_certificate_page.gif	9,504
revoke_certificate_page_suspend.gif	8,825
revoke_certificate_page_unsuspend.gif	10,072
save_cert_p12_drop-down.gif	3,629
save_certificate_page_import.gif	5,811
save_certificate_page_multiple.gif	10,305
save_certificate_page_multiple_PKCS11.gif	15,606
save_certificate_page_p12.gif	11,978
save_certificate_page_pem.gif	12,137
save_certificate_page_smartcard3.gif	8,402
save_key_cert.gif	5,900
saving_keys_and_certificates_screen.gif	13,379
saving_keys_and_certificates_screen_multiple_certificates.gif	8,985
saving_keys_and_certificates_screen_p7c_file.gif	10,049
saving_keys_and_certs_collect.gif	5,866
saving_keys_and_certs_key1.gif	13,655
saving_keys_and_certs_key2.gif	13,794
saving_keys_and_certs_key2_diff_file.gif	13,750
saving_keys_and_certs_recover.gif	13,538
search_criteria_page_authorize.gif	10,585
search_criteria_page_ch_cert_status.gif	10,768
search_criteria_page_collect.gif	9,888
search_criteria_page_collect_keys.gif	9,865
search_criteria_page_recover.gif	9,394
search_criteria_page_revoke.gif	3,743
search_criteria_page_status.gif	3,781
select_certificate_screen_collect.gif	10,793
select_certificate_screen_collect_key.gif	5,324
select_certificate_screen_recover.gif	7,800
select_certificate_screen_status.gif	9,233
select_registration_policy_page.gif	9,686
select_request_page2.gif	7,335
select_request_page3.gif	5,474
select_request_page4.gif	5,456
select_request_status.gif	5,436
smartcard2_ro_screen.gif	7,460
smartcard2_screen.gif	10,225
smartcard3_ro_screen.gif	6,783
smartcard3_screen.gif	6,973
smartcard4_ro_screen.gif	7,305
smartcard4_screen.gif	7,391
status.gif	6,738
warn.gif	1,171
welcome_rro.gif	9,985
Files in /docs/webrao/wwhdata/common	
context.js	68
files.js	9,256
popups.js	35
title.js	66
topics.js	62
towwhdir.js	50

Filename	File size (bytes)
wwhpagef.js	4,299
Files in /docs/webrao/wwhdata/java	
files.xml	16,863
ix.xml	35,201
search.xml	83,025
toc.xml	11,326
Files in /docs/webrao/wwhdata/js	
index.js	23,010
search.js	1,575
toc.js	8,479
Files in /docs/webrao/wwhdata/js/search	
search0.js	15,817
search1.js	15,837
search2.js	15,818
search3.js	15,875
search4.js	15,872
search5.js	12,113
Files in /docs/wwhelp	
books.xml	685
messages.xml	31,554
settings.xml	3,792
Files in /docs/wwhelp/images	
altclose.gif	156
altopen.gif	173
caution.gif	1,533
info.gif	1,155
warn.gif	1,171
Files in /docs/wwhelp/wwhimpl	
version.htm	838
Files in /docs/wwhelp/wwhimpl/common/html	
blank.htm	323
bookmark.htm	326
content.htm	1,217
controll.htm	1,365
controlr.htm	1,404
default.htm	4,401
document.css	534
document.htm	1,017
init0.htm	901
init1.htm	1,354
init2.htm	1,059
init3.htm	901
pagenav.htm	1,295
switch.htm	1,341
title.htm	1,098
wwhelp.htm	3,532
Files in /docs/wwhelp/wwhimpl/common/images	
bkmark.gif	250
bkmarkx.gif	99
close.gif	214
divider.gif	46
divider2.gif	46
doc.gif	150
email.gif	289
emailx.gif	93
fc.gif	235
fo.gif	174
frameset.gif	234
home.gif	287
logo.jpg	4,851
next.gif	248
nextx.gif	76

Filename	File size (bytes)
prev.gif	252
prevx.gif	76
print.gif	313
printx.gif	94
related.gif	440
relatedi.gif	95
relatedx.gif	95
spacer4.gif	51
spc1w2h.gif	43
spc1w7h.gif	44
spc2w1h.gif	43
spc5w1h.gif	43
sync.gif	270
syncx.gif	86
Files in /docs/wwhelp/wwhimpl/common/private	
books.js	785
locale.js	11,978
options.js	1,541
popupf.js	2,955
title.js	158
Files in /docs/wwhelp/wwhimpl/common/scripts	
bklist1s.js	409
bookgrps.js	4,810
booklist.js	7,619
browseri.js	3,351
controls.js	12,394
documt1s.js	184
filelist.js	1,633
handler.js	742
help.js	18,388
highlt.js	5,499
pophash.js	1,397
popup.js	12,447
related.js	13,055
strutils.js	11,920
switch.js	4,949
Files in /docs/wwhelp/wwhimpl/java/html	
ie60win.htm	2,634
iemac.htm	1,756
iewindow.htm	2,215
netscape.htm	2,156
nosecie.htm	2,020
nosecie6.htm	2,439
nosecns.htm	2,155
wwhelp.htm	4,104
Files in /docs/wwhelp/wwhimpl/java/private	
books.xml	762
locale.js	2,576
locale.xml	21,679
options.js	139
options.xml	1,062
Files in /docs/wwhelp/wwhimpl/java/scripts	
handler.js	867
java.js	5,241
Files in /docs/wwhelp/wwhimpl/js/html	
indexsel.htm	1,122
navigate.htm	1,315
panel.htm	1,510
panelini.htm	1,087
tabs.htm	1,112
wwhelp.htm	4,501
Files in /docs/wwhelp/wwhimpl/js/images	

Filename	File size (bytes)
tabsbg.gif	45
Files in /docs/wwhelp/wwhimpl/js/private	
locale.js	13,315
options.js	2,602
Files in /docs/wwhelp/wwhimpl/js/scripts	
handler.js	450
index.js	42,949
index1s.js	165
javascpt.js	4,179
outlfast.js	6,285
outlin1s.js	161
outline.js	22,438
outlsafe.js	5,294
panels.js	6,473
search.js	32,343
search1s.js	333
search2s.js	141
search3s.js	136
search4s.js	136
tabs.js	3,593

Table A-3 – UniCERT Core v5.2.1 Documentation Files for Solaris

Version History

Version No.	Details	Date of change	Author
5.0.a	Draft	Apr 2002	GeorgeS
5.0.b	Draft	June 2002	GeorgeS
5.0.c	Draft	July 2002	GeorgeS
5.0.d	Draft	Sep 2002	GeorgeS
5.0.e	Draft	Jan 2003	GS,JAF,ML.
5.0.f	Draft	Mar 2003	GS,JAF,ML
5.0.g	First Release for CC Pre-eval	Mar 2003	GS,JAF,ML
5.0.h	Release for entry into ASIEP	April 2003	CL,GS,JAF,ML
5.0.i	Various	May 2003	CL
5.0.j	Addressed comments by DSD and Betrusted, for review and release to evaluators for evaluation.	June 2003	CL
5.0.k	Minor updates while working on other docs	July 2003	CL,GS,JAF,ML
5.0.l	More updates while working on other docs and to address EORs	July 2003	CL,GS,JAF,ML
5.0.m	Second Release to Evaluators (almost!)	July 2003	CL,GS,JAF,ML
5.0.n	Second Release to Evaluators (almost!)	July 2003	CL,GS,JAF,ML
5.0.o	As above	July 2003	CL,GS,JAF,ML
5.0.p	Third Release to Evaluators Reflects updates related to FS and other documents. Addresses EOR14&15.	October 2003	CL,GS,JAF,ML
5.0.q	Incorporate updates from completion of HLD and LLD. Fourth Release to Evaluators	November 2003	CL, GS, JAF, ML
5.0.r	Update to Betrusted and update to synchronise with FS.	Jan 2004	GS
5.0.s	Disassociated unused template so file can open; minor reformatting and changed company refs/logo to Cybertrust (per Mick);	April 2005	NOD
5.0.t	Deleted IA_Identify from the Token Manager description. Deleted IA_Identify and KG_Destroy from the KGU description. Clarified differences between the TM and KGU on Win and Solaris. Updated descriptions of CG_Register and IA_Identify based on other changes described above. Renumbered Nancy's 5.0.2 version to 5.0.s to be consistent with earlier version numbering scheme. Updated version to 5.0.t. Accepted earlier changes, but left latest changes marked for Judy's review.	May 24 2005	GS, ML

Version No.	Details	Date of change	Author
5.0.u	Accepted changes that George and Michael added in last version. Removed DP_Export from RA description. Added KG_Export to KGU description. Updated Web Server, Web Browser and Crypto Module section to reflect current version. Minor editorial changes Updated version to 5.0.u Updated month to June 2005	June 3, 2005	JAF
5.0.v	Updated Luna CA3 information to reflect version used with UniCERT 5.2.1 and what is evaluated. Accepted changes and updated version and date.	July 1, 2005	JAF
5.0.w	Updated description of IA_Identify. Updated version, date and TOC.	July 4, 2005	ML
5.0.x	Updated reference to FIPS 180 and FIPS 186 Updated version and date	July 5, 2005	JAF
5.0.y	Updated reference to PKCS11. Updated definition of PP_PKIVerify to remove verification of the PKI Version number. Updated document version and TOC.	July 29, 2005	ML
5.0.z	Clean up of EORs 19, 23, 32 See change-note 89053 Dublin-1. Minor editorial changes Added note about relationship of Cybertrust and Betrusted Updated month to September 2005	September 2005	GS, JAF,ML
5.0.aa	Updated wording in section 2.5.1.6 per discussion with SafeNet. Updated section 2.3.13.1 to address RFC 13. Minor editorial changes, terminology consistency with user docs. Updated date and version. Added 5.2.1.900 to release version being evaluated and CD file contents (2.6, App A) Accepted changes	December 2005	NOD, JAF
5.0.ab	Removed incorrect references to Windows NT Updated version, publication date and year of copyright.	January 2006	JAF