AUSTRALASIAN INFORMATION SECURITY EVALUATION PROGRAM

Certification Report

Certificate Number: 2003/25

Baltimore Technologies Ltd.

Timestamp Server 2.0.2 Patch 1

Issue 1.0
May 2003

Issued by:

Defence Signals Directorate - Australasian Certification Authority

Executive Summary

This report describes the findings of the evaluation of Timestamp Server version 2.0.2 Patch 1, developed by Baltimore Technologies Ltd., to the Common Criteria (CC) Evaluation Assurance Level EAL3. The report concludes that the product has met the target assurance level of CC EAL3, and includes recommendations by the Australasian Certification Authority (ACA) that are specific to the secure use of the product. The evaluation was performed by CMG and was completed in December 2002.

Timestamp Server 2.0.2 Patch 1 is designed to provide evidence to third parties of the existence of a data item, with an indication of the time at which the data existed. This evidence can be used for time-critical applications such as the submission of a tender, or to indicate the time of transaction for entries in a log. A timestamp server also complements a Public Key Infrastructure by providing the means to verify that a digital signature was applied before the corresponding certificate was revoked. This facilitates the use of a revoked public key certificate for verifying signatures created prior to the time of revocation.

Timestamp Server version 2.0.2 Patch 1 has been found to uphold the claims made in the Security Target (ref [10]), and potential customers are urged to consult this document before planning to implement the product. The scope of the evaluation is described in detail in Chapter 3: Intended Environment for the TOE. The product should be installed and configured to operate according to the evaluated configuration, which is described in Chapter 7: Evaluated Configuration. Details of the requirements for the organisational security policy can be found in Chapter 2: Security Policy, and details of the assumptions that have been made in defining the intended operational environment for Timestamp Server version 2.0.2 Patch 1 can be found in Chapter 3: Intended Environment for the TOE.

Ultimately, it is the responsibility of the user to ensure that Timestamp Server 2.0.2 Patch 1 meets their requirements. For this reason, it is ***strongly*** recommended that prospective users of the product obtain a copy of the Security Target (ref [10]) from the product vendor, and read this Certification Report thoroughly prior to deciding whether to purchase or implement the product.

Please note that certificate 2003/25 for Timestamp Server 2.0.2 Patch 1 supersedes certificate 2001/20 for Timestamp Server 2.0.2. Users that have implemented Timestamp Server 2.0.2 are strongly encouraged to obtain and apply Patch 1 from Baltimore Technologies, and to read this report and the Security Target (ref [10]) to ensure that the product has been implemented correctly according to the evaluated configuration.

Table of Contents

Chapter 1 Introduction

Intended Audience

This certification report states the outcome of the IT security evaluation of Timestamp Server 2.0.2 Patch 1. It is intended to assist potential users when judging the suitability of the product for their particular requirements, and to provide advice to security administrators to ensure that the product is used in a secure manner.

This report should be read in conjunction with the Security Target for Baltimore Timestamp Server version 2.0.2 Patch 1 (ref [10]), which provides a full description of the security requirements and specifications that were used as the basis of the evaluation. A copy of the Security Target can be obtained from Baltimore Technologies, Ltd.

Identification

Table 1 provides identification details for the evaluation. For a detailed description of the hardware and software components included in the evaluated configuration refer to Chapter 7: Evaluated Configuration.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Timestamp Server 2.0.2 Patch 1
Software Version	Version 2.0.2 with Patch 1 applied
Security Target	Security Target for Baltimore Timestamp Server version 2.0.2 Patch 1 Version 2.0.2k, 12 December 2002
Protection Profile Claims	The Security Target does not claim conformance to any PPs
Evaluation Technical Report	Baltimore Timestamp Server v2.0.2 Patch 1 Evaluation Technical Report (ETR), Issue 1.1, December 2002
Evaluation Level	CC EAL 3
Conformance Result	CC Part 2 Conformant CC Part 3 Conformant
Version of CC	CC Version 2.1, August 1999
Version of CEM	CEM-99/045 Version 1.0, August 1999
Sponsor	Baltimore Technologies, Ltd.
Developer	Baltimore Technologies, Ltd.
Evaluation Facility	CMG
Certifier	Kirk Cheney

Description of the TOE

The Target of Evaluation (TOE) is Baltimore's Timestamp Server, which is a PKI/Cryptography standards compliant server for generating digital timestamps in response to requests from remote clients.

The purpose of a timestamping service is to provide evidence to third parties of the existence of a data item, with an indication of the time at which the data existed. This evidence can be used for time-critical applications such as the submission of a tender, or to indicate the time of transaction for entries in a log. A timestamp server also complements a Public Key Infrastructure by providing the means to verify that a digital signature was applied before the corresponding certificate was revoked. This facilitates the use of a revoked public key certificate for verifying signatures created prior to the time of revocation.

A client application sends a request to the Timestamp Server, the content of which conforms to the Internet X.509 Public Key Infrastructure Time Stamp Protocol [RFC3161], over a TCP/IP socket interface. The request message includes a hash of the data to be timestamped, and reference to the required timestamping policy that is supported by a Timestamp Authority within the server. The Timestamp Authority (TSA) is a logical entity within the Timestamp Server that is responsible for issuing a timestamp according to a published policy. The Timestamp Server generates a Timestamp Token in response to this request, which includes the original data and the time that the request was processed. This Timestamp Token is digitally signed by the Timestamp Authority, using Public Key technology, and returned to the requestor. The client is responsible for validating and storing this token as proof of the existence of the data at that time.

The Timestamp Server utilises SHA-1 cryptographic hashes and RSA/DSA digital signing. It supports the PKCS#12 format for software key storage or the PKCS#11 format for storing keys in compliant hardware devices. The cryptographic signing, verification and hashing functions can be performed either in software or by a third party PKCS#11 compliant hardware device. The PKCS#11 hardware device is outside the scope of the evaluation, although it is assumed that any such device used with the Timestamp Server has been evaluated to CC EAL3 or equivalent.

For further information on the specific software components and hardware platforms included in the evaluated configuration refer to Chapter 7: Evaluated Configuration, or Section 2.5 of the Security Target (ref [10]).

Chapter 2 Security Policy

This section outlines the security policies or rules that the TOE must enforce, or comply with, for correct operation.

Organisational Security Policies

The TOE is designed to enforce the following Organisational Security Policies (OSPs):

- **P.Cryptography:** All cryptographic operations (signing and verification) must be implemented by algorithms approved by the National Authority;
- **P.Key_Generation_Destruction:** All cryptographic keys and certificates (TOE Administrator and system related) must be produced and destroyed externally to the TOE by a method approved by the National Authority; and
- **P.Passphrases_PINs:** All passphrases and PINs used to access private keys associated with the TOE (TOE Administrator and system related) must be kept confidential, changed regularly and conform to the requirements set by the National Authority.

The cryptographic functions have been evaluated by the Defence Signals Directorate, as the National Authority for Australia, and found suitable for Australian and New Zealand Government use. For further information, see the Cryptography section in Chapter 9: Recommendations.

TOE Security Policies

The TOE Security Policies (TSPs) define the security policies that the TOE must comply with in order to enforce the organisational security policy and meet the security functional requirements. No TSPs are explicitly defined for the TOE, as they are fully inferred from the definition of the security functions and the requirements on the TOE environment.

Chapter 3 Intended Environment for the TOE

This section outlines the requirements and assumptions that govern the intended environment in which the TOE is designed to operate and for which the TOE has been evaluated, and clarifies the scope of the evaluation. Organisations wishing to implement the TOE in its evaluated configuration should review the evaluation scope to confirm that all the required functionality has been included in the evaluation, and must ensure that any assumed conditions are met in their operational environment.

Secure Usage Assumptions

The evaluation of Timestamp Server 2.0.2 Patch 1 took into account the following assumptions about the secure usage of the TOE:

- It is assumed that the TOE owners are responsible for ensuring that a time source for timestamping is available, and that its reliability and accuracy is acceptable to the TOE owners;
- It is assumed that the TOE operates within a securely managed PKI such that all keys and certificates associated with the TOE are issued and revoked securely and that the status of all keys and certificates are checked prior to their use;
- It is assumed that all private keys used in the operation and administration of the TOE are securely stored to prevent access by persons other than authorised TOE Administrators;
- It is assumed that all Timestamp Server components are located within controlled access facilities that will prevent unauthorised physical access to those components;
- It is assumed that all Timestamp Server components reside on a dedicated network segment and that measures are in place to protect this network from attacks from external networks;
- It is assumed that one or more authorised persons are assigned the responsibility for securely installing and maintaining the TOE in its evaluated configuration, but are not given access to any of the keys associated with the TOE. These are the System Administrators. System Administrators are assumed to be trusted, competent and possess sufficient knowledge and training to carry out their duties. Their duties include:
  - Ensuring that no malicious software is running on the same platform as the TOE or has access to the TOE;
  - Ensuring that there is adequate disk space for the TOE's requirements; and
  - Ensuring that the TOE's databases are properly maintained;

- It is assumed that one or more authorised persons are assigned the responsibility to securely configure and manage the TOE. These are the TOE Administrators. TOE Administrators are assumed to be trusted, competent and possess sufficient knowledge and training to carry out their duties. The following classes of TOE Administrator are defined (a single person may play one or more of these roles):
  - **Bootstrap Administrator:** Initially configures the system during BOOTSTRAP mode, requires access to the Audit Key and Administrator certificates;
  - **TSS Administrator:** Administers the TSS Server, requires access to a TSS Administrator Key; and
  - **TSS Operator:** Starts up the TSS Server, may need to type in passphrase for Audit and/or TSA Keys;

- It is assumed that the Timestamp User (Timestamp Requestor) validates and retains the timestamp token produced. This includes checking, using out-of-band methods, that the TSA certificate has not been revoked and that the timestamp token was signed by the correct TSA, and retaining the timestamp token for non-repudiation evidence; and

- If used, it is assumed that the TOE owners will select a hardware cryptographic device that is approved by the National Authority or evaluated to Common Criteria EAL3 or equivalent, and can:
  - Perform RSA (1024 or 2048 bit) and DSA (1024 bit) signing and verification;
  - Produce a SHA-1 secure hash; and
  - Comply with the PKCS#11 standard.

Clarification of Scope

The scope of the evaluation is limited to those claims made in the Security Target (ref [10]). All security related claims in the Security Target were evaluated by CMG as a component of the evaluation. A summary of the Security Target is provided in Appendix A of this Certification Report.

The TOE is Timestamp Server v2.0.2, with Patch 1 applied after the installation of the Timestamp Server components. The installation of Patch 1 includes procedures to ensure that the host system timezone is set to "(GMT) Casablanca, Monrovia".

The TOE is implemented entirely in software. Hardware components that are required for the operation of Timestamp Server, such as the system clock, network interfaces and optional PKCS#11 hardware cryptography modules, are not part of the TOE, and are beyond the scope of the evaluation. The evaluated configuration for the TOE is given in Chapter 7: Evaluated Configuration.

The components that make up the TOE are described in Chapter 2 of the Security Target (ref [10]).

The TOE provides the following (evaluated) security functionality:

- **Register Administrators:** The set of TOE Administrators that may administer the TOE can only be specified during the Bootstrap process. This list is stored in the configuration parameters file and remains fixed for the duration of the TOE's installation. It may only be viewed from the Administration GUI;

- **Identify Administrator:** The Administration GUI may only be accessed via a login prompt. TOE Administrators identify themselves by specifying details of their private key, which is stored either in a software file or on a hardware device;

- **Authenticate Administrator:** All requests originating from the Administration GUI are digitally signed using the TOE Administrator's private key. The Timestamp Server verifies this signature and authenticates the TOE Administrator prior to carrying out the request;

- **Manage TSAs:** Management of Timestamp Authorities is only possible when the TOE is in Configuration mode. TOE Administrators perform management functions via the Administration GUI;

- **Generate Timestamp:** The Timestamp Server only accepts timestamp requests when in the Timestamping mode of operation. The Timestamp Server generates a timestamp token according to the policy specified in the request, containing the data that was timestamped, the time and date of timestamp and the policy Object Identifier. The TSA associated with the requested policy Object Identifier digitally signs the timestamp token;

- **Register Audit Key:** The Audit key and associated certificate is registered by a TOE Administrator as part of the Bootstrap process. The Audit key cannot be changed at a later time - only its location and passphrase may be modified via the Administration GUI;

- **Events logging:** The Timestamp Server logs all security related events to the Events log;

- **Protect Audit Records:** The Timestamp Server assures the integrity of each security related event record in the Events log, and the existence of the previous record, by signing each record with the Audit key and including in each security related audit record, the hash of the previous record (except the first). This is the hash of the previous security related record's data;

- **Protect Configuration:** The Timestamp Server assures the integrity of the Configuration Parameters File by signing the file with the Audit key. The file is signed upon creation during the Bootstrap process and thereafter every time a change is made to the configuration of the Timestamp Server. The Timestamp Server verifies the Configuration Parameter File's signature every time the system starts. If the file was not signed by the Audit key, execution of the Timestamp Server ceases;

- **Protect Audit Key:** Replacement of the Audit key is prevented by the use of an Audit Key Vault Token (AKVT) - a salted hash of the Audit Key certificate created during the system bootstrap process. The Timestamp Server uses the AKVT to check the integrity of the Audit key every time the system starts. If the Audit key does not match the AKVT, execution of the Timestamp Server ceases;

- **Protect TSA Key(s):** Replacement of the TSA key(s) is prevented by use of the Configuration File and the Audit Key that signs the Configuration file every time it is changed. On startup the TimeStamp Server verifies that the TSA key details match those stored in the Configuration File. If the TSA key does not match, execution of Timestamp Server ceases.

Potential users of the TOE are advised that the following **have not been evaluated** as part of the evaluation of Timestamp Server 2.0.2 Patch 1:

- The TSS Client development kit, TSS Client Timestamp API or any other client software;

- System timezone settings other than "(GMT) Casablanca, Monrovia";

- The reliability of the time source from which the Timestamp Server draws its time information;

- The Oracle database containing the Transaction Logs (although the generation of those logs by the Timestamp Server has been evaluated);

- The operation of Timestamp Server using Oracle version 8.0.5, which is supported by the developer but is not within the scope of the evaluation (the evaluated configuration requires Oracle version 8.1.6);

- Any means of viewing or verifying either the Transaction Log or the Events Log;

- The cryptographic functions provided by PKCS#11 compliant hardware devices, if used; and

- Cryptographic key and certificate generation.

Chapter 4 TOE Architecture

The TOE functionality is implemented entirely in software, with interfaces to hardware devices that are not part of the TOE.

The developer's high level design identifies two functional subsystems of the TOE, which each implement a component of the security functionality. They are described here:

- **TSS Server Administration GUI:** The Administration Utility subsystem controls the identification and authentication of the TOE Administrators; and

- **TSS Server:** The Server subsystem is responsible for controlling all other functions that enforce the TOE security policies. Within the TSS Server subsystem a number of modules have been identified which provide the necessary TSP enforcing functionality:
    - Bootstrap module, which is responsible for registering the administrators and Audit Key and initialising the Event Log and Configuration files;
    - Check Status module, which is responsible for checking the TSA keys and certificates, Audit key and Event Log and Configuration Parameters files;
    - TSS Configuration Manager module, which is responsible for authenticating administrators, creating, modifying and deleting TSAs, modifying the Event Log location, signing the Configuration Parameters file, and viewing the lists of parameters and administrators;
    - TSA / Client Transactions Processing module, which is responsible for generating timestamps;
    - Audit Log module, which is responsible for generating and protecting audit records; and
    - Transaction Logging module, which is responsible for generating the transaction records.

Chapter 5 Documentation

It is important that Timestamp Server version 2.0.2 Patch 1 is used in accordance with the guidance documentation in order to ensure the secure usage of the TOE. The developer provides the following documents with the product:

- UniCERT Extended Technology – Timestamp Server v2.0.2 Administrator's Guide (ref [12]);
- UniCERT Extended Technology – Timestamp Server v2.0.2 Installation Guide (ref [13]);
- UniCERT Extended Technology – Timestamp Server v2.0.2 Release Notes (ref [14]);
- "Readme.txt" file (ref [15]); and
- "TimestampServer2.0.2Patch1_ReadMe.htm" file (ref [16]).

Full documentation for the secure installation of the Timestamp Server v2.0.2 is provided in the Timestamp Server v2.0.2 Installation Guide, referenced above. This document includes some guidance on the installation and configuration of the Oracle database that is required for the correct operation of the TOE, although prior knowledge of the installation and operation of Oracle is required.

The Timestamp Server v2.0.2 Installation Guide does not provide any information relating to the installation of Patch 1. Patch 1 is required to be installed once installation of Timestamp Server v2.0.2 has been completed. Instructions for installing Patch 1 are included in the "TimestampServer2.0.2Patch1_ReadMe.htm" file, which is included on the product CDROM. The "Readme.txt" file, also included on the product CDROM, contains additional information for Administrators, which is intended to be consulted before installing the product. This file includes directions to consult the "TimestampServer2.0.2Patch1_ReadMe.htm" file for instructions for the installation of Patch 1.

Full documentation for the secure administration and operation of the Timestamp Server v2.0.2 are provided in the Timestamp Server v2.0.2 Administration Guide.

No user guidance is included, as users interact with the Timestamp Server through client applications. No installation, operation or user guidance is included relating to client applications, as client applications are not part of the TOE.

Chapter 6 IT Product Testing

The objectives associated with the testing phase of evaluation can be placed into the following categories:

- **Functional testing:** Tests performed to ensure that the TOE operates according to its specification and is able to meet the requirements stated in the Security Target (ref [10]).
- **Penetration testing:** Tests conducted to identify exploitable vulnerabilities in the TOE's intended operational environment.

Functional Testing

In this phase the evaluators analysed evidence of the developer's testing effort, including test coverage and depth analyses, test plans and procedures, and expected and actual results, to gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE. In addition, the evaluators drew on this evidence to develop a set of independent tests, comprising a sample of the developer tests, in order to verify that the test results matched those recorded by the developers, as well as a selection of independent functional tests that expanded on the testing done by the developers.

The evaluators conducted independent testing of the TOE, using a small test network at the evaluation facilities. The test configuration is described in the TOE Configuration for Testing section, below.

The evaluators repeated approximately 57% of the developer's functional tests. The tests were chosen with the intention of repeating at least 50% of the developer's tests for every security function. The results of these evaluator tests were consistent with the actual results recorded by the developers from their own testing.

In addition, the evaluators developed and executed additional functional tests that were not in the developer's test plan.

The results of the evaluator testing effort demonstrate that the security functions of Timestamp Server 2.0.2 Patch 1 operate as expected in the evaluated configuration.

The functions tested covered the full range of Security Functional Requirements identified in the Security Target (ref [10]), with the exception of those that rely on cryptographic operations. Testing of the cryptographic processes is considered the responsibility of the national cryptographic authority. In Australia, the cryptographic functions have been evaluated by the Defence Signals Directorate, as the national authority, and found suitable for Australian and New Zealand Government use. Australian and New Zealand Government users should carefully read the Cryptography section in Chapter 9: Recommendations.

Penetration Testing

The developers performed a vulnerability analysis of Timestamp Server 2.0.2 Patch 1, in order to identify any obvious vulnerabilities in the product and to show that they

are not exploitable in the intended environment for the TOE. This analysis included a search for possible vulnerability sources in the evaluation deliverables, the intended TOE environment and public domain sources. A number of potential vulnerabilities relevant to the product type were identified and in each case the developers were able to show that the vulnerability was not exploitable on the TOE version of the product in the intended environment.

Based on the information given in the developer's vulnerability analysis, the evaluators were able to devise a penetration test plan that would test that the TOE is resistant to penetration, exploiting any of the identified vulnerabilities. In addition, the evaluators identified further independent penetration tests that had not been addressed by the developers. All penetration tests were conducted using the test facilities set up at the evaluators' laboratory, using the test network described in the TOE Configuration for Testing section, below.

Upon completion of the penetration testing activity, the evaluators concluded that the TOE, in its evaluated configuration, did not display any susceptibility to vulnerabilities identified by the developer.

TOE Configuration for Testing

The evaluators conducted testing of the TOE using a small test network consisting of three computers, each with identical hardware that exceeded the minimum requirements, as described in section 2.5 of the Security Target (ref [10]). The computers were connected and configured to communicate using TCP/IP. The three computers were configured as a Timestamp Server, a Timestamp Requestor (client) and an Oracle database server for the Transaction Logs. They were configured with Timestamp Server 2.0.2 Patch 1 on Windows NT Server 4.0 Service Pack 6a, TSS Client Utilities (supplied with Timestamp Server) on Windows NT Workstation 4.0 Service Pack 6a and Oracle 8.1.6 Server on Windows NT Workstation 4.0 Service Pack 6a, respectively.

The TOE was evaluated using both software and hardware cryptographic key storage formats and operations, using the PKCS#11 and PKCS#12 standards. For the purposes of testing, the PKCS#11 compliant device used was a Baltimore Sureware Keyper version 2.1 Professional. The Sureware Keyper Interface software version 2.0 was installed on the Timestamp Server computer to interface with the Keyper device. It should be noted that the Baltimore Sureware Keyper Hardware Security Module was not evaluated to Common Criteria EAL3 or equivalent at the time of testing, as required. However, no device was available at that time that did meet these requirements.

Chapter 7 Evaluated Configuration

Timestamp Server 2.0.2 Patch 1 requires the Windows NT Server 4.0, Service Pack 6a operating system, with TCP/IP networking enabled. The minimum hardware required includes a 350 MHz Pentium II processor and 128 Mb of RAM.

Timestamp Server also requires an Oracle database to be installed, for housing the Transaction Logs, and the product supports Oracle versions 8.0.5 and 8.1.6. However, only Oracle version 8.1.6 is included in the evaluated configuration.

The TCP/IP protocol is used to enable the Timestamp Server to communicate with the Administration Utility, the Oracle database server and the interface to the PKCS#11 hardware cryptographic device. The Oracle server and PKCS#11 device interface have the option of being on the same physical device, or elsewhere within the protected local network. However, the Administration Utility must be installed on the same physical device as the Timestamp Server.

Cryptographic keys and certificates may be provided in either software format (PKCS#12 compliant) or on a hardware device (PKCS#11 compliant). If a PKCS#11 hardware device is used cryptographic operations will be performed on that device. If such a device is not present, or the hardware device does not support the required operations, they will be performed in software. Any PKCS#11 device used with Timestamp Server 2.0.2 Patch 1 must be approved by the National Authority or evaluated to Common Criteria EAL3 or equivalent. The following key usage parameters must be set for certificates used with Timestamp Server:

Table 2: Key Usage Parameters

Key	Parameters
Audit Key	key usage includes: “digitalSignature” and/or “nonRepudiation”
TSA Key(s)	key usage includes: “digitalSignature” extended key usage: “timestamping”
Administrator Key	no key usage necessary

A single implementation of Timestamp Server hosts one or more logically independent Timestamp Authorities (TSAs), each supporting a different timestamping policy, defined by the Object Identifier (OID). These are the entities that process and sign the timestamp requests, which must specify the required OID. Each TSA can have a unique signing key, or may share a key with other TSAs.

Timestamp Server allows administrators to store passphrases for the TSA and Audit keys in the Configuration Parameters file. This functionality is not included in the Evaluated Configuration for the TOE. The evaluated version of Timestamp Server 2.0.2 Patch 1 requires administrators to manually enter the passphrases to unlock the keys each time the Timestamp Server is started.

The evaluated configuration for Timestamp Server 2.0.2 Patch 1 can also be found in section 2.5 of the Security Target (ref [10]).

Procedures for Determining the Evaluated Version of the TOE

When purchasing Timestamp Server 2.0.2 Patch 1 from Baltimore Technologies, Ltd the product will be delivered directly to the customer by a commercial courier. On receipt, customers should ensure that the tamper-evident packaging has not been damaged or opened, and that the package contains a correctly labelled product, and a Consignment Release Form with the correct details noted.

Administrators should ensure that the software correctly reports that it is version 2.0.2. The software will not, however, report whether Patch 1 has been installed.

To verify that Patch 1 is installed, administrators should verify that the file "TSA_Server.dll" in the "ServiceDll" directory is identical to the file of the same name in the compressed file "TimestampServer_2_0_2_Patch_1.zip" on the CDROM. If in doubt, the patch can be safely reinstalled by following the instructions in the "TimestampServer2.0.2Patch1_ReadMe.htm" file on the CDROM.

Chapter 8 Results of the Evaluation

Evaluation Procedures

The evaluation of Timestamp Server version 2.0.2 Patch 1 was conducted using the Common Criteria for Information Technology Security Evaluation (refs [5] to [8]), under the procedures of the Australasian Information Security Evaluation Program (AISEP) (refs [1] to [4]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (ref [9]) were also upheld during the evaluation and certification of this product.

Certification Result

After due consideration of the Evaluation Technical Report (ref [11]) produced by the evaluators and the conduct of the evaluation as witnessed by the certifiers, the Australasian Certification Authority has determined that Timestamp Server version 2.0.2 Patch 1 upholds the claims made in the Security Target (ref [10]) and has met the requirements of the Common Criteria EAL3 assurance level.

Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability that exploitable vulnerabilities remain undiscovered.

Common Criteria EAL3

EAL3 provides assurance by an analysis of the security functions, using a functional and interface specification, guidance documentation, and the high-level design of the TOE, to understand the security behaviour.

The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and high-level design, selective independent confirmation of the developer test results, strength of function analysis, and evidence of a developer search for obvious vulnerabilities (e.g. those in the public domain).

EAL3 also provides assurance through the use of development environment controls, TOE configuration management, and evidence of secure delivery procedures.

A detailed explanation of the assurance requirements for EAL3 can be found in the Common Criteria, Part 3 (ref [7]).

General Observations

The certifiers would like to acknowledge the invaluable assistance provided by CMG and Baltimore Technologies staff during the evaluation. The successful completion of this evaluation was made possible by their cooperation, technical assistance and attention to issues raised during the process.

Chapter 9 Recommendations

The following recommendations include information highlighted by the evaluators during their analysis of the developer's deliverables, during the conduct of the evaluation, and during the additional activities performed by the certifiers.

Scope of the Certificate

This certificate is only valid when Timestamp Server 2.0.2 Patch 1 is installed and configured in its evaluated configuration. The evaluated configuration of Timestamp Server 2.0.2 Patch 1 is described in Chapter 7: Evaluated Configuration, and should be verified on receipt of the delivered product. Users are reminded that Patch 1 must be installed after the installation of Timestamp Server 2.0.2, according to the instructions given in the "TimestampServer2.0.2Patch1_ReadMe.htm" file on the product CDROM.

Timestamp Server 2.0.2 Patch 1 should only be used in accordance with the intended environment described in Chapter 3: Intended Environment for the TOE and Chapter 3 of the Security Target (ref [10]). This includes ensuring that all assumptions identified in the Security Target (ref [10]) are upheld.

Importantly, the evaluated configuration does not include the full functionality offered by Timestamp Server 2.0.2 Patch 1. Potential users of the TOE are advised to consult the Clarification of Scope section, in Chapter 3: Intended Environment for the TOE, for details of which components have been evaluated.

TOE Administration

To ensure the competent administration of the TOE, administrators of the TOE should be trained in Timestamp Server 2.0.2 Patch 1 administration and have sound knowledge of relevant networking protocols. Also, it is the responsibility of the TOE Administrators to ensure that the time source, i.e. system clock, used by Timestamp Server for generating timestamps, is accurate and reliable.

Denial of Service

Administrators should note that the Security Target for Baltimore Timestamp Server version 2.0.2 Patch 1 (ref [10]) does not claim the ability to counter any external threats to the availability of the TOE, therefore the TOE has not been evaluated with regards to resistance to denial of service attacks. Attacks which deny the availability of networking devices are common on public networks, and can be extremely difficult to defend against. Whilst the developers have made every effort to counter known vulnerabilities in the product which could result in a denial of service to legitimate users, administrators should be aware that vulnerabilities of this nature may still be exploitable in the intended environment for the TOE.

Cryptography

The evaluation of the cryptographic functions of Timestamp Server 2.0.2 Patch 1 is beyond the scope of the Common Criteria evaluation, and has been undertaken as a separate process by the Defence Signals Directorate, the national cryptographic authority for Australia. Australian and New Zealand Government users wishing to implement the TOE should take the following recommendations into account when planning their operational environment.

The cryptographic functions of Timestamp Server 2.0.2 Patch 1 have been found to be suitable for Australian Government use, subject to the following recommendations:

- **Audit log security:** Each entry in the Audit Log takes the form of:
  ["prefix"] "data" ["time"] ["hash1"] ["signature"]
  where the "signature" field is a digitally signed hash of the preceding fields, and the "hash1" field is a cryptographic hash of the "data" field from the previous log entry. This provides linkage between successive log entries, reducing the likelihood that log entries could be subsequently removed or altered without any evidence being available. However, it is noted (and recognised in the security target) that these measures do not prevent the last entry, and any number of subsequent entries in the log being deleted, or any blocks of log entries between two entries with identical "data" fields being deleted, without evidence being generated. It is recommended that administrators ensure that the Audit Log file has minimal file-level security permissions assigned to it, in order to ensure that unauthorised users are unable to write to the Audit Log file;

- **Passphrase security:** Timestamp Server 2.0.2 allows the Audit Key and TSA Key passphrases to be stored in the Configuration Parameters file (it is noted that this functionality is not part of the evaluated configuration). Administrators must not select options that allow the passphrases to be stored in the Configuration Parameters file. All passphrases should be entered by the user at the keyboard each time the Timestamp Server starts.

Appendix A Security Target Information

A brief summary of the Security Target (ref [10]) is given below. Potential purchasers should obtain a copy of the full Security Target to ensure that the security enforcing functions meet the requirements of their security policy. A copy of the Security Target can be obtained from Baltimore Technologies Ltd.

Security Objectives for the TOE

Timestamp Server 2.0.2 Patch 1 has the following IT Security Objectives:

- The TOE will ensure that each TOE Administrator is uniquely identified and that the claimed identity is authenticated before the TOE Administrator is granted access to the TOE's security related data;
- The TOE will provide the means for generating and issuing timestamp tokens by binding time information with some given data. The TOE will provide the means for ensuring that timestamp tokens are associated with the identity of the TOE;
- The TOE will provide the means of recording security related events so as to assist a TOE Administrator 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 that allows the TOE Administrator to verify the integrity of the record and to detect if the previous record has been deleted or modified. This does not prevent the case where the last record or records are deleted before a new record is added;
- The TOE will provide the means of preserving the integrity of the TOE's configuration. This includes the configuration data stored in the Configuration Parameters File, and protection of the audit and TSA keys.

Security Objectives for the Environment

Timestamp Server 2.0.2 Patch 1 has the following IT Security Objectives for the environment:

- 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;
- Those responsible for the TOE must ensure that the TOE operates within a securely managed PKI such that all keys and certificates are issued and revoked securely and that the status of all keys and certificates are checked prior to their use;

- Those responsible for the TOE must ensure that all cryptographic operations (signing and verification) have been implemented by algorithms approved by the National Authority;

- Those responsible for the TOE must ensure that any hardware device used with the TSS shall:

  - Perform RSA [1024 or 2048 bit] and DSA [1024 bit] signing and verification;

  - Produce a SHA-1 secure hash;

  - Be compliant with PKCS#11 [PKCS11] standard; and

  - Be approved by the National Authority or evaluated to Common Criteria EAL3 or equivalent for these requirements.

- Those responsible for the TOE must ensure that all cryptographic keys and certificates used in the operation and administration of the TOE have been produced and destroyed by a source approved by the National Authority;

- Those responsible for the TOE must ensure that procedures exist for the selection and management of passphrases and PINs to conform to the requirements set by the National Authority;

- 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;

- Those responsible for the TOE must ensure that those parts of the TOE that are critical to security policy enforcement are protected from physical attack which might compromise IT security;

- Those responsible for the TOE must ensure that no connections are provided from the TOE to outside systems that would undermine IT security;

- Those responsible for the TOE must ensure that all System Administrators are appropriately vetted, possess the required knowledge and receive sufficient training to carry out their duties. System Administrators must ensure that the TOE is installed and maintained in a manner which maintains IT security, as specified in the product documentation;

- Those responsible for the TOE must ensure that all TOE Administrators are appropriately vetted, possess the required knowledge and receive sufficient training to carry out their duties. TOE Administrators must ensure that the TOE is configured and run in a manner which maintains security, as specified in the product documentation;

- The Timestamp Requestor is responsible for validating and retaining the timestamp token produced by the TOE. This includes checking, using out-

of-band methods, that the TSA certificate has not been revoked, and that the timestamp token was signed by the correct TSA. The Timestamp Requestor is assumed to retain the timestamp token for non-repudiation evidence;

- Those responsible for the TOE must provide some management and protection of the audit log, as follows:
  - they must ensure that adequate space is available by archiving and removing old records; and
  - while the TOE provides some protection for the Audit Log, there is also a requirement for the environment to provide some protection. This is because audit records can be deleted starting from the most recent without detection.

Threats

The following threats are addressed by Timestamp Server 2.0.2 Patch 1:

- Persons other than an authorised TOE Administrator gain access to the administration utility by impersonating an authorised TOE Administrator. The attacker would be required to forge or steal an identity and authenticate themselves to the TOE;
- A hacker located on a network external to the TOE's network, and possessing a high level of expertise and resources, impersonates the TOE by forging timestamp tokens;
- The contents of the timestamp produced by the TOE are altered by either the intended recipient of the timestamp or a hacker who intercepts the timestamp destined for its recipient;
- The intended recipient of a timestamp refutes the origin of the timestamp by claiming that it did not come from the TOE. The client would need to modify the signature of the Timestamp token;
- A TOE Administrator makes changes to the configuration of the TOE that is undetected by the TOE. It is subsequently not possible to determine the configuration of the TOE at a given point in time;
- A TOE Administrator inadvertently makes changes to the Events log. It is subsequently not possible to verify the integrity of the log;
- Changes to the Configuration Parameters File - either unintentionally by a TOE Administrator or deliberately by an attacker (persons other than TOE Administrators) - alters the configuration of the TOE. Such changes will not be recorded in the events log. This would require the impersonation of the TOE;

- Replacement of the Audit key - either unintentionally by a TOE Administrator or deliberately by an attacker (persons other than TOE Administrators) - goes undetected. For the Administrator this would require a lack of knowledge of the TOE. For an attacker this would require access to the TOE or TOE network; and

- Replacement of TSA key(s) - either unintentionally by a TOE Administrator or deliberately by an attacker (persons other than TOE Administrators) - goes undetected. For the Administrator this would require a lack of knowledge of the TOE. For an attacker this would require access to the TOE or TOE network.

Summary of the TOE Security Functional Requirements

The Timestamp Server 2.0.2 Patch 1 SFRs are given below. Full description of these SFRs can be found in Section 5.2 of the Security Target (ref [10]).

- Class FAU: Audit
  - Audit Data Generation (FAU_GEN.1)
- Class FCO: Communication
  - Enforced Proof of Origin (FCO_NRO.2)
- Class FCS: Cryptographic Support
  - Cryptographic Key Access (FCS_CKM.3)
  - Cryptographic Operation (FCS_COP.1 – 3 iterations)
- Class FIA: Identification and Authentication
  - Timing of Authentication (FIA_UAU.1)
  - Timing of Identification (FIA_UID.1)
- Class FPT: Protection of the TSF
  - Basic Internal TSF Data Transfer Protection (FPT_ITT.1)
  - TSF Data Integrity Monitoring (FPT_ITT.3)

Security Requirements for the IT Environment

None included.

Appendix B Acronyms

ACE	AISEP Certificate Extension
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

Appendix C References

[1] AISEP Publication No.1- Description of the AISEP
AP 1, Version 2.0, February 2001
Defence Signals Directorate

[2] AISEP Publication No.2 - The Licensing of the AISEFs
AP 2, Version 2.1, February 2001
Defence Signals Directorate

[3] Manual of Computer Security Evaluation Part I - Evaluation Procedures
EM 4, Issue 1.0, April 1995
Defence Signals Directorate
(EVALUATION-IN-CONFIDENCE)

[4] Manual of Computer Security Evaluations Part II - Evaluation Tools and Techniques
EM 5, Issue 1.0, April 1995
Defence Signals Directorate
(EVALUATION-IN-CONFIDENCE)

[5] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC)
Version 2.1, August 1999, CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements (CC)
Version 2.1, August 1999, CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (CC)
Version 2.1, August 1999, CCIMB-99-033

[8] Common Methodology for Information Technology Security Evaluation (CEM)
Version 1.0, August 1999, CEM-99/045

[9] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security
May 2000

[10] Security Target for Baltimore Timestamp Server version 2.0.2 Patch 1
Version 2.0.2k, 12 December 2002
Baltimore Technologies, Ltd.

[11] Baltimore Timestamp Server v2.0.2 Patch 1 Evaluation Technical Report (ETR)
Issue 1.1, December 2002
CMG
(EVALUATION-IN-CONFIDENCE)

[12] UniCERT Extended Technology – Timestamp Server v2.0.2 Administrator's Guide
Version 2.0h
Baltimore Technologies Ltd.

[13] UniCERT Extended Technology – Timestamp Server v2.0.2 Installation Guide
Version 2.0h
Baltimore Technologies Ltd.

[14] UniCERT Extended Technology – Timestamp Server v2.0.2 Release Notes
Version 2.0.2
Baltimore Technologies Ltd.

[15] Readme.txt file supplied with Timestamp Server v2.0.2 Patch 1
August 2001
Baltimore Technologies Ltd.

[16] TimestampServer2.0.2Patch1_ReadMe.htm file supplied with Timestamp Server v2.0.2 Patch 1
August 2001
Baltimore Technologies Ltd.