TOSHIBA

e-STUDIO2020AC/2520AC

with FAX Unit SYSV5.2

Security Target

Version 0.08

This document is a translation of the evaluated and certified security target written in Japanese.

Copyright 2024 TOSHIBA TEC CORPORATION All rights reserved.

TABLE OF CONTENTS

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

List of Tables

Copyright© 2024 TOSHIBA TEC. All rights reserved.

List of Tables

Copyright© 2024 TOSHIBA TEC. All rights reserved.

1. ST Introduction

ST Reference, TOE Reference, TOE Overview, and TOE Description are described in this Chapter.

1.1. ST Reference

The identity of the ST is described below.

Title: TOSHIBA e-STUDIO2020AC/2520AC with FAX Unit SYSV5.2 Security Target
Version: 0.08
Date Created: July 23, 2024
Author: TOSHIBA TEC CORPORATION

1.2. TOE Reference

The identity of the TOE is described below.

TOE Name: TOSHIBA e-STUDIO2020AC/2520AC with FAX Unit
Version: SYS V5.2
TOE Type: Multifunction Product
Developer Name: TOSHIBA TEC CORPORATION

The TOE shown above is consists of the MFP, Fax unit as shown in **Table 1**.

Table 1 TOE Configuration Item

Required components	Identification information of TOE	Version	Sales Area
MFP	TOSHIBA e-STUDIO2020AC	SYS V5.2	Japan
FAX unit	GD-1370J		
MFP	Either TOSHIBA e-STUDIO2020AC or TOSHIBA e-STUDIO2520AC	SYS V5.2	North America
FAX unit	GD-1370NA-N		
MFP	Either TOSHIBA e-STUDIO2020AC or TOSHIBA e-STUDIO2520AC	SYS V5.2	Europe
FAX unit	GD-1370EU		

1.3. TOE Overview

1.3.1. TOE Type

The TOE is the Multifunction Products that work in a network environment and provide capabilities of print, copy, scan, and fax.

1.3.2. Usage and Major Security Features of the TOE

The TOE is intended to be installed in a general office and used in a network environment.
The network environment to be used is an internal network (LAN) protected by a firewall from unauthorized access from the external network, where the TOE is connected to the client PCs, servers (FTP server, mail server, SYSLOG server), and public telephone network. Also, users use the basic functions of the MFP on the control panel of the MFP or from a client PC through a web browser or printer driver. Figure 1 shows the operational environment.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

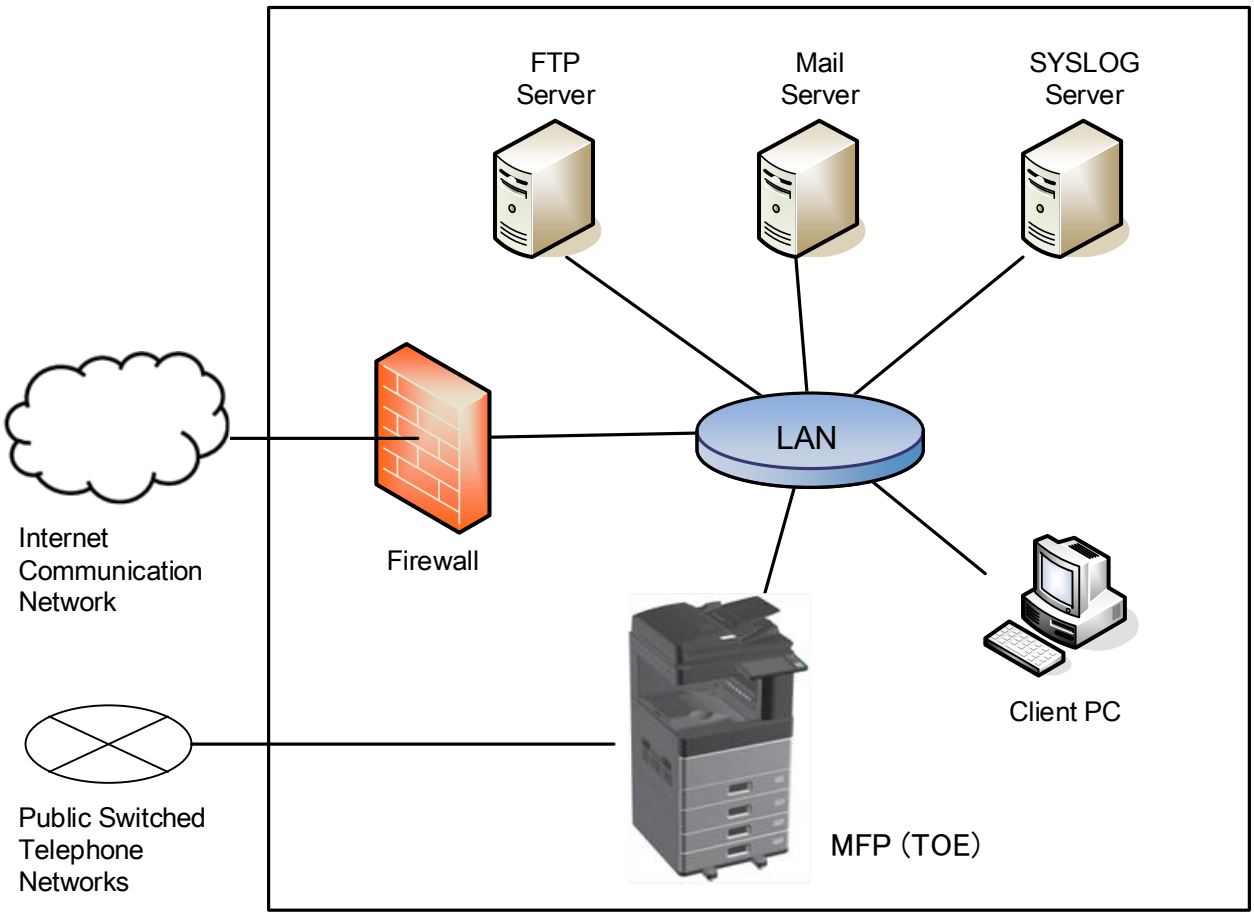


Figure1　Environment for the usage of the MFP

The TOE is a digital multifunction product equipped with the basic functions, such as copying, printing, scanning, and faxing.　In addition, in order to protect user document data and security-related data, the TOE has the following functions: a function to identify and authenticate users, an access control function based on user authority, a function to record a log of TOE use history and send it to the audit server, a function to encrypt data stored in the storage in the TOE, a function to protect communication data on the LAN, a setting function that limits security setting operations to administrators, a function to guarantee the normal operation of the security functions of the TOE, and a function to prohibit bridge connections between the public telephone network（PSTN）and the LAN.　In addition, data clearing and purging functions are excluded from the security functions evaluated.

1.3.3. Required Non-TOE Hardware and Software

Required hardware and firmware other than the TOE are shown below.

- Client PC

  U.NORMAL(a) can request printing of the document data through the LAN to the TOE.　The U.ADMIN(a) can refer to or change the setting data in the MFP using the Web browser.
  The browser and printer driver are as follows:

  - Web browser：Microsoft Edge
  - Printer Driver：TOSHIBA Universal Printer Driver2 (Version：7.222.5412.30)

Copyright© 2024 TOSHIBA TEC. All rights reserved.

- Mail Server

  The Mail Server is a server which transmits email using SMTP. The TOE and the Mail Server is connected with TLS communication. (This operation assumes a server using Sendmail 8.15.2.)

- FTP Server

  The FTP Server is a server which activates the File Transfer Protocol Server Software. The TOE and the FTP Server is connected with TLS communication. (This operation assumes a server using ProFTPD 1.3.6.)

- SYSLOG Server

  The SYSLOG Server is a server which transmits/receives TOE log data which is transferred using the Syslog protocol. The TOE and the SYSLOG Server is connected with TLS communication. (This operation assumes a server using Syslog-ng 3.14.)

1.4. TOE Description

1.4.1. Physical Boundary

The TOE comprises the MFP unit equipped with the Fax unit, which is a mandatory option, and guidance. The TOE is composed of the following:

Table 2 Hardware which composes TOE

MFP	Fax unit	Sales Area	Format	Distribution method
TOSHIBA e-STUDIO2020AC (CPU identification number: 3930)	GD-1370J	Japan	The MFP and the fax unit are hardware components that incorporate firmware in binary format.	The MFP unit and the fax unit are each shipped to the user as separate distribution items, packaged in cardboard boxes by the shipping carrier.
TOSHIBA e-STUDIO2020AC (CPU identification number: 3930)	GD-1370NA-N	North America		
TOSHIBA e-STUDIO2520AC (CPU identification number: 3930)	GD-1370NA-N			
TOSHIBA e-STUDIO2020AC (CPU identification number: 3930)	GD-1370EU	Europe		
TOSHIBA e-STUDIO2520AC (CPU identification number: 3930)	GD-1370EU			

The MFP versions are as follows:

- SYSTEM FIRMWARE: TS20SF0W1810
- SYSTEM SOFTWARE: TS20SD0W1810
- ENGINE FIRMWARE: TK160MWW62
- SCANNER FIRMWARE: TK160SLGWW16

The Fax unit versions are as follows:

- FAX1 FIRMWARE: FAXH625TA13

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Table 3　Guidance which composes TOE

Title	Identifier	Format	Distribution method	Sales Area
かんたん操作ガイド	OMJ210011B0	PDF and Printed documents	It is distributed to the user bundled with the MFP.	Japan
安全にお使いいただくために	OMJ210013B0	PDF and Printed documents		
コピー	OMJ210017B0	PDF		
スキャン	OMJ210019B0	PDF		
設定/登録	OMJ210027B0	PDF		
インストール	OMJ210031B0	PDF		
印刷	OMJ210033B0	PDF		
TopAccess	OMJ210035B0	PDF		
よくあるご質問	OMJ210029B0	PDF		
困ったときは	OMJ210005B0	PDF		
ハイセキュリティモード	OMJ210039E0	PDF		
用紙の準備	OMJ210003B0	PDF		
本機の仕様	OMJ210037B0	PDF		
機体の情報	OMJ210015B0	PDF		
ファクス	OMJ210021B0	PDF		
Quick Start Guide	OME210012B0	PDF and Printed documents	It is distributed to the user bundled with the MFP.	North America, Europe
Safety Information	OME210014B0	PDF and Printed documents		
Copy	OME210018B0	PDF		
Scan	OME210020B0	PDF		
User Functions	OME210028B0	PDF		
Installation	OME210032B0	PDF		
Print	OME210034B0	PDF		
TopAccess	OME210036B0	PDF		
Frequently Asked Questions	OME210030B0	PDF		
Troubleshooting	OME210006B0	PDF		
High Security Mode	OME210040E0	PDF		
Preparation of Paper	OME210004B0	PDF		
Information About Equipment	OME210016C0	PDF		
Specifications	OME210038C0	PDF		
Fax	OME210022B0	PDF		

Copyright© 2024 TOSHIBA TEC. All rights reserved.

1.4.2. Logical Boundary

The logical boundary of the TOE is defined by the TOE security function and a basic function which are described in the following section.

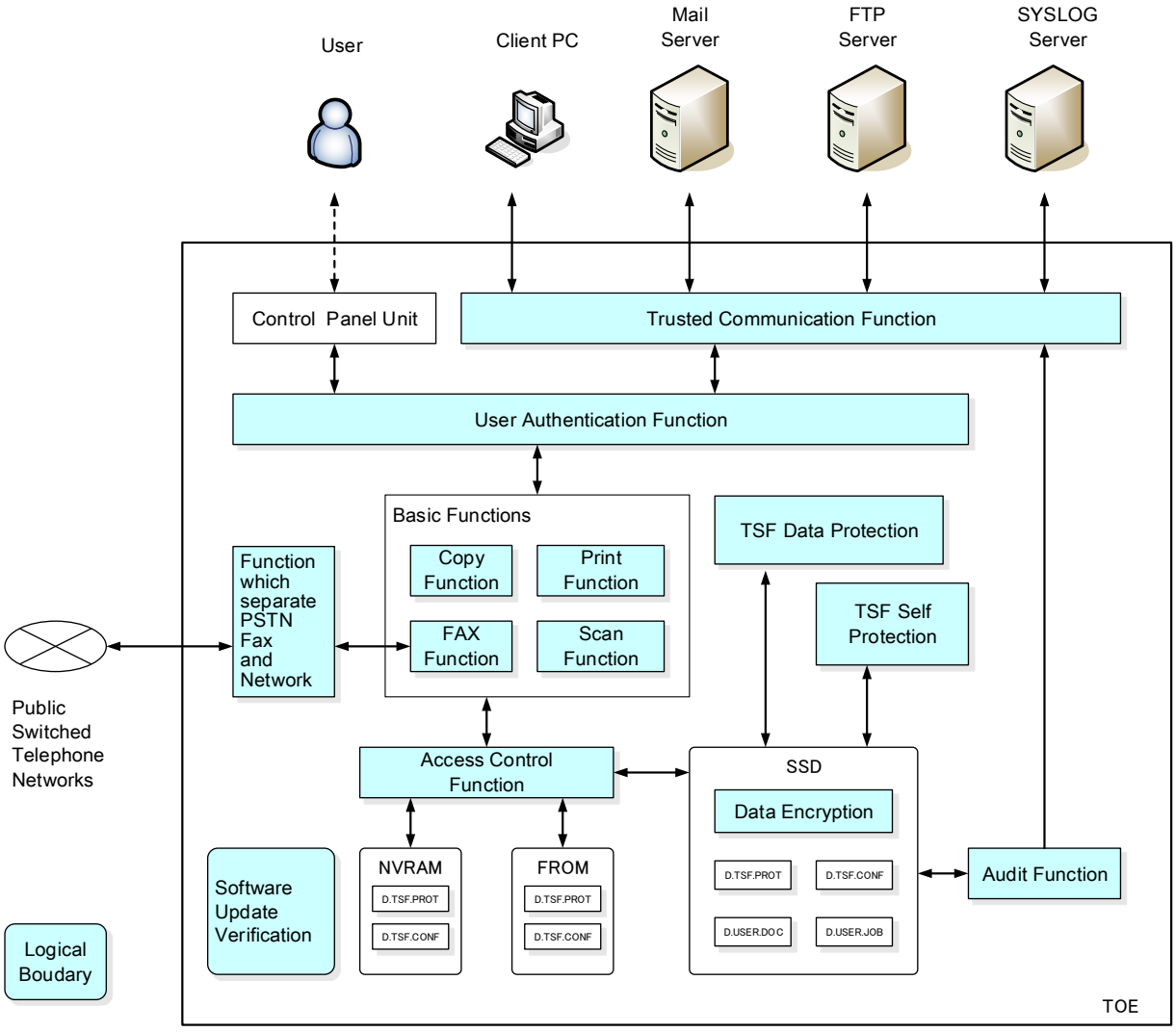


Figure 2 Logical Boundary

1.4.2.1. Basic Functions

The TOE is provided with a series of functions associated with images, such as Copy, Print, and Scan, as the Basic Functions, and controls these functions integrally.

- Copy function

  A Copy function is a function to read the original with the scanner and print it out from the printer according to the general user's operation from the control panel.

- Print function

  A Print function is a function which transmits the print data from the client PC to the TOE through the LAN and prints the data on a paper.

- Scan function

  The Scan function can attach and send a paper documentby user operation on the control panel and readingthe paper document with the Scanner to an email and the FTP server.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

- Fax function

  The Fax function consists of the Fax transmission function and the Fax reception function.
  The Fax transmission function is a function which transmits the paper document data read with the Scanner Unit to the external Fax machine through the PSTN. The Fax reception function is a function which receives the document data transmitted from the ex ternal Fax machine through the PSTN.

1.4.2.2. Security Functions

The security functions provided by the TOE are as follows:

- Function which gives permission to use the identity, authentication, and HCD functions

  It is a function which verifies whether a user who wants to use the TOE is an authorized user, and gives the user a permission to use the TOE only when the user is identified.
  The TOE prompts a user to enter the user ID and user password from the control panel or the client PC for user authentication, and has the feedback protection function which displays dummy characters during user password entry and the lockout function which locks a user who failed in authentication out. In addition, if there is no operation for a predetermined time after logging in, it has a function to automatically log out.

- Access Control Function

  The TOE controls access to the user data and functions that are secured assets to the authorized users.

- Audit Function

  The TOE generates audit log s for tracking the state of the TOE. All logs recorded per event are transferred to the audit server and viewable from the audit server.

- Trusted Communication Function

  The TOE supports the cryptographic communication protocol in order to prevent communic ation data from being leaked or tampered on the network during connection and communication with the LAN.
  The TOE communicates with the client PC, mail server, SYSLOG server, and FTP server in the operational environment using TLS for data encryption. The TOE protects the print data by using TLS and print protocol IPPS during communication with the client PC when IPP print is performed by the client PC using the printer driver.

- TSF Self Protection

  The TOE perfor performs integrity tests on its static executables and configuration files using verification of their digital signatures against the known signatures. This allows the TOE to detect any tampering of its trusted state.

- TSF Data Protection

  Only an administrator role user authenticated by the Identity Authentication function has the capability to manage the TSF data from the control panel or TopAccess. For example, you can change the date and time, register/delete users, and enable or disable available services and protocols.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

- Data Encryption

  The Data Encryption is a function to encrypt user data saved in the SSD to protect them from being leaked.

- Function which separate PSTN Fax and Network

  This function prohibits bridge connections between the public telephone network and the LAN by restricting entry from PSTN to Fax reception.

- Software Update Verification

  This function is a function which verifies whether software to be updated is authorized when software of the TOE is updated.

1.4.2.3. Terminology

The terms which are defined by CC and PP in Chapter 2 out of the specific terms associated with the ST should follow the definition thereof. The other terms are defined as shown in **Table 4.**

Table 4 Terminology

Terminology	Definition
User ID	An identifier given to a general user and MFP administrator. The TOE specifies the user by the identifier.
User Password	A password which is used to log into the TOE by a user.
Job Log	The job information such as Print Job, Transmission Journals, Reception Journals and Scan Job.
Message Log	Logs regarding MFP's device information or operations executed by users.
TopAccess	A web-based job and device control tool. The MFP information can be retrieved by using this tool through network.
Auto Logout Time	Time to log out when a logged in user does not operate the MFP for a certain period of time.
Lockout Time	Time until the locked out account is released.
Date and Time	Time information for log management. Year/moth/day/hour/min/sec
Role	U.NORMAL、U.ADMIN. U.NORMAL is refined to U.NORMAL(a) and U.FAXOPERATOR. U.ADMIN is refined to U.ADMIN(a), U.ACCOUNTMANAGER, and U.ADDRESSBOOKOPERATOR.
Firmware	Software which is embedded into the device to control hardware.
Cipher Suite	Combination of the cryptographic algorithms used for TLS communication, which consists of the combination of “Key replacement_Signature_Encryption_Hash function”.
Address Book	Fax numbers and email addresses can be registered and displayed in the destination list. It enables simple specification of the fax transmission destinations and scan email transmission destinations.
User Authentication Failure Handling	An administrator can change the number of retries for entering the login password and lockout time and clear the locked out account status.
Secure Channel	A communication channel in which data is encrypted to prevent wiretapping by the third party.
European Special Characters	Words with the German umlauts and French cedilla.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

2. Conformance Claim

2.1. CC Conformance Claim

The following shows the CC Conformance Claim of the ST and TOE.

Common Criteria version: Version 3.1 Release 5

- Part1: Introduction and general model April 2017 Version 3.1 Revision 5
- Part2: Security functional components April 2017 Version 3.1 Revision 5
- Part3: Security assurance components April 2017 Version 3.1 Revision 5
- Conformance of ST to CC part2: CC part 2 Extended
- Conformance of ST to CC part3: CC part 3 Conformant

2.2. PP Conformance Claim

The ST and TOE conform to the following PP.

PP Name: Protection Profile for Hardcopy Devices
PP Version: 1.0 dated September 10, 2015
Certification Identification: JISEC-C0553
Errata: Protection Profile for Hardcopy Devices – v1.0 Errata #1, June 2017

2.3. Package Conformance Claim

The ST does not conform to the packages.

2.4. Conformance Rationale

The following conditions requested by PP have been satisfied and must be “Exact Conformance” as requested by PP. Therefore, the TOE type is consistent with PP.

- Required Uses
  Printing, Scanning, Copying、Networking communications, Addministration
- Conditionally Mandatory Uses
  PSTN faxing, Fileld-Replaceable Nonvolatile Storage
- Optional Uses
  None

Copyright© 2024 TOSHIBA TEC. All rights reserved.

3. Security Problem Definitions

3.1. Users

The User and role of the TOE are defined as shown below in the ST.

Table 5 User Categories

Role		Category name	Definition
U.NORMAL A User who has been identified and authenticated and does not have an administrative role	U.NORMAL(a)	Normal User	A User who is authorized to execute Copy, Print, Scan, and Fax functions which are the basic functions of the TOE. A Normal User is authorized to operate each function and can execute only the authorized function
	U.FAXOPERATOR	Normal User	A user who can execute the Fax transmission/reception functions
U.ADMIN A User who has been identified and authenticated and has an administrative role	U.ADMIN(a)	Administrator	An administrator who is authorized to manage the entire TOE, such as setting of the TOE security functions, change of the user account information, and browse of the audit log
	U.ACCOUNTMANAGER	Administrator	An administrator who can perform the settings for the user account management (setting of the user ID and role of the user and operation authority of the basic functions)
	U.ADDRESSBOOKOPERATOR	Administrator	A user who can edit the address book

3.2. Assets

Two asset classifications are defined in the ST.

Table 6 Asset Classification

Designation	Asset category	Definition
D.USER	User Data	Data created by and for Users that do not affect the operation of the TSF.
D.TSF	TSF Data	Data created by and for the TOE that might affect the operation of the TSF.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

3.2.1. User Data

The two User Data is defined in the ST.

Table 7 User Data types

Designation	User Data type	Definition	Details
D.USER.DOC	User Document Data	Information contained in a User's Document, in electronic or hardcopy form	Copy Document Data
			Print Document Data
			Scan Document Data
			Fax Transmission Document Data
			Fax Reception Document Data
D.USER.JOB	User Job Data	Information related to a User's Document or Document Processing Job	Print Job
			Scan Job
			Copy Job
			Fax Transmission Job
			Fax Reception Job

3.2.2. TSF Data

The TSF Data consist of the following 2 types.

Table 8 TSF Data types

Designation	TSF Data type	Definition	Details
D.TSF.PROT	Protected TSF Data	TSF Data for which alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE, but for which disclosure is acceptable	Enable/Disable of the Secure Channel
			User ID
			Role
			Allowable Number of entry for Login Password
			Lockout Time
			Locked Account Status
			Auto Logout Time
			Date and Time Information
			Minimum Password Length
			Address Book
			SYSLOG Server Settings
			FTP Server Settings
			Software update
D.TSF.CONF	Confidential TSF Data	TSF Data for which either disclosure or alteration by a User who is neither the data owner nor in an Administrator role might affect the security of the TOE	User Password
			Encryption Key

Copyright© 2024 TOSHIBA TEC. All rights reserved.

3.3. Threats

The Threats to the TOE which are countered by the conforming products are as shown below. Threats are defined by a threat agent that performs an action resulting in an outcome that has the potential to violate TOE security policies.

Table 9 Threats

Designation	Definition
T.UNAUTHORIZED_ACCESS	An attacker may access (read, modify, or delete) USER.DOCument Data or change (modify or delete) User Job Data in the TOE through one of the TOE's interfaces.
T.TSF_COMPROMISE	An attacker may gain Unauthorized Access to TSF Data in the TOE through one of the TOE's interfaces.
T.TSF_FAILURE	A malfunction of the TSF may cause loss of security if the TOE is permitted to operate.
T.UNAUTHORIZED_UPDATE	An attacker may cause the installation of unauthorized software on the TOE.
T.NET_COMPROMISE	An attacker may access data in transit or otherwise compromise the security of the TOE by monitoring or manipulating network communication.

3.4. Organization Security Policies

The following are Organizational Security Policies3 (OSPs) that are upheld by conforming products.

3.4.1. Organizational Security Policy Definitions

Organizational Security Policies are used to provide a basis for Security Objectives that are not practical to define on the basis of Threats to Assets or that originate primarily from customer expectations.

Table 10 Organization Security Policies

Designation	Definition
P.AUTHORIZATION	Users must be authorized before performing Document Processing and administrative functions.
P.AUDIT	Security-relevant activities must be audited and the log of such actions must be protected and transmitted to an External IT Entity.
P.COMMS_PROTECTION	The TOE must be able to identify itself to other devices on the LAN.
P.STORAGE_ENCRYPTION (conditionally mandatory)	If the TOE stores USER.DOCument Data or Confidential TSF Data on Field-Replaceable Nonvolatile Storage Devices, it will encrypt such data on those devices.
P.KEY_MATERIAL (conditionally mandatory)	Cleartext keys, submasks, random numbers, or any other values that contribute to the creation of encryption keys for Field-Replaceable Nonvolatile Storage of USER.DOCument Data or Confidential TSF Data must be protected from unauthorized access and must not be stored on that storage device.
P.FAX_FLOW (conditionally mandatory)	If the TOE provides a PSTN fax function, it will ensure separation between the PSTN fax line and the LAN.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

3.5. Assumption Definitions

Assumptions are conditions that must be satisfied in order for the Security Objectives and functional requirements to be effective.

Table 11 Assumptions

Designation	Definition
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it stores or processes, is assumed to be provided by the environment.
A.NETWORK	The Operational Environment is assumed to protect the TOE from direct, public access to its LAN interface.
A.TRUSTED_ADMIN	TOE Administrators are trusted to administer the TOE according to site security policies.
A.TRAINED_USERS	Authorized Users are trained to use the TOE according to site security policies.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

4. Security Objectives

4.1. Security Objectives for Operational Environment

The details of the Security Objectives for the Operational Environment are as described in Table 12.

Table 12 Security Objectives for the Operational Environment

Designation	Definition
OE.PHYSICAL_PROTECTION	The Operational Environment shall provide physical security, commensurate with the value of the TOE and the data it stores or processes.
OE.NETWORK_PROTECTION	The Operational Environment shall provide network security to protect the TOE from direct, public access to its LAN interface.
OE.ADMIN_TRUST	The TOE Owner shall establish trust that Administrators will not use their privileges for malicious purposes.
OE.USER_TRAINING	The TOE Owner shall ensure that Users are aware of site security policies and have the competence to follow them.
OE.ADMIN_TRAINING	The TOE Owner shall ensure that Administrators are aware of site security policies and have the competence to use manufacturer's guidance to correctly configure the TOE and protect passwords and keys accordingly.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

5. Extended Component Definitions

Extended component definitions are listed below.

5.1. FAU_STG_EXT Extended: External Audit Trail Storage

Family Behavior:

This family defines requirements for the TSF to ensure that secure transmission of audit data from TOE to an External IT Entity.

Component leveling:

FAU_STG_EXT.1 External Audit Trail Storage requires the TSF to use a trusted channel implementing a secure protocol.

Management:

The following actions could be considered for the management functions in FMT:

- The TSF shall have the ability to configure the cryptographic functionality.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- There are no auditable events foreseen.

FAU_STG_EXT.1 Extended: Protected Audit Trail Storage

Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation,
FTP_ITC.1 Inter-TSF trusted channel

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an External IT Entity using a trusted channel according to FTP_ITC.1.

Rationale:

The TSF is required that the transmission of generated audit data to an External IT Entity which relies on a non-TOE audit server for storage and review of audit records. The storage of these audits records and the ability to allow the administrator to review these audit records is provided by the Operational Environment in that case. The Common Criteria does not provide a suitable SFR for the transmission of audit data to an External IT Entity.

This extended component protects the audit records, and it is therefore placed in the FAU class with a single component.

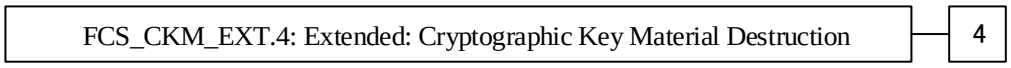
5.2. FCS_CKM_EXT Extended: Cryptographic Key Management

Family Behavior:

This family addresses the management aspects of cryptographic keys. Especially, this extended component is intended for cryptographic key destruction.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Component leveling:



FCS_CKM_EXT.4 Cryptographic Key Material Destruction ensures not only keys but also key materials that are no longer needed are destroyed by using an approved method.

Management:

The following actions could be considered for the management functions in FMT:

- There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- There are no auditable events foreseen.

FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

Hierarchical to: No other components.
Dependencies: [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)], FCS_CKM.4 Cryptographic key destruction

Rationale:

Cryptographic Key Material Destruction is to ensure the keys and key materials that are no longer needed are destroyed by using an approved method, and the Common Criteria does not provide a suitable SFR for the Cryptographic Key Material Destruction.
This extended component protects the cryptographic key and key materials against exposure, and it is therefore placed in the FCS class with a single component.

5.3. FCS_HTTPS_EXT Extended: HTTPS selected

Family Behavior:

Components in this family define requirements for protecting remote management sessions between the TOE and a Security Administrator. This family describes how HTTPS will be implemented. This is a new family defined for the FCS Class.

Component leveling:

FCS_HTTPS_EXT.1 HTTPS selected, requires that HTTPS be implemented according to RFC 2818 and supports TLS.

Management:

The following actions could be considered for the management functions in FMT:

- There are no management actions foreseen.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- Failure of HTTPS session establishment

FCS_HTTPS_EXT.1 Extended: HTTPS selected

Hierarchical to: No other components.
Dependencies: No dependencies.

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

Rationale:

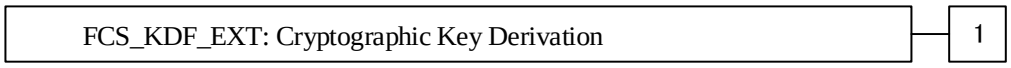
HTTPS is one of the secure communication protocols, and the Common Criteria does not provide a suitable SFR for the communication protocols using cryptographic algorithms.
This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.4. FCS_KDF_EXT Extended: Cryptographic Key Derivation

Family Behavior:

This family specifies the means by which an intermediate key is derived from a specified set of submasks.

Component leveling:



FCS_KDF_EXT.1 Cryptographic Key Derivation requires the TSF to derive intermediate keys from submasks using the specified hash functions.

Management:

The following actions could be considered for the management functions in FMT:

- There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- There are no auditable events foreseen.

FCS_KDF_EXT.1 Extended: Cryptographic Key Derivation

Hierarchical to: No other components.
Dependencies: FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication), [if selected: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)]

Copyright© 2024 TOSHIBA TEC. All rights reserved.

FCS_KDF_EXT.1.1 The TSF shall accept [selection: *a RNG generated submask as specified in FCS_RBG_EXT.1, a conditioned password submask, imported submask*] to derive an intermediate key, as defined in [selection: *NIST SP 800-108 [selection: KDF in Counter Mode, KDF in Feedback Mode, KDF in Double-Pipeline Iteration Mode], NIST SP 800-132*], using the keyed-hash functions specified in FCS_COP.1(h), such that the output is at least of equivalent security strength (in number of bits) to the BEV.

Rationale:

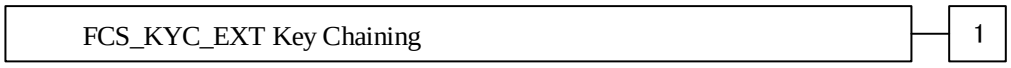
The TSF is required to specify the means by which an intermediate key is derived from a specified set of submasks using the specified hash functions.
This extended component protects the Data Encryption Keys using cryptographic algorithms in the maintained key chains, and it is therefore placed in the FCS class with a single component.

5.5. FCS_KYC_EXT Extended: Cryptographic Operation (Key Chaining)

Family Behavior:

This family provides the specification to be used for using multiple layers of encryption keys to ultimately secure the protected data encrypted on the storage.

Component leveling:



FCS_KYC_EXT Key Chaining requires the TSF to maintain a key chain and specifies the characteristics of that chain.

Management:

The following actions could be considered for the management functions in FMT:

- There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- There are no auditable events foreseen.

FCS_KYC_EXT.1 Extended: Key Chaining

Hierarchical to: No other components.
Dependencies: [FCS_COP.1(e) Cryptographic operation (Key Wrapping),
FCS_SMC_EXT.1 Extended: Submask Combining,
FCS_COP.1(i) Cryptographic operation (Key Transport),
FCS_KDF_EXT.1 Cryptographic Operation (Key Derivation),
and/or
FCS_COP.1(f) Cryptographic operation (Key Encryption)].

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [selection: *one, using a submask as the BEVor DEK; intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s)*: [selection: *key wrapping as specified in FCS_COP.1(e), key combining as specified in*

Copyright© 2024 TOSHIBA TEC. All rights reserved.

FCS_SMC_EXT.1, key encryption as specified in FCS_COP.1(f), key derivation as specified in FCS_KDF_EXT.1, key transport as specified in FCS_COP.1(i)]] while maintaining an effective strength of [selection: *128 bits, 256 bits*].

Rationale:

Key Chaining ensures that the TSF maintains the key chain, and also specifies the characteristics of that chain. However, the Common Criteria does not provide a suitable SFR for the management of multiple layers of encryption key to protect encrypted data.
This extended component protects the TSF data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.6. FCS_RBG_EXT Extended: Cryptographic Operation (Random Bit Generation)

Family Behavior:

This family defines requirements for random bit generation to ensure that it is performed in accordance with selected standards and seeded by an entropy source.

Component leveling:

FCS_RBG_EXT.1 Random Bit Generation requires random bit generation to be performed in accordance with selected standards and seeded by an entropy source.

Management:

The following actions could be considered for the management functions in FMT:

- There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- There are no auditable events foreseen.

FCS_RBG_EXT.1 Extended: Random Bit Generation

Hierarchical to: No other components.
Dependencies: No dependencies.

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with [selection: ISO/IEC 18031:2011, NIST SP 800-90A] using [selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES)].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from [selection: [assignment: *number of software-based sources*] *software-based noise source(s)*, [assignment: *number of hardware-based sources*] *hardware-based noise source(s)*] with a minimum of [selection: *128 bits, 256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security strength table for hash functions”, of the keys and hashes that it will generate.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Rationale:

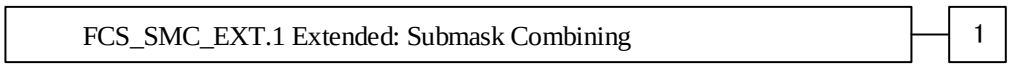
Random bits/number will be used by the SFRs for key generation and destruction, and the Common Criteria does not provide a suitable SFR for the random bit generation.
This extended component ensures the strength of encryption keys, and it is therefore placed in the FCS class with a single component.

5.7. FCS_SMC_EXT Extended: Submask Combining

Family Behavior:

This family defines the means by which submasks are combined, if the TOE supports more than one submask being used to derive or protect the BEV.

Component leveling:



FCS_SMC_EXT.1 Submask combining requires the TSF to combine the submasks in a predictable fashion.

Management:

The following actions could be considered for the management functions in FMT:

- There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- There are no auditable events foreseen.

FCS_SMC_EXT.1 Extended: Submask Combining

Hierarchical to: No other components.
Dependencies: FCS_COP.1(c) Cryptographic operation (Hash Algorithm)

FCS_SMC_EXT.1.1 The TSF shall combine submasks using the following method [selection: exclusive OR (XOR), SHA-256, SHA-512] to generate an intermediary key or BEV.

Rationale:

Submask Combining is to ensure the TSF combine the submasks in order to derive or protect the BEV.
This extended component protects the TSF data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

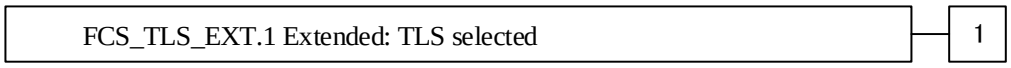
5.8. FCS_TLS_EXT Extended: TLS selected

Family Behavior:

This family addresses the ability for a server and/or a client to use TLS to protect data between a client and the server using the TLS protocol.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Component leveling:



FCS_TLS_EXT.1 TLS selected, requires the TLS protocol implemented as specified.

Management:

The following actions could be considered for the management functions in FMT:

- There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- Failure of TLS session establishment

FCS_TLS_EXT.1 Extended: TLS selected

Hierarchical to: No other components.
Dependencies: No dependencies.

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: *TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)*] supporting the following ciphersuites:

Mandatory Ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

[selection:

- None
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

].

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Rationale:

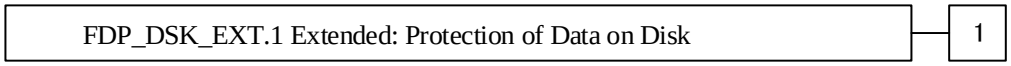
TLS is one of the secure communication protocols, and the Common Criteria does not provide a suitable SFR for the communication protocols using cryptographic algorithms.
This extended component protects the communication data using cryptographic algorithms, and it is therefore placed in the FCS class with a single component.

5.9. FDP_DSK_EXT Extended: Protection of Data on Disk

Family Behavior:

This family is to mandate the encryption of all protected data written to the storage.

Component leveling:



FDP_DSK_EXT.1 Extended: Protection of Data on Disk, requires the TSF to encrypt all the Confidential TSF and User Data stored on the Field-Replaceable Nonvolatile Storage Devices in order to avoid storing these data in plaintext on the devices.

Management:

The following actions could be considered for the management functions in FMT:

- There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- There are no auditable events foreseen.

FDP_DSK_EXT.1 Extended: Protection of Data on Disk

Hierarchical to: No other components.
Dependencies: FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption)

FDP_DSK_EXT.1.1 The TSF shall [selection: *perform encryption in accordance with FCS_COP.1(d), use a self-encrypting Field-Replaceable Nonvolatile Storage Device that is separately CC certified to conform to the FDE EE cPP*] such that any Field-Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext confidential TSF Data.

FDP_DSK_EXT.1.2 The TSF shall encrypt all protected data without user intervention.

Rationale:

Extended: Protection of Data on Disk is to specify that encryption of any confidential data without user intervention, and the Common Criteria does not provide a suitable SFR for the Protection of Data on Disk.
This extended component protects the Data on Disk, and it is therefore placed in the FDP class with a single component.

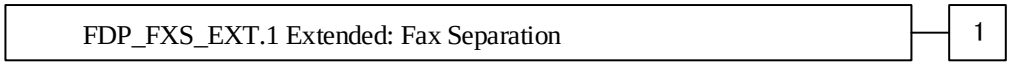
Copyright© 2024 TOSHIBA TEC. All rights reserved.

5.10. FDP_FXS_EXT Extended: Fax Separation

Family Behavior:

This family addresses the requirements for separation between Fax PSTN line and the LAN to which TOE is connected.

Component leveling:



FDP_FXS_EXT.1 Fax Separation, requires the fax interface cannot be used to create a network bridge between a PSTN and a LAN to which TOE is connected.

Management:

The following actions could be considered for the management functions in FMT:

- There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- There are no auditable events foreseen.

FDP_FXS_EXT.1 Extended: Fax separation

Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_FXS_EXT.1.1 The TSF shall prohibit communication via the fax interface, except transmitting or receiving User Data using fax protocols.

Rationale:

Fax Separation is to protect a LAN against attack from PSTN line, and the Common Criteria does not provide a suitable SFR for the Protection of TSF or User Data.
This extended component protects the TSF Data or User Data, and it is therefore placed in the FDP class with a single component.

5.11. FIA_PMG_EXT Extended: Password Management

Family Behavior:

This family defines requirements for the attributes of passwords used by administrative users to ensure that strong passwords and passphrases can be chosen and maintained.

Component leveling:

FIA_PMG _EXT.1 Password management requires the TSF to support passwords with varying composition requirements, minimum lengths, maximum lifetime, and similarity constraints.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Management:

The following actions could be considered for the management functions in FMT:

- There are no auditable events foreseen.

FIA_PMG _EXT.1 Extended: Password management

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_PMG _EXT.1.1 The TSF shall provide the following password management capabilities for User passwords:

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [assignment: other characters]];
- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater.

Rationale:

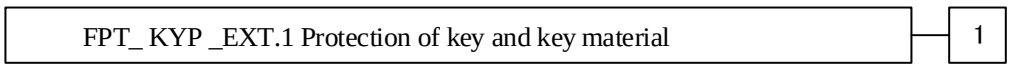
Password Management is to ensure the strong authentication between the endpoints of communication, and the Common Criteria does not provide a suitable SFR for the Password Management.
This extended component protects the TOE by means of password management, and it is therefore placed in the FIA class with a single component.

5.12. FPT_KYP_EXT Extended: Protection of Key and Key Material

Family Behavior:

This family addresses the requirements for keys and key materials to be protected if and when written to nonvolatile storage.

Component leveling:



FPT_ KYP _EXT.1 Extended: Protection of key and key material, requires the TSF to ensure that no plaintext key or key materials are written to nonvolatile storage.

Management:

The following actions could be considered for the management functions in FMT:

- There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- There are no auditable events foreseen.

FPT_ KYP _EXT.1 Extended: Protection of Key and Key Material

Hierarchical to: No other components.
Dependencies: No dependencies.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

FPT_ KYP _EXT.1.1 The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in any Field-Replaceable Nonvolatile Storage Device, and not store any such plaintext key on a device that uses the key for its encryption.

Rationale:

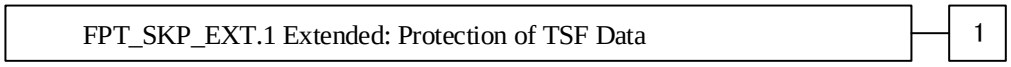
Protection of Key and Key Material is to ensure that no plaintext key or key material are written to nonvolatile storage, and the Common Criteria does not provide a suitable SFR for the protection of key and key material.
This extended component protects the TSF data, and it is therefore placed in the FPT class with a single component.

5.13. FPT_SKP_EXT Extended: Protection of TSF Data

Family Behavior:

This family addresses the requirements for managing and protecting the TSF data, such as cryptographic keys. This is a new family modelled as the FPT Class.

Component leveling:



FPT_SKP_EXT.1 Protection of TSF Data (for reading all symmetric keys), requires preventing symmetric keys from being read by any user or subject. It is the only component of this family.

Management:

The following actions could be considered for the management functions in FMT:

- There are no management actions foreseen.

FPT_SKP_EXT.1 Extended: Protection of TSF Data

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

Rationale:

Protection of TSF Data is to ensure the pre-shared keys, symmetric keys and private keys are protected securely, and the Common Criteria does not provide a suitable SFR for the protection of such TSF data.
This extended component protects the TOE by means of strong authentication using Pre-shared Key, and it is therefore placed in the FPT class with a single component.

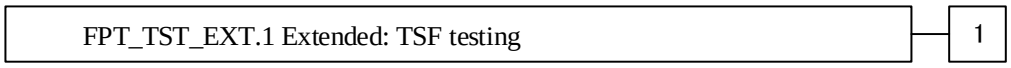
5.14. FPT_TST_EXT Extended: TSF testing

Family Behavior:

This family addresses the requirements for self-testing the TSF for selected correct operation.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Component leveling:



FPT_TST_EXT.1 TSF testing requires a suite of self-testing to be run during initial start-up in order to demonstrate correct operation of the TSF.

Management:

The following actions could be considered for the management functions in FMT:

- There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

- There are no auditable events foreseen.

FPT_TST_EXT.1 Extended: TSF testing

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests during initial start-up (and power on) to demonstrate the correct operation of the TSF.

Rationale:

TSF testing is to ensure the TSF can be operated correctly, and the Common Criteria does not provide a suitable SFR for the TSF testing. In particular, there is no SFR defined for TSF testing. This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

5.15. FPT_TUD_EXT Extended: Trusted Update

Family Behavior:

This family defines requirements for the TSF to ensure that only administrators can update the TOE firmware/software, and that such firmware/software is authentic.

Component leveling:

FPT_TUD_EXT.1 Trusted Update, ensures authenticity and access control for updates.

Management:

The following actions could be considered for the management functions in FMT:

- There are no management actions foreseen.

Audit:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

Copyright© 2024 TOSHIBA TEC. All rights reserved.

- There are no auditable events foreseen.

FPT_TUD_EXT.1 Trusted Update

Hierarchical to: No other components.
Dependencies: [FCS_COP.1(b) Cryptographic Operation (for signature generation/verification), or
FCS_COP.1(c) Cryptographic operation (Hash Algorithm)].

FPT_TUD_EXT.1.1 The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [selection: no other functions] prior to installing those updates.

Rationale:

Firmware/software is a form of TSF Data, and the Common Criteria does not provide a suitable SFR for the management of firmware/software. In particular, there is no SFR defined for importing TSF Data.
This extended component protects the TOE, and it is therefore placed in the FPT class with a single component.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

6. Security Requirements

6.1. Notation

- **Bold** typeface indicates the portion that has been “completed” or “refined” in this PP.
- ***Bold italic*** typeface indicates the portion that has been “assigned”, “selected” or “refined” in this ST.
- Letters in brackets indicate the “assigned” or “selected” results.
- SFR components that are followed by a letter in parentheses, e.g., (a), (b)… represent required iterations.

6.2. Class FAU: Security Audit

6.2.1. FAU_GEN.1 Audit data generation

(for O.AUDIT)
Hierarchical to: No other components.
Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

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

c) **All auditable events specified in Table 13**, [***none***].

FAU_GEN.1.2 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 (if applicable), 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, **additional information specified in Table 13,** [***none***].

Table 13 Auditable Events

Auditable events	Relevant SFR	Additional information
Job completion	FDP_ACF.1	Type of job
Unsuccessful User authentication	FIA_UAU.1	None
Unsuccessful User identification	FIA_UID.1	None
Use of management functions	FMT_SMF.1	None
Modification to the group of Users that are part of a role	FMT_SMR.1	None
Changes to the time	FPT_STM.1	None
Failure to establish session	FTP_ITC.1, FTP_TRP.1(a), FTP_TRP.1(b)	Reason for failure

6.2.2. FAU_GEN.2 User identity association

(for O.AUDIT)
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

Copyright© 2024 TOSHIBA TEC. All rights reserved.

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.3. FAU_STG_EXT.1 Extended: External Audit Trail Storage

(for O.AUDIT)
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation,
FTP_ITC.1 Inter-TSF trusted channel.

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an External IT Entity using a trusted channel according to FTP_ITC.1.

6.3. Class FCS: Cryptographic Support

6.3.1. FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys)

(for O.COMMS_PROTECTION)
Hierarchical to: No other components.
Dependencies: FCS_COP.1(b) Cryptographic Operation (for signature generation/ verification)
FCS_COP.1(i) Cryptographic operation (Key Transport)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_CKM.1.1(a) **Refinement:** The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance **with [**

- ***NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes***

] and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

6.3.2. FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)

(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION)
Hierarchical to: No other components.
Dependencies: [FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(e) Cryptographic Operation (Key Wrapping)
FCS_COP.1(f) Cryptographic operation (Key Encryption)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_CKM.1.1(b) **Refinement:** The TSF shall generate **symmetric** cryptographic keys **using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes [*128 bit, 256 bit*] that meet the following: No Standard.**

6.3.3. FCS_CKM.4 Cryptographic key destruction

(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA))
Hierarchical to: No other components.
Dependencies: [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or
FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]

Copyright© 2024 TOSHIBA TEC. All rights reserved.

FCS_CKM.4.1 **Refinement:** The TSF shall **destroy** cryptographic keys in accordance with a specified cryptographic key **destruction** method [

For volatile memory, the destruction shall be executed by [*powering off a device*].

For nonvolatile storage, the destruction shall be executed by a [*single*] overwrite of key data storage location consisting of *[a static pattern],* followed by a [*none*]. If read-verification of the overwritten data fails, the process shall be repeated again;

] that meets the following: [***no standard***].

6.3.4. FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

(for O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)
Hierarchical to: No other components.
Dependencies: [FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric keys), or
FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)],
FCS_CKM.4 Cryptographic key destruction

FCS_CKM_EXT.4.1 The TSF shall destroy all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed.

6.3.5. FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)

(for O.COMMS_PROTECTION)
Hierarchical to: No other components.
Dependencies: FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(a) **Refinement:** The TSF shall perform **encryption and decryption** in accordance with a specified cryptographic algorithm **AES operating in [*CBC modes*]** and cryptographic key sizes **128-bits and 256-bits** that meets the following:

- **FIPS PUB 197, "Advanced Encryption Standard (AES)"**
- [***NIST SP 800-38A***]

6.3.6. FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)

(for O.UPDATE_VERIFICATION, O.COMMS_PROTECTION)
Hierarchical to: No other components.
Dependencies: [FCS_CKM.1(a) Cryptographic key generation]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(b) **Refinement:** The TSF shall perform **cryptographic signature services** in accordance with a **[*RSA Digital Signature Algorithm (rDSA) with key sizes (modulus) of [2048 bits]*]** that meets the following **[*FIPS PUB 186-4, "Digital Signature Standard"*]**.

6.3.7. FCS_RBG_EXT.1(a) Extended: Cryptographic Operation (Random Bit Generation)

(for O.STORAGE_ENCRYPTION)
Hierarchical to: No other components.
Dependencies: No dependencies.

FCS_RBG_EXT.1.1(a) The TSF shall perform all deterministic random bit generation services in accordance with [***NIST SP 800-90A***] using [***Hash_DRBG (any)***].

Copyright© 2024 TOSHIBA TEC. All rights reserved.

FCS_RBG_EXT.1.2(a) The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [***[single] hardware-based noise source(s)***] with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

6.3.8. FCS_RBG_EXT.1(b) Extended: Cryptographic Operation (Random Bit Generation)

(for O.COMMS_PROTECTION)
Hierarchical to: No other components.
Dependencies: No dependencies.

FCS_RBG_EXT.1.1(b) The TSF shall perform all deterministic random bit generation services in accordance with [***NIST SP 800-90A***] using [***CTR_DRBG (AES)***].

FCS_RBG_EXT.1.2(b) The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [***[single] hardware-based noise source(s)***] with a minimum of [***128bits***] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

6.3.9. FCS_COP.1(c) Cryptographic operation (Hash Algorithm)

(selected in FPT_TUD_EXT.1.3, or with FCS_SNI_EXT.1.1)
Hierarchical to: No other components.
Dependencies: No dependencies.

FCS_COP.1.1(c) Refinement: The TSF shall perform cryptographic hashing services in accordance with [***SHA-1, SHA-256, SHA-384, SHA-512***] that meet the following: [**ISO/IEC 10118-3:2004**].

6.3.10. FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption)

(for O.STORAGE_ENCRYPTION)
Hierarchical to: No other components.
Dependencies: [~~FDP_ITC.1 Import of user data without security attributes, or~~
~~FDP_ITC.2 Import of user data with security attributes, or~~
FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(d) The TSF shall perform **data encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [*CBC*] mode** and cryptographic key sizes **[*128 bits*]** that meet the following: **AES as specified in ISO/IEC 18033-3, [*CBC as specified in ISO/IEC 10116*]**.

6.3.11. FCS_COP.1(f) Cryptographic operation (Key Encryption)

(selected from FCS_KYC_EXT.1.1)
Hierarchical to: No other components.
Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

Copyright© 2024 TOSHIBA TEC. All rights reserved.

FCS_COP.1.1(f) Refinement: The TSF shall perform **key encryption and decryption** in accordance with a specified cryptographic algorithm **AES used in [[*CBC*] mode]** and cryptographic key sizes **[*128 bits*]** that meet the following: [**AES as specified in ISO /IEC 18033-3, [*CBC as specified in ISO/IEC 10116*]**].

6.3.12. FCS_SMC_EXT.1 Extended: Submask Combining

(selected in FCS_KYC_EXT.1.1)
Hierarchical to: No other components.
Dependencies: FCS_COP.1(c) Cryptographic operation (Hash Algorithm)
FCS_SMC_EXT.1.1 The TSF shall combine submasks using the following method [***exclusive OR (XOR)***] to generate an intermediary key or BEV.

6.3.13. FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)

(selected with FCS_IPSEC_EXT.1.4)
Hierarchical to: No other components.
Dependencies: [FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(g) Refinement: The TSF shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-[***SHA-1, SHA-256***], key size [***160, 256***]bits, and message digest sizes [***160, 256***] bits that meet the following: FIPS PUB 198-1, "The Keyed-Hash Message Authentication Code, and FIPS PUB 180-3, “Secure Hash Standard.”

6.3.14. FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication)

(selected with FCS_PCC_EXT.1, FCS_KDF_EXT.1.1)
Hierarchical to: No other components.
Dependencies: FCS_CKM.1(b) Cryptographic key generation (Symmetric Keys)]
FCS_COP.1(c) Cryptographic operation (Hash Algorithm),
FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction

FCS_COP.1.1(h) Refinement: The TSF shall perform [**keyed-hash message authentication**] in accordance with [***HMAC-SHA-256***] and cryptographic key sizes [256] that meet the following: [**ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”**; ISO/IEC 10118].

6.3.15. FCS_TLS_EXT.1 Extended: TLS selected

(selected in FTP_ITC.1.1, FTP_TRP.1.1)
Hierarchical to: No other components.
Dependencies: FCS_CKM.1(a) Cryptographic Key Generation (for asymmetric Keys)
FCS_COP.1(a) Cryptographic Operation (Symmetric encryption/decryption)
FCS_COP.1(b) Cryptographic Operation (for signature generation/verification)
FCS_COP.1(c) Cryptographic Operation (Hash Algorithm)
FCS_COP.1(g) Cryptographic Operation (for keyed-hash message authentication)
FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [***TLS 1.2 (RFC 5246)***] supporting the following ciphersuites:

Mandatory Ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Optional Ciphersuites:
[
- *TLS_RSA_WITH_AES_256_CBC_SHA*
- *TLS_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_RSA_WITH_AES_256_CBC_SHA256*

].

6.3.16. FCS_HTTPS_EXT.1 Extended: HTTPS selected

Hierarchical to: No other components.
Dependencies: No dependencies.

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

6.3.17. FCS_KDF_EXT Extended: Cryptographic Key Derivation

(for O.STORAGE_ENCRYPTION)
Hierarchical to: No other components.
Dependencies: FCS_COP.1(h) Cryptographic Operation (for keyed-hash message authentication),
[if selected: FCS_RBG_EXT.1 Extended: Cryptographic Operation (Random Bit Generation)]

FCS_KDF_EXT.1.1 The TSF shall accept [***a RNG generated submask as specified in FCS_RBG_EXT.1***] to derive an intermediate key, as defined in [***NIST SP 800-108 [KDF in Counter Mode]***], using the keyed-hash functions specified in FCS_COP.1(h), such that the output is at least of equivalent security strength (in number of bits) to the BEV.

6.3.18. FCS_KYC_EXT.1 Extended: Key Chaining

(for O.STORAGE_ENCRYPTION)
Hierarchical to: No other components.
Dependencies: [FCS_COP.1(e) Cryptographic operation (Key Wrapping),
FCS_SMC_EXT.1 Extended: Submask Combining,
FCS_COP.1(i) Cryptographic operation (Key Transport),
FCS_KDF_EXT.1 Cryptographic Operation (Key Derivation),
and/or FCS_COP.1(f) Cryptographic operation (Key Encryption)].

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [***intermediate keys originating from one or more submask(s) to the BEV or DEK using the following method(s)***: [***key combining as specified in FCS_SMC_EXT.1, key encryption as specified in FCS_COP.1(f), key derivation as specified in FCS_KDF_EXT.1***]] while maintaining an effective strength of [***128 bits***].

Copyright© 2024 TOSHIBA TEC. All rights reserved.

6.4. Class FDP: User Data Protection

6.4.1. FDP_ACC.1 Subset access control

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 **Refinement:** The TSF shall enforce the **User Data Access Control SFP** on subjects, objects, and operations among subjects and objects specified in **Table 14** and **Table 15.**

Table 14 D.USER.DOC Access Control SFP

		"Create"	"Read"	"Modify"	"Delete"
Print	*Operation:*	*Submit a document to be printed*	*View image or Release printed output*	*Modify stored document*	*Delete stored document*
	Job owner	(note 1)		denied	
	U.ADMIN(a)		denied	denied	
	U.NORMAL(a)		denied	denied	denied
	U.ACCOUNTMANAGER	denied	denied	denied	denied
	U.FAXOPERATOR	denied	denied	denied	denied
	U.ADDRESSBOOKOPERATOR	denied	denied	denied	denied
	Unauthenticated	(condition 1)	denied	denied	denied
Scan	*Operation:*	*Submit a document for scanning*	*View scanned image*	*Modify stored image*	*Delete stored image*
	Job owner	(note 2)			
	U.ADMIN(a)		denied	denied	
	U.NORMAL(a)		denied	denied	denied
	U.ACCOUNTMANAGER	denied	denied	denied	denied
	U.FAXOPERATOR	denied	denied	denied	denied
	U.ADDRESSBOOKOPERATOR	denied	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Copy	*Operation:*	*Submit a document for copying*	*View scanned image or Release printed copy output*	*Modify stored image*	*Delete stored image*
	Job owner	(note 2)		denied	
	U.ADMIN(a)		denied	denied	
	U.NORMAL(a)		denied	denied	denied
	U.ACCOUNTMANAGER	denied	denied	denied	denied
	U.FAXOPERATOR	denied	denied	denied	denied

Copyright© 2024 TOSHIBA TEC. All rights reserved.

		"Create"	"Read"	"Modify"	"Delete"
	U.ADDRESSBOOKOPERATOR	denied	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax send	*Operation:*	*Submit a document to send as a fax*	*View scanned image*	*Modify stored image*	*Delete stored image*
	Job owner	(note 2)			
	U.ADMIN(a)		denied	denied	
	U.NORMAL(a)		denied	denied	denied
	U.ACCOUNTMANAGER	denied	denied	denied	denied
	U.FAXOPERATOR		denied	denied	denied
	U.ADDRESSBOOKOPERATOR	denied	denied	denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax receive	*Operation:*	*Receive a fax and store it*	*View fax image or Release printed fax output*	*Modify image of received fax*	*Delete image of received fax*
	Job owner	(note 3)		denied	
	U.ADMIN(a)	(note 4)		denied	
	U.NORMAL(a)	(note 4)	denied	denied	denied
	U.ACCOUNTMANAGER	(note 4)	denied	denied	denied
	U.FAXOPERATOR	(note 4)		denied	
	U.ADDRESSBOOKOPERATOR	(note 4)	denied	denied	denied
	Unauthenticated	(note 4)	denied	denied	denied

Table 15　D.USER.JOB Access Control SFP

		"Create" *	"Read"	"Modify"	"Delete"
Print	*Operation:*	*Create print job*	*View print queue / log*	*Modify print job*	*Cancel print job*
	Job owner	(note 1)		denied	
	U.ADMIN(a)			denied	
	U.NORMAL(a)			denied	denied
	U.ACCOUNTMANAGER	denied		denied	denied
	U.FAXOPERATOR	denied		denied	denied
	U.ADDRESSBOOKOPERATOR	denied		denied	denied
	Unauthenticated		denied	denied	denied
Scan	*Operation:*	*Create scan job*	*View scan status / log*	*Modify scan job*	*Cancel scan job*
	Job owner	(note 2)		denied	
	U.ADMIN(a)			denied	
	U.NORMAL(a)			denied	denied
	U.ACCOUNTMANAGER	denied		denied	denied

Copyright© 2024 TOSHIBA TEC. All rights reserved.

		"Create" *	"Read"	"Modify"	"Delete"
	U.FAXOPERATOR	denied		denied	denied
	U.ADDRESSBOOKOPERATOR	denied		denied	denied
	Unauthenticated	denied	denied	denied	denied
Copy	*Operation:*	*Create copy job*	*View copy status / log*	*Modify copy job*	*Cancel copy job*
	Job owner	(note 2)		denied	
	U.ADMIN(a)			denied	
	U.NORMAL(a)			denied	denied
	U.ACCOUNTMANAGER	denied		denied	denied
	U.FAXOPERATOR	denied		denied	denied
	U.ADDRESSBOOKOPERATOR	denied		denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax send	*Operation:*	*Create fax send job*	*View fax job queue / log*	*Modify fax send job*	*Cancel fax send job*
	Job owner	(note 2)		denied	
	U.ADMIN(a)			denied	
	U.NORMAL(a)			denied	denied
	U.ACCOUNTMANAGER	denied		denied	denied
	U.FAXOPERATOR			denied	denied
	U.ADDRESSBOOKOPERATOR	denied		denied	denied
	Unauthenticated	denied	denied	denied	denied
Fax receive	*Operation:*	*Create fax receive job*	*View fax receive status / log*	*Modify fax receive job*	*Cancel fax receive job*
	Fax owner	(note 3)		denied	denied
	U.ADMIN(a)	(note 4)		denied	denied
	U.NORMAL(a)	(note 4)	denied	denied	denied
	U.ACCOUNTMANAGER	(note 4)	denied	denied	denied
	U.FAXOPERATOR	(note 4)		denied	denied
	U.ADDRESSBOOKOPERATOR	(note 4)	denied	denied	denied
	Unauthenticated	(note 4)	denied	denied	denied

Application note:

Condition 1: *Jobs submitted by unauthenticated users must contain a credential that the TOE can use to identify the Job Owner.*

Note 1: *Job Owner is identified by a credential or assigned to an authorized User as part of the process of submitting a print or storage Job.*

Note 2: *Job Owner is assigned to an authorized User as part of the process of initiating a scan, copy, fax send, or retrieval Job.*

Note 3: *Job Owner of received faxes is assigned by default or configuration. Ownership of received faxes is assigned to U.FAXOPERATOR and U.ADMIN(a) role.*

Note 4: *PSTN faxes are received from outside of the TOE, they are not initiated by Users of the TOE.*

Copyright© 2024 TOSHIBA TEC. All rights reserved.

6.4.2. FDP_ACF.1 Security attribute based access control

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 **Refinement:** The TSF shall enforce the **User Data Access Control SFP** to objects based on the following: subjects, objects, and attributes specified in **Table 14** and **Table 15**.

FDP_ACF.1.2 **Refinement:** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects specified in Table 14 and Table 15***.

FDP_ACF.1.3 **Refinement:** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***none***].

FDP_ACF.1.4 **Refinement:** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***none***].

6.4.3. FDP_FXS_EXT.1 Extended: Fax separation

(for O.FAX_NET_SEPARATION)
Hierarchical to: No other components.
Dependencies: No dependencies.

FDP_FXS_EXT.1.1 The TSF shall prohibit communication via the fax interface, except transmitting or receiving User Data using fax protocols.

6.4.4. FDP_DSK_EXT.1 Extended: Protection of Data on Disk

(for O.STORAGE_ENCRYPTION)
Hierarchical to: No other components.
Dependencies: FCS_COP.1(d) Cryptographic operation (AES Data Encryption/Decryption).

FDP_DSK_EXT.1.1 The TSF shall [*perform encryption in accordane with FCS_COP.1(d)*], such that any Field-Replaceable Nonvolatile Storage Device contains no plaintext User Document Data and no plaintext Confidential TSF Data.

FDP_DSK_EXT.1.2 The TSF shall encrypt all protected data without user intervention.

6.5. Class FIA: Identification and Authentication

6.5.1. FIA_AFL.1 Authentication failure handling

(for O.USER_I&A)
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when [***an administrator configurable positive integer within [1 - 30]***] unsuccessful authentication attempts occur related to [***the unsuccessful user authentication attempts of following the last successful authentication or clear of user account lock***].

Copyright© 2024 TOSHIBA TEC. All rights reserved.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [*lockout each account in lockout time, U.ADMIN(a) and U.ACCOUNTMANAGER can release a lockout account*].

6.5.2. FIA_ATD.1 User attribute definition

(for O.USER_AUTHORIZATION)
Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [*User ID, Role*].

6.5.3. FIA_PMG_EXT Extended:Password Management

(for O.USER_I&A)
Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for User passwords:

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [***"!", "@", "#", "$", "^", "*", "(", ")", [refer to Table 16]***];
- Minimum password length shall be settable by an Administrator, and have the capability to require passwords of 15 characters or greater;

Table 16 Other Available Characters

Type of Characters	Available Characters
Punctuation	+ , - . / : ; = ? ¥ _ ` { | } ~ Space
European Special Characters	¢£§ª°µ¿₣€ ÀÁÂÃÄÅÆÇÈÉÊËÌÍÎÏÐÑÒÓÔÕÖØÙÚÛÜÝÞßàáâãäåæçèéêëìíîïðñòóôõö øùúûüýþÿĀāĂăĄąĆćČčĎďĐđĒēĖėĘęĚěĞğĢģĪīĮįıĶĹĺĻļĽľŁłŃŇňŌōŐőŒœŔŕ ŖŗŘřŚśŞŠšŢţŤťŪūŮŰűŲųŸŹźŻżŽžƒЁ ЂЃЄЅІЇЈЉЊЋЌЎЏ А Б В Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я а б в г д е ж з и й к л м н о п т у ф х ц ч ш щ ъ ы ь э ю я ё ђѓєѕіїјљњћќўџҐΆΈΉΊΌΎΩΐάέήίΰαβγδεζηθικλμνξοπρςσ τυφχψωϊϋόύώ

6.5.4. FIA_UAU.1 Timing of authentication

(for O.USER_I&A)
Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 **Refinement:** The TSF shall allow [***storing the document data from printer driver, receive PSTN Fax data***] on behalf of the user to be performed before the user is authenticated.

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

Copyright© 2024 TOSHIBA TEC. All rights reserved.

6.5.5. FIA_UAU.7 Protected authentication feedback

(for O.USER_I&A)
Hierarchical to: No other components.
Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [***display dummy characters***] to the user while the authentication is in progress.

6.5.6. FIA_UID.1 Timing of identification

(for O.USER_I&A and O.ADMIN_ROLES)
Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UID.1.1 **Refinement:** The TSF shall allow [***receive PSTN fax data***] on behalf of the user to be performed before the user is identified.

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

6.5.7. FIA_USB.1 User-subject binding

(for O.USER_I&A)
Hierarchical to: No other components.
Dependencies: FIA_ATD.1 User attribute definition

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [***User ID, Role***].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [***none***].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [***none***].

6.6. Class FMT: Security Management

6.6.1. FMT_MOF.1 Management of security functions behavior

(for O.ADMIN_ROLES)
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1 The TSF shall restrict the ability to [***disable, enable***] the functions [***Secure Channel***] to ***U.ADMIN(a)***.

6.6.2. FMT_MSA.1 Management of security attributes

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control,
~~FDP_IFC.1 Subset information flow control~~]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

Copyright© 2024 TOSHIBA TEC. All rights reserved.

FMT_MSA.1.1 **Refinement:** The TSF shall enforce the **User Data Access Control SFP** to restrict the ability to [***query, modify, delete, [create, export]***] the security attributes [***User ID, Role***] to [*refer to* ***Table 17***].

Table 17 Security Attributes List

Security Attributes	Operation	Role
User ID	*create, modify, query , delete, export*	***U.ADMIN(a)***
	query, export	***U.ACCOUNTMANAGER***
	query	***U.NORMAL, U.ADDRESSBOOKOPERATOR***
User ID (Except for U.ADMIN(a))	*create, modify, delete*	***U.ACCOUNTMANAGER***
Role	*create, modify, query, delete, export*	***U.ADMIN(a)***
	query, export	***U.ACCOUNTMANAGER***
	query	***U.NORMAL U.ADDRESSBOOKOPERATOR***
Role (Except for U.ADMIN(a))	*create, modify, delete*	***U.ACCOUNTMANAGER***

6.6.3. FMT_MSA.3 Static attribute initialization

(for O.ACCESS_CONTROL and O.USER_AUTHORIZATION)
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 **Refinement:** The TSF shall enforce the **User Data Access Control SFP** to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 **Refinement:** The TSF shall allow the [***no role***] to specify alternative initial values to override the default values when an object or information is created.

6.6.4. FMT_MTD.1 Management of TSF data

(for O.ACCESS CONTROL)
Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1 **Refinement:** The TSF shall restrict the ability to **perform the specified operations on the specified TSF Data to the roles specified in Table 18**.

Table 18 Management of TSF Data

Data	Operation	Authorised role(s)
User Password of *U.NORMAL*	*modify*	***the owning U.NORMAL***
	modify, export	***U.ADMIN(a) U.ACCOUNTMANAGER***
User Password of *U.ADMIN(a)*	*modify, export*	***U.ADMIN(a)***
User Password of *U.ACCOUNTMANAGER*	*modify, export*	***U.ADMIN(a), U.ACCOUNTMANAGER***

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Data	Operation	Authorised role(s)
User Password of *U.ADDRESSBOOKOPERATOR*	modify	***the owning U.ADDRESSBOOKOPERATOR***
	modify, export	***U.ADMIN(a), U.ACCOUNTMANGER***
Allowable Number of entry for Login Password	modify	***U.ADMIN(a)***
Lockout Time	modify	***U.ADMIN(a)***
Locked-out Account Status	clear	***U.ADMIN(a), U.ACCOUNTMANGER***
Auto Logout Time	modify	***U.ADMIN(a)***
Date and Time Information	modify	***U.ADMIN(a)***
Minimum Password Length	modify	***U.ADMIN(a)***
Address Book	create, modify, delete	***U.ADMIN(a), U.ADDRESSBOOKOPERATOR***
SYSLOG Server Settings	modify	***U.ADMIN(a)***
FTP Server Settings	modify	***U.ADMIN(a)***
Software	query, modify	***U.ADMIN(a)***

6.6.5. FMT_SMF.1 Specification of Management Functions

(for O.USER_AUTHORIZATION, O.ACCESS_CONTROL, and O.ADMIN_ROLES)
Hierarchical to: No other components.
Dependencies: No dependencies.

FMT_SMF.1.1: The TSF shall be capable of performing the following management functions: [*refer to* ***Table 19***].

Table 19 Management Functions

SFR	Management	Management Functions	Reason
FAU_GEN.1	There are no management activities foreseen.	None	-
FAU_GEN.2	There are no management activities foreseen.	None	-
FAU_STG_EXT.1	The TSF shall have the ability to configure the cryptographic functionality.	None	This function is not provided.
FCS_CKM.1(b)	There are no management activities foreseen.	None	-
FCS_CKM.4	There are no management activities foreseen.	None	-
FCS_CKM_EXT.4	There are no management activities foreseen.	None	-
FCS_COP.1(b)	There are no management activities foreseen.	None	-
FCS_COP.1(c)	There are no management activities foreseen.	None	-
FCS_COP.1(d)	There are no management activities foreseen.	None	-

Copyright© 2024 TOSHIBA TEC. All rights reserved.

SFR	Management	Management Functions	Reason
FCS_COP.1(f)	There are no management activities foreseen.	None	-
FCS_COP.1(g)	There are no management activities foreseen.	None	-
FCS_COP.1(h)	There are no management activities foreseen.	None	-
FCS_RBG_EXT.1(a)	There are no management activities foreseen.	None	-
FCS_RBG_EXT.1(b)	There are no management activities foreseen.	None	-
FCS_TLS_EXT.1	There are no management activities foreseen.	None	-
FCS_HTTPS_EXT.1	There are no management activities foreseen.	None	-
FCS_KDF_EXT.1	There are no management activities foreseen.	None	-
FCS_KYC_EXT.1	There are no management activities foreseen.	None	-
FDP_ACC.1	There are no management activities foreseen.	None	-
FDP_ACF.1	a) Management of attributes used for decision based on explicit access or denial.	None	The default value of an attribute is fixed and cannot be changed.
FDP_FXS_EXT.1	There are no management activities foreseen.	None	-
FDP_DSK_EXT.1	There are no management activities foreseen.	None	-
FIA_AFL.1	a) Management of the threshold for unsuccessful authentication attempts	Management of unsuccessful user authentication processing	-
	b) Management of actions which are taken for the unsuccessful authentication events	None	It is a predefined action and not managed.
FIA_ATD.1	a) If “assigned”, an authorized administrator can define additional security attributes to a user.	None	This function is not provided.
FIA_PMG_EXT.1	There are no management activities foreseen.	Minimum Password Length management	-

Copyright© 2024 TOSHIBA TEC. All rights reserved.

SFR	Management	Management Functions	Reason
FIA_UAU.1	a) Authentication data management by an administrator	・Management of User Password (U.ACCOUNTMANAGER/U.ADMIN(a) /U.NORMAL /U.ADDRESSBOOKOPERATOR) by U.ADMIN(a). ・Management of User Password (U.ACCOUNTMANAGER/U.NORMAL/U.ADDRESSBOOKOPERATOR) by U.ACCOUNTMANAGER	-
	b) Authentication data management by a relative user	・Management of own User Password by U.NORMAL ・Management of own User Password by U.ADDRESSBOOKOPERATOR	-
	c) List of actions to be taken before user authentication shall be managed.	None	It is a predefined action and not managed.
FIA_UAU.7	There are no management activities foreseen.	None	-
FIA_UID.1	a) Management of User Identity	Management of User ID	-
	b) If an authorized administrator can change the authorized actions before identification, the action list must be controlled.	None	It is a predefined action and not managed.
FIA_USB.1	a) An authorized administrator can define security attributes for a default subject.	None	There are no permitted roles.
	b) An authorized administrator can change security attributes of a subject.	None	There are no permitted roles.
FMT_MOF.1	a) Groups of roles which may affect reciprocally with the TSF Functions shall be managed.	None	It is a predefined action and not managed.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

SFR	Management	Management Functions	Reason
FMT_MSA.1	a) Groups of roles which may affect reciprocally with the Security Attributes shall be managed.	None	It is a predefined action and not managed.
	b) Rules for which the Security Attributes take over any particular values shall be managed.	None	It is a predefined action and not managed.
FMT_MSA.3	a) Groups which may be able to identify the default value shall be managed.	None	There are no roles to specify the default value.
	b) Restrictive or permissive settings of the default value for the prescribed access control SFP shall be managed.	None	The default value is fixed and cannot be changed.
	c) Rules for which the Security Attributes take over any particular values shall be managed.	None	The rules cannot be changed.
FMT_MTD.1	a) Groups of roles which may affect reciprocally with the TSF Data shall be managed.	None	It is a predefined action and not managed.
FMT_SMF.1	There are no management activities foreseen.	None	-
FMT_SMR.1	a) Management of Groups of Users who are part of the Role.	None	It is a predefined action and not managed.
FPT_SKP_EXT.1	There are no management activities foreseen.	None	-
FPT_STM.1	a) Maqnagement of time	Management of the time stamp settings	-
FPT_TST_EXT.1	There are no management activities foreseen.	None	-
FPT_TUD_EXT.1	There are no management activities foreseen.	Management of the Software	-
FTA_SSL.3	a) Specification of the time in which an user who may cause termination of the interactive session between each user is non-active	None	Users cannot configure the setting individually.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

SFR	Management	Management Functions	Reason
	b) Specification of the default time in which an user who may cause termination of the interactive session is non-active	Specification of the default time in which a user is non-active after a session finishes.	-
FTP_ITC.1	a) Configuration of actions which require the trusted channle, if supported.	Secure channel settings	-
FTP_TRP.1(a)	a) Configuration of actions which require the trusted path, if supported.	None	It is a predefined action and not managed.
FTP_TRP.1(b)	a) Configuration of actions which require the trusted path, if supported.	None	It is a predefined action and not managed.
-	-	・Address Book management ・SYSLOG Server Settings ・FTP Server Settings	-

6.6.6. FMT_SMR.1 Security roles

(for O.ACCESS_CONTROL, O.USER_AUTHORIZATION, and O.ADMIN_ROLES)
Hierarchical to: No other components.
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles *U.ADMIN(a), U.ACCOUNTMANAGER, U.ADDRESSBOOKOPERATOR, and U.NORMAL*.

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

6.7. Class FPT: Protection of the TSF

6.7.1. FPT_SKP_EXT.1 Extended: Protection of TSF Data

(for O.COMMS_PROTECTION)
Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

6.7.2. FPT_STM.1 Reliable time stamps

(for O.AUDIT)
Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.7.3. FPT_TST_EXT.1 Extended: TSF testing

(for O.TSF_SELF_TEST)

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_TST_EXT.1.1 The TSF shall run a suite of self-tests during initial start-up (and power on) to demonstrate the correct operation of the TSF.

6.7.4. FPT_TUD_EXT.1 Extended: Trusted Update

(for O.UPDATE_VERIFICATION)
Hierarchical to: No other components.
Dependencies: FCS_COP.1(b) Cryptographic Operation (for signature generation/verification),
FCS_COP.1(c) Cryptographic operation (Hash Algorithm).

FPT_TUD_EXT.1.1 The TSF shall provide authorized administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide authorized administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a digital signature mechanism and [***no other functions***] prior to installing those updates.

6.7.5. FPT_KYP_EXT.1 Extended: Protection of Key and Key Material

(for O.KEY_MATERIAL)
Hierarchical to: No other components.
Dependencies: No dependencies.

FPT_KYP_EXT.1.1 **Refinement:** The TSF shall not store plaintext keys that are part of the keychain specified by FCS_KYC_EXT.1 in **any Field-Replaceable Nonvolatile Storage Device**.

6.8. Class FTA: TOE Access

6.8.1. FTA_SSL.3 TSF-initiated termination

(for O.USER_I&A)
Hierarchical to: No other components.
Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [***refer to Table 20***].

Table 20 Time Interval of User Inactivity

Interface	Auto Logout Time
Control Panel	15 - 150 Sec.
Web Browser	5 - 999 Min.
Printer Driver	There is no inactive sessions

6.9. Class FTP: Trusted Paths/Channels

6.9.1. FTP_ITC.1 Inter-TSF trusted channel

(for O.COMMS_PROTECTION, O.AUDIT)
Hierarchical to: No other components.
Dependencies: [FCS_IPSEC_EXT.1 Extended: IPsec selected, or
FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or

Copyright© 2024 TOSHIBA TEC. All rights reserved.

FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_ITC.1.1 **Refinement:** The TSF shall **use [*TLS*] to** provide **a trusted** communication channel between itself and **authorized IT entities supporting the following capabilities:** [***[SYSLOG server, Ftp server, mail server]***] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

FTP_ITC.1.2 **Refinement:** The TSF shall permit **the TSF, or the authorized IT entities**, to initiate communication via the trusted channel

FTP_ITC.1.3 **Refinement:** The TSF shall initiate communication via the trusted channel for [***SYSLOG service, FTP service, mail service***].

6.9.2. FTP_TRP.1(a) Trusted path (for Administrators)

(for O.COMMS_PROTECTION)
Hierarchical to: No other components.
Dependencies: [FCS_IPSEC_EXT.1 Extended: IPsec selected, or
FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or
FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_TRP.1.1(a) **Refinement:** The TSF shall **use** [***TLS, TLS/HTTPS***] **to** provide **a trusted** communication path between itself and **remote administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data**.

FTP_TRP.1.2(a) **Refinement:** The TSF shall permit **remote administrators** to initiate communication via the trusted path

FTP_TRP.1.3(a) **Refinement:** The TSF shall require the use of the trusted path for **initial administrator authentication and all remote administration actions**.

6.9.3. FTP_TRP.1(b) Trusted path (for Non-administrators)

(for O.COMMS_PROTECTION))
Hierarchical to: No other components.
Dependencies: [FCS_IPSEC_EXT.1 Extended: IPsec selected, or
FCS_TLS_EXT.1 Extended: TLS selected, or
FCS_SSH_EXT.1 Extended: SSH selected, or
FCS_HTTPS_EXT.1 Extended: HTTPS selected].

FTP_TRP.1.1(b) **Refinement:** The TSF shall **use** [***TLS, TLS/HTTPS***] **to** provide **a trusted** communication path between itself and **remote** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **disclosure and detection of modification of the communicated data**.

FTP_TRP.1.2(b) **Refinement:** The TSF shall permit [***remote users***] to initiate communication via the trusted path

FTP_TRP.1.3(b) **Refinement:** The TSF shall require the use of the trusted path for **initial user authentication and all remote user actions**.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

6.10. Security Assurance Requirements

Table 21 lists the security assurance requirements for the Protection Profile for Hardcopy Devices – v1.0. ASE_SPD.1 is added to the component set defined in EAL1 of the evaluation assurance level in this table.

Table 21 TOE Security Assurance Requirements

Assurance Class	Assurance Component	Assurance Components Description
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic functional specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Assurance Class	ALC_CMC.1	Labelling of the TOE
	ALC_CMS.1	TOE CM coverage
Tests	ATE_IND.1	Independent testing – Conformance
Vulnerability assessment	AVA_VAN.1	Vulnerability survey

6.11. Security Functional Requirements Rationale

6.11.1. Dependencies of Security Functional Requirements Documents

Table 22 shows the analysis results of dependencies for the TOE Security Functional Requirements in this ST.

Table 22 Analysis Results of Dependencies for Security Functional Requirements

TOE Security Functional Requirements	Dependencies Required by CC and PP	Fulfilled Dependencies in ST	Un-fulfilled Dependencies in ST	Reason
FAU_GEN.1	FPT_STM.1	FPT_STM.1	None	
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.1	None	
FAU_STG_EXT.1	FAU_GEN.1, FTP_ITC.1	FAU_GEN.1, FTP_ITC.1	None	
FCS_CKM.1(a)	[FCS_COP.1(b), or FCS_COP.1(i)], FCS_CKM_EXT.4	FCS_COP.1(b), FCS_CKM_EXT.4	None	
FCS_CKM.1(b)	[FCS_COP.1(a), or FCS_COP.1(d), or FCS_COP.1(e), or FCS_COP.1(f), or FCS_COP.1(g), or FCS_COP.1(h)], FCS_CKM_EXT.4, FCS_RBG_EXT.1	FCS_COP.1(a), FCS_COP.1(g), FCS_CKM_EXT.4, FCS_RBG_EXT.1(a), FCS_RBG_EXT.1(b)	None	

Copyright© 2024 TOSHIBA TEC. All rights reserved.

TOE Security Functional Requirements	Dependencies Required by CC and PP	Fulfilled Dependencies in ST	Un-fulfilled Dependencies in ST	Reason
FCS_CKM.4	[FCS_CKM.1(a), or FCS_CKM.1(b)]	FCS_CKM.1(a), FCS_CKM.1(b)	None	
FCS_CKM_EXT.4	[FCS_CKM.1(a) or FCS_CKM.1(b)], FCS_CKM.4	FCS_CKM.1(a), FCS_CKM.1(b), FCS_CKM.4	None	
FCS_COP.1(a)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	None	
FCS_COP.1(b)	[FCS_CKM.1(a)], FCS_CKM_EXT.4	FCS_CKM.1(a) FCS_CKM_EXT.4	None	
FCS_COP.1(c)	None	None	None	
FCS_COP.1(d)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	None	
FCS_COP.1(f)	FCS_CKM.1(b), FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	None	
FCS_COP.1(g)	[FCS_CKM.1(b)], FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_CKM_EXT.4	None	
FCS_COP.1(h)	FCS_CKM.1(b), FCS_COP.1(c), FCS_CKM_EXT.4	FCS_CKM.1(b), FCS_COP.1(c), FCS_CKM_EXT.4	None	
FCS_SMC_EXT.1	FCS_COP.1(c)	FCS_COP.1(C)	None	
FCS_RBG_EXT.1(a)	None	None	None	
FCS_RBG_EXT.1(b)	None	None	None	
FCS_TLS_EXT.1	FCS_CKM.1(a), FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(g), FCS_RBG_EXT.1	FCS_CKM.1(a), FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(g), FCS_RBG_EXT.1(b)	None	
FCS_HTTPS_EXT.1	FCS_TLS_EXT.1	FCS_TLS_EXT.1	None	
FPT_KYP_EXT.1	None	None	None	
FCS_KYC_EXT.1	[FCS_COP.1(e), FCS_SMC_EXT.1, FCS_COP.1(i), FCS_KDF_EXT.1, and/or FCS_COP.1(f)]	FCS_KDF_EXT.1, FCS_SMC_EXT.1, FCS_COP.1(f)	None	
FCS_KDF_EXT.1	FCS_COP.1(h)	FCS_COP.1(h)	None	
FDP_DSK_EXT.1	FCS_COP.1(d)	FCS_COP.1(d)	None	
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	None	
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3	None	
FDP_FXS_EXT.1	None	None	None	
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	None	
FIA_ATD.1	None	None	None	
FIA_PMG_EXT.1	None	None	None	
FIA_UAU.1	FIA_UID.1	FIA_UID.1	None	
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	None	

Copyright© 2024 TOSHIBA TEC. All rights reserved.

TOE Security Functional Requirements	Dependencies Required by CC and PP	Fulfilled Dependencies in ST	Un-fulfilled Dependencies in ST	Reason
FIA_UID.1	None	None	None	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	None	
FMT_MOF.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	None	
FMT_MSA.1	[FDP_ACC.1], FMT_SMR.1, FMT_SMF.1	FDP_ACC.1, FMT_SMR.1, FMT_SMF.1	None	
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1	None	
FMT_MTD.1	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1	None	
FMT_SMF.1	None	None	None	
FMT_SMR.1	FIA_UID.1	FIA_UID.1	None	
FPT_SKP_EXT.1	None	None	None	
FPT_STM.1	None	None	None	
FPT_TST_EXT.1	None	None	None	
FPT_TUD_EXT.1	FCS_COP.1(b), FCS_COP.1(c)	FCS_COP.1(b), FCS_COP.1(c)	None	
FTA_SSL.3	None	None	None	
FTP_ITC.1	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	FCS_TLS_EXT.1, FCS_HTTPS_EXT.1	None	
FTP_TRP.1(a)	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1]	FCS_TLS_EXT.1, FCS_HTTPS_EXT.1	None	
FTP_TRP.1(b)	[FCS_IPSEC_EXT.1, or FCS_TLS_EXT.1, or FCS_SSH_EXT.1, or FCS_HTTPS_EXT.1	FCS_TLS_EXT.1, FCS_HTTPS_EXT.1	None	

6.11.2. Security Assurance Requirements Rationale

The rationale for choosing these security assurance requirements is that they define a minimum security baseline that is based on the anticipated threat level of the attacker, the security of the Operational Environment in which the TOE is deployed, and the relative value of the TOE itself. The assurance activities throughout the ST are used to provide tailored guidance on the specific expectations for completing the security assurance requirements.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

7. TOE Summary Specification

Summary Specification of the TOE Security Functionality (TSF) is described in this Chapter.

7.1. Audit

The Summary Specification of the Class FAU Requirements is described as follows.

FAU_GEN.1

The TOE generates audit logs and record them in the audit log file when audit-relevant events occur. This causes FAU_GEN.1 to be realized.

Table 23 Recorded Events and Audit Logs

Auditableevents	Events	Recorded User ID	Result
Start-up of audit functions	MFP power-on	None	None
Shutdown of audit functions	MFP power-off	None	None
Job completion	Print job completion	Job owner	Success or failure
	Scan job completion	Job owner	Success or failure
	Copy job completion	Job owner	Success or failure
	Fax transmission job completion	Job owner	Success or failure
	Fax reception job completion	Job owner	Success or deletion
Unsuccessful user authentication and identification	Failure of login	Logged in User	Success or failure
Unsuccessful user identification	Failure of login (Print Job)	User not registered in the TOE	Failure
Use of management functions	Addition of User	User who made modifications	Success or failure
	Change of User ID	User who made modifications	Success or failure
	Deletion of User	User who made modifications	Success
	Management of unsuccessful user authentication processing、Minimum Password Length management、Management of User Password (U.ACCOUNTMANAGER/U.ADMIN(a) /U.NORMAL/U.ADDRESSBOOKOPERATOR) by U.ADMIN(a)、Management of User Password(U.ACCOUNTMANAGER/U.NORMAL/U.ADDRESSBOOKOPERATOR) by U.ACCOUNTMANAGER、Management of own User Password by U.NORMAL、Management of own User Password by U.ADDRESSBOOKOPERATOR、	User who made modifications	Success

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Auditableevents	Events	Recorded User ID	Result
	Management of the Software、 Specification of the default time in which a user is non-active after a session finishes、 Secure channel settings、 Address Book management、 SYSLOG Server Settings、 FTP Server Settings		
Modification to the group of Users that are part of a role	Change of the role information	User who made modifications	Success
Changes to the time	Modification of the time	User who made modifications	Success
Failure to establish session	Failure of TLS session establishment	None	Success or failure

The TOE adds the following data to the events to be audited.

- Date and Time: Time when an error/event occurred.
- Message: Sentence which describes the event content (Reason of failure when session failed)
- Error Code: An event is defined as a code, and represented as 4-digit hexadecimal numbers.
- User ID: Identifier of a Logged in user
- Result: Result of event implementation

[Relevant TSFI]

- Control Panel: Login, Home screen, Copy, Simple Copy, Scan, Simple Scan, Fax transmission, Print, Job display and Log display, Admin settings, Power key
- TopAccess: Login, Job status, Account, User management, Admin settings
- Printer Driver: Interface to a Print request
- Others: Main switch, PSTN Fax interface

FAU_GEN.2

If an auditable event occurs, the TOE realizes FAU_GEN.2 by attaching the user ID of a user who caused the event to the audit log.

[Relevant TSFI]

- Control Panel: Login, Home screen, Copy, Simple Copy, Scan, Simple Scan, Fax transmission, Print, Job display and Log display, Admin settings, Power key
- TopAccess: Login, Job status, Account, User management, Admin settings
- Printer Driver: Interface to a Print request
- Others: Main switch, PSTN Fax interface

FAU_STG_EXT.1

U.ADMIN(a) can set the SYSLOG server as the server where an audit log is transferred from the Admin settings in TopAccess.

The TOE can save the generated audit log to the internal storage device first, then transfer the data to the SYSLOG server which is the external audit log server using the communication protocol TLS1.2. The maximum number of records which can be stored in the storage area of

Copyright© 2024 TOSHIBA TEC. All rights reserved.

the audio log in the internal storage is as follows: 10,000 message logs, 5,000 print logs, 5,000 scan logs, 5,000 Fax transmission journals, and 5,000 Fax reception journals. When the maximum number of records of each log reaches the limit, the oldest audit data will be deleted to save the newest one.
Only U.ADMIN(a) can refers to all the audit logs which were saved to the internal storage and other users can refer to own job log only by access control.

[Relevant TSFI]

- Control Panel: Login, Home screen, Copy, Simple Copy, Scan, Simple Scan, Fax transmission, Print, Job display and Log display, Admin settings, Power key
- TopAccess: Login, Job status, Account, User management, Admin settings
- Printer Driver: Interface to a Print request
- Others: Main switch, PSTN Fax interface

7.2. Cryptographic Support

The following describes the summary specifications for requirements of Class FCS.

FCS_CKM.1(a)

The TOE creates the RSA key pair as the asymmetric cryptographic key used for server certificate for TLS communication by the rsakpg1-crt method described in Section 6.3.1.3. of NIST SP 800-56B, Revision 1. Random numbers used for key creation is created by CTR_DRBG (AES) according to FCS_RBG_EXT.1(b). In accordance with FDP_DSK_EXT.1 and FCS_CKM.1(d), the server certificate and server private key, including the generated public key, are encrypted and stored on the SSD. The TOE does not include the TOE-specific extensions, unique processing which is not written in HCD-PP, or another implementation which is permitted, for the TSF.
The following shows the TSFI related to this requirement.

[Relevant TSFI]

- TopAccess: Admin settings

FCS_CKM.1(b)

The TSF creates a session key and HMAC key for communication at the TLS communication negotiation. The session key and HMAC key are created from the random number shared between the server and client. The random number is created by CTR_DRBG (AES) according to FCS_RBG_EXT.1(b). The parameters of each key differ depending on the selected Cipher Suite as shown below.

- Session key
  A session key is used for encrypting the communication data. The used cryptographic algorithm and key length differ depending on the selected Cipher Suite. The cryptographic algorithm uses AES-CBC, and 128bit and 256bit can be selected as the session key length.
- HMAC key
  A HMAC key is used to verify the integrity of communication data, with the selected cipher suite determining the cryptographic algorithms and key lengths used. The cryptographic algorithms employed are HMAC-SHA-1 or HMAC-SHA-256, in accordance with FCS_COP.1(g), with HMAC key lengths of 160 bits and 256 bits, respectively.

These keys are saved to the volatile memory and deleted by turning off the power.

[Relevant TSFI]

- Control Panel: Login, Home screen, Copy, Simple Copy, Scan, Simple Scan, Fax transmission, Print, Job display and Log display, Admin settings, Power key

Copyright© 2024 TOSHIBA TEC. All rights reserved.

- TopAccess: Login, Job status, Account, User management, Admin settings
- Printer Driver: Interface to a Print request
- Others: Main switch, PSTN Fax interface

The TSF generates the following keys for storage encryption. These keys are protected in accordance with FPT_KYP_EXT.1.

- KEK Derivation Key and Key Material Encryption Key
  These keys are used to protect keys and key materials, with one generated for each at the time of TOE setup. In accordance with FCS_RBG_EXT.1(a), a 256-bit random number is generated using Hash_DRBG (SHA-512), which is then split into two 128-bit segments to form the 128-bit KEK derivation key and the 128-bit key material encryption key, stored in volatile memory and FROM.

- DEK
  This key used to protect user document data and confidential TSF data is generated individually for each encryption partition at the time of TOE setup. In accordance with FCS_RBG_EXT.1(b), a 128-bit random number is generated using CTR_DRBG (AES) and stored in volatile memory as the DEK for that encryption partition. In accordance with FPT_KYP_EXT.1 and FCS_COP.1(f), the key materials, including the DEK, are encrypted and stored in an encrypted state on the SSD.

- DEK for the Swapping Partition
  This key is used to protect swapped-out data and is generated once at TOE start-up. In accordance with FCS_RBG_EXT.1(b), a 128-bit random number is generated using CTR_DRBG (AES) and stored only in volatile memory as the DEK for the swapping partition. This key is changed with each TOE start-up.

[Relevant TSFI]
- Control Panel: Power key
- Others: Main switch

FCS_CKM_EXT.4/FCS_CKM.4

The following plaintext secret keys, private cryptographic keys, and cryptographic critical parameters handled by the TSF shall be destroyed of when they are no longer needed.

- KEK derivation key and key material encryption key in the FROM
  The keys used to decrypt user data and confidential TSF data stored in an encrypted state on the SSD are no longer needed when the TOE is decommissioned. Therefore, all CSPs used for decryption become unnecessary. Upon decommissioning the TOE, the areas in the FROM where the keys are stored are treated as unnecessary keys or key materials and are destroyed of by overwriting them once with a fixed value.

[Relevant TSFI]
- Control Panel: Power key
- Others: Main switch

KEK derivation key, key material encryption key, KEK, DEK, DEK for the swapping partition, submask, LUKS key, context for KEK derivation, session keys for communication, HMAC keys, and server secret key stored in volatile memory. All CSPs used for the encryption of user data and secret TSF data, as well as all CSPs for communication, are no longer needed between the time the TOE's power is turned off and on.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

When the power is off, these are treated as unnecessary keys or key material, and the plaintext secret keys and cryptographic critical parameters stored in volatile memory are destroyed.

[Relevant TSFI]

- Control Panel: Power key
- Others: Main switch

FCS_COP.1(a)

The TSF encrypts and decrypts the communication data by operating the 128 bit or 256 bit cryptographic key generated by FCS_CKM.1(b) and AES cryptographic algorithm conforms to FIPS PUB197 in the CBC mode complies with NIST SP 800-38A so as to protect the communication data in FTP_ITC.1, FTP_TRP.1(a), and FTP_TRP.1(b).
The TSFI related to this requirement is as shown below.

[Relevant TSFI]

- Conform to TSFI of FTP_ITC.1, FTP_TRP.1(a), and FTP_TRP.1(b)

FCS_COP.1(b)

The TSF uses the RSA digital signature algorithm (rDSA) of which the key length is 2048bit which complies with the Digital Signature Standard prescribed in FIPS PUB 186-4 for creation of signatures during device certificate creation and verification of the server certificate by FTP_ITC.1 and firmware update by FPT_TUD_EXT.1. The TSF uses RSASSA-PKCS1-v1_5 for creation of the signatures during device certificate creation and verification of the server certificate, and RSASSA-PSS for verification of firmware update. Also, the RSA key generated by FCS_CKM.1 (a) is used for creation of the certificate.
The TSFI related to this requirement is as shown below.

[Relevant TSFI]

- Conform to TSFI of FCS_ITC.1 and FPT_TUD_EXT.1.
- TopAccess: Admin settings

FCS_RBG_EXT.1(a)

The TSF generates random numbers using an entropy source and DRBG to generate the KEK derivation key and the key material encryption key for TOE storage encryption. This DRBG uses Hash_DRBG (SHA-512) to generate random numbers according to NIST SP 800-90A. The entropy source includes a hardware-based noise source, and the amount of entropy provided to the DRBG is described below. The noise source uses the ES of the hardware embedded in SoC (Intel Atom Processor x5-E3930) of the TOE. Output from the noise source is used for seeding the DRBG in SoC, and outputted by the RDRAND instruction after processing according to CTR_DRBG (AES) of NIST SP 800-90A. It is known that the noise source includes the minimum entropy, 0.5bit or more per 1bit, by the description in [Rambus 2012], the RDRAND instruction is the output of the DRBG with the security strength of 128 bits which was initialized at the seed of 256 bit entropy from the noise source. The RDRAND instruction is reseeded from the ES after outputting 511 of 128 bits. Thus, the rngd daemon process which constitutes the entropy source collects the RDRAND instruction output of which the seed differs per 16 bytes by compressing 128*512=65,536bit=8,192bytes acquired by the RDRAND instruction into 16 bytes by the AES-CBC-MAC processing, and temporarily compiles almost full entropy data in the three 2,500 bytes buffers of rngd. When this TSF is used, the parameters are set such that the Linux PRNG holds more than 2048 bits of entropy, so the 128 bytes of data that the TSF's Hash_DRBG (SHA-512) reads from the Linux PRNG's /dev/urandom output is , which is assumed to be almost full entropy. Of the 128 bytes, 96 bytes are used as Entropy Input and Nonce, and are supplied as a seed value for

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Hash_DRBG(SHA-512). From the Minimum entropy estimate in Section 6 of NIST SP800-90B, the TSF developer confirmed that the /dev/urandom output included the minimum entropy, 0.88 bits or more per 1 bit, within the TOE operation conditions range. Even if it is pessimistically estimated that it is not full entropy, it is estimated that the 96 bytes bit string of the /dev/urandom output contains 675.84(=96*8*0.88) bits of entropy by evaluating the lower limit of the amount of entropy according to Section 3.1.5 of NIST SP800-90B.
FCS_RGB_EXT.1 (a) is realized by making this bit string as the Entropy Input and Nonce and supplying the seed value to Hash_DRBG (SHA-512).

[Relevant TSFI]

- Control Panel: Power key (Only for the first start-up after TOE establishment)
- Others: Main switch (Only for the first start-up after TOE establishment)

FCS_RBG_EXT.1(b)

The TSF generates the following random numbers using the entropy source and DRBG: random numbers for generating keys and key material (KEK derivation context, DEK, submask and LUKS key) for each encryption partition for storage encryption of TOE and random numbers for generating server secret keys for TLS communications and for negotiation of TLS communications to protect communication data in FTP_ITC.1、FTP_TRP.1(a) and FTP_TRP.1(b). The CTR_DRBG of the TOE consists of a master DRBG and a private DRBG with the same structure as the CTR_DRBG (AES) according to NIST SP 800-90A. The output of the private DRBG is the random number generated by the TSF, which is used to produce keys and key materials. The entropy source includes a hardware-based noise source, and the amount of entropy supplied to the DRBG is described later. The noise source uses the ES of the hardware embedded in SoC (Intel Atom Processor x5-E3930) of the TOE. Output from the noise source is used for seeding the DRBG in SoC, and outputted by the RDRAND instruction after processing according to CTR_DRBG (AES) of NIST SP 800-90A. It is known that the noise source includes the minimum entropy, 0.5bit or more per 1bit, by the description in [Rambus 2012], the RDRAND instruction is the output of the DRBG with the security strength of 128 bits which was initialized at the seed of 256 bits entropy from the noise source. The RDRAND instruction is reseeded from the ES after outputting 511 of 128 bits. Thus, the rngd daemon process which constitutes the entropy source collects the RDRAND instruction output of which the seed differs per 16 bytes by compressing 128*512=65,536bit=8,192bytes acquired by the RDRAND instruction into 16 bytes by the AES-CBC-MAC processing, and temporarily compiles almost full entropy data in the three 2,500 bytes buffers of rngd. The necessary entropy is sufficiently supplied from rngd to Linux PRNG. So the data read from the /dev/random output of Linux PRNG by the TSF is supposed to be almost full entropy. The TSF developers confirmed that the /dev/random output contains a minimum entropy of more than 0.90 bits per bit over the range of the TOE operating conditions, according to the minimum entropy estimate in Section 6 of NIST SP800-90B. Even if pessimistically estimating that it is not full entropy, it is estimated that the 32 bytes bit string of /dev/random output contains 230.40 (=32*8*0.90) bits of entropy, based on a lower bound evaluation of the amount of entropy according to section 3.1.5 of NIST SP800-90B. Similarly, it is estimated that the 16 bytes bit string in the /dev/random output contains 115.20 (=16*8*0.90) bits of entropy. This 48 bytes bit sequence, referred to as the master DRBG, is used as a seed by concatenating the 32 bytes entropy_input and 16 bytes nonce for initializing the CTR_DRBG (AES). The master DRBG's CTR_DRBG (AES) has a security strength of 128 bits. Additionally, the private DRBG receives the same 32 bytes entropy_input and 16 bytes nonce from the master DRBG. The private DRBG is also considered to have 128-bit security. The use of FCS_RBG_EXT.1(b) invokes the random number generation function of the private DRBG's CTR_DRBG (AES). Regarding reseeding, the master DRBG performs reseeding using a 32 bytes entropy_input derived from /dev/random before up to 2^{32} calls to the private DRBG, along with reseeding of the private DRBG using the master

Copyright© 2024 TOSHIBA TEC. All rights reserved.

DRBG output as its 32 bytes entropy_input. These processes ensure that the private DRBG achieves the 128-bit security strength defined by FCS_RBG_EXT.1(b).

[Relevant TSFI]

- Conform to TSFI of FTP_ITC_EXT.1, FTP_TRP.1(a) and FTP_TRP.1(b)
- Control Panel: Power key (Only for the first start-up after TOE establishment)
- Others: Main switch (Only for the first start-up after TOE establishment)

7.3. Storage Encryption (Conditionally mandatory)

The following describes the summary specifications for the conditional requirements B.1.

FPT_KYP_EXT.1

Keys and key materials identified by the key chain of FCS_KYC_EXT.1 are generated during TOE setup and are protected until TOE decommissioning. As described below for the key storage locations and protection status, the plaintext keys are not stored on nonvolatile storage devices, FRAM or SSD, that is Field-Replaceable. The sizes of the keys and key materials are described in the TSS of FCS_KYC_EXT.1.

- KEK derivation key and Key material encryption key
  The KEK derivation key and the key material encryption key are each generated as a single key in the TOE in accordance with FCS_COP.1(b) and stored in plaintext on the volatile memory and nonvolatile storage device, FROM, that is Field-nonReplaceable.
- KEK Derivation Context
  The KEK derivation context is generated individually from random numbers for each encryption partition of the SSD that stores user data or confidential TSF data, and is stored in volatile memory. The KEK derivation context is encrypted with the key material encryption key in accordance with FCS_COP.1(f) and is then stored in an encrypted state within the management header area at the beginning of the SSD's encryption partition.
- KEK
  The KEK is generated individually for each encryption partition of the SSD that stores user data or confidential TSF data, in accordance with FCS_KDF_EXT.1, using the KEK derivation key, key material encryption key, and KEK derivation context, and is stored only in volatile memory.
- DEK
  The DEK is a separate key generated for each encryption partition of the SSD that stores user data or confidential TSF data, in accordance with FCS_COP.1(b), and is stored only in volatile memory.
- Submask and LUKS Key
  The LUKS data used to derive the submask is generated individually from random numbers for each encryption partition of the SSD that stores user data or confidential TSF data, and is stored in volatile memory. The submask is derived from a specific range of the LUKS data according to the coding generation rules and is stored only in volatile memory. In generating the LUKS key, the submask is XORed with the DEK in accordance with FCS_SMC_EXT.1 to derive the LUKS key, which is stored in volatile memory at the end of the LUKS data (unused portion). The LUKS data, including the LUKS key, is encrypted with the KEK according to FCS_COP.1(f) and is then stored in an encrypted state within the management header area at the beginning of the SSD's encryption partition.

[Relevant TSFI]

- None

Copyright© 2024 TOSHIBA TEC. All rights reserved.

FCS_KYC_EXT.1

The BEV in the TOE's key chain defined by FCS_KYC_EXT.1 is the Data Encryption Key (DEK). During TOE setup, the keys and key materials that constitute the key chain of FCS_KYC_EXT.1 are generated. The key chain consists of the following keys and key materials.

- KEK derivation key and Key material encryption key
  During TOE setup, a 256-bit random number is generated using Hash_DRBG (SHA-512) in accordance with FCS_RBG_EXT.1(a), which is then split into two 128-bit segments to create the KEK derivation key and the key material encryption key. The KEK derivation key and key material encryption key are stored in plaintext in both volatile memory and the FROM. The FROM is a nonvolatile storage that is Field-nonReplaceable. At the time of TOE start-up, the KEK derivation key and key material encryption key read from the FROM are used.

- KEK derivation context
  During TOE setup, a 256-bit random number generated using CTR_DRBG (AES) in accordance with FCS_RBG_EXT.1(b) serves as the KEK derivation context. This context is generated for each encryption partition and is stored in volatile memory as well as in an encrypted state on the SSD. The KEK derivation context is included in the management header, which is encrypted using the 128-bit key material encryption key with AES-CBC in accordance with FCS_COP.1(f) and stored in encrypted form on the SSD. At the time of TOE start-up, the encrypted management header read from the SSD is decrypted using the key material encryption key with AES-CBC in accordance with FCS_COP.1(f), and the KEK derivation context is extracted and stored in volatile memory.

- KEK
  During TOE setup, the KEK derivation key, key material encryption key, and KEK derivation context stored in volatile memory are used in accordance with FCS_KDF_EXT.1. Following the KDF counter mode defined in SP800-108, a 128-bit key is derived using HMAC-SHA-256 as specified in FCS_COP.1(h) and is stored in volatile memory as the KEK. At the time of TOE start-up, the same procedure is followed to derive a 128-bit key, which is again stored in volatile memory as the KEK.

- DEK, Submask, and LUKS key
  During TOE setup, a 128-bit random number generated using CTR_DRBG (AES) in accordance with FCS_RBG_EXT.1(b) serves as the DEK. The DEK is generated for each encryption partition and stored in volatile memory. Next, a 63,984 bytes random number generated using CTR_DRBG (AES) in accordance with FCS_RBG_EXT.1(b) is saved in volatile memory as LUKS data. A 128-bit submask is derived from a specific range of the LUKS data according to coding generation rules and is stored in volatile memory. For LUKS key generation, a 128-bit LUKS key is derived by XORing the 128-bit DEK with the 128-bit submask in accordance with FCS_SMC_EXT.1, and the LUKS key is stored in volatile memory at the end of the LUKS data (unused portion). Then, the 64,000 bytes LUKS data, including the LUKS key, is encrypted using AES-CBC with the 128-bit KEK in accordance with FCS_COP.1(f) and stored in an encrypted state on the SSD. At the time of TOE start-up, the encrypted LUKS data read from the SSD is decrypted using AES-CBC with the 128-bit KEK in accordance with FCS_COP.1(f), from which the submask is derived and the LUKS key is extracted. In generating the DEK, a 128-bit DEK is derived by XORing the 128-bit LUKS key with the 128-bit submask in accordance with FCS_SMC_EXT.1, and the DEK is stored in volatile memory.

- Strength of the key chain
  The KEK derivation key and key material encryption key are each 128 bits, and sufficient entropy is provided in accordance with FCS_RBG_EXT.1(a) and FCS_RBG_EXT.1(b), ensuring a key strength of 128 bits. Since the key derivation processes defined by FCS_KDF_EXT.1 and

Copyright© 2024 TOSHIBA TEC. All rights reserved.

FCS_COP.1(f) also provide 128-bit security strength, 128-bit security strength is maintained at each stage of the key chain.

[Relevant TSFI]

- Control Panel: Power key
- Others: Main switch

FDP_DSK_EXT.1

The TOE's Field-Replaceable Nonvolatile storage consists of two types: FRAM and SSD. In the TOE state, the FRAM stores only non-sensitive data, such as MFP's printing settings and adjustments, and the TOE does not write user document data or confidential TSF data to the disk. User document data and confidential TSF data are stored in an encrypted state only on the SSD. The SSD is divided into partitions, each with its own file system. The following describes the types of the three SSD partitions and the areas that are not encrypted. Details of the keys and key materials used are outlined in the TSS under the section for FCS_KYC_EXT.1.

- Non-encrypted Partition
  This type of partition is used to store any data that is not user document data or confidential TSF data, and it does not include any data subject to data protection requirements outlined in this document.

- Encrypted Partition
  This type of partition is used to store user document data, confidential TSF data, and related data such as core dumps. The transparent encryption function for the encrypted partition starts when the partition is mounted. All files and metadata written to the regular file system created in this partition must be encrypted according to FCS_COP.1(d) before being stored on the SSD in encrypted form via the block device driver. During the read process, the data is decrypted according to FCS_COP.1(d) using the reverse procedure and is read from the file system in plaintext. A 128-bit DEK specific to each encrypted partition is used for the encryption and decryption processes in accordance with FCS_COP.1(d).
  During TOE installation, keys and key materials are generated. First, a single KEK derivation key and key material encryption key are generated in the TOE, and these are stored in plaintext in volatile memory and in Field-nonReplaceable Nonvolatile storage area known as FROM. Next, the transparent encryption functionality for each encrypted partition that stores user data and confidential TSF data is enabled. At this time, the KEK derivation context, KEK, DEK, LUKS data, submask, and LUKS key are generated for each encrypted partition. The KEK derivation context and LUKS data, which includes the LUKS key, are saved in encrypted form on the SSD, excluding the submask derived from the KEK, DEK, and LUKS data.
  First, a 128-bit KEK is derived from the KEK derivation key, key material encryption key, and KEK derivation context in accordance with FCS_KDF_EXT.1 and is stored in volatile memory. The management header containing the KEK derivation context is encrypted with the key material encryption key according to FCS_COP.1(f), while the LUKS data, which includes the LUKS key, is encrypted with the KEK in accordance with FCS_COP.1(f). Each of these encrypted forms is stored in encrypted state at specific locations in the management header area at the beginning of the encrypted partition. Finally, a file system is created in the encrypted partition with the transparent encryption functionality enabled.
  In the TOE state, during start-up, the KEK derivation key and key material encryption key are read from FROM and stored in volatile memory. Next, the ciphertext containing the KEK

Copyright© 2024 TOSHIBA TEC. All rights reserved.

derivation context and the ciphertext of the LUKS data, which includes the LUKS key, are read from the management header area at the beginning of the encrypted partition and stored in volatile memory. The ciphertext containing the KEK derivation context is decrypted using the key material encryption key according to FCS_COP.1(f), and the KEK derivation context is saved in volatile memory. Then, a 128-bit KEK is derived from the KEK derivation key, key material encryption key, and KEK derivation context in accordance with FCS_KDF_EXT.1 and stored in volatile memory.

Next, the ciphertext of the LUKS data containing the LUKS key is decrypted using the KEK according to FCS_COP.1(f), and both the LUKS data and the LUKS key are stored in volatile memory. A DEK is derived by XORing the LUKS key with the submask derived from the LUKS data and stored in volatile memory. The encryption and decryption processes, in accordance with FCS_COP.1(d), using the DEK derived from this series of operations, are then initiated.

- Swap Partition

  The TOE's swap function is a type of partition used to store lower-priority data (swap-out data) when the TOE's volatile memory is under pressure. The transparent encryption function for the swap partition is initiated when the swap partition is mounted. All swap-out data and metadata written to the swap file system of this partition must be encrypted according to FCS_COP.1(d) before being stored in ciphertext state on the SSD via the block device driver. This provides protection under FDP_DSK_EXT even if the swap-out data contains user document data or confidential TSF data. During the read process, the data is decrypted in reverse order according to FCS_COP.1(d), allowing the swap-out data to be read in plaintext from the file system.

  The transparent encryption function for the swap partition is enabled during TOE setup and at the start-up of the TOE state. A 128-bit random number generated using CTR_DRBG(AES) in accordance with FCS_RBG_EXT.1(b) is saved in volatile memory as the DEK for the swap partition. Encryption and decryption processes according to FCS_COP.1(d) are then initiated using this DEK for the transparent encryption function. Following this, the swap file system is created, and the partition is put into use as a swap partition.

- Non-encrypted Area

  The non-encrypted area of the SSD includes the bootloader, partition table, partitions that store data that is neither user document data nor confidential TSF data, and non-encrypted areas for management headers at the beginning of each partition that stores user document data and confidential TSF data. More specifically, the first 1 MiB of each encrypted partition on the SSD is designated for management headers. The management header stored in the ciphertext state occupies 1 KiB starting from 1 KiB of the partition's beginning, and the LUKS data stored in the ciphertext state occupies 64,000 bytes starting from 4 KiB of the partition's beginning. Other areas within the management header area are non-encrypted, but no confidential data is stored there.

[Relevant TSFI]

- Control Panel: Login, Home screen, Copy, Simple Copy, Scan, Simple Scan, Fax transmission, Print, Job display and Log display, Admin settings
- TopAccess: Login, Job status, Account, User management, Admin settings
- Printer Driver: Interface to a Print request
- Others: PSTN Fax interface

Copyright© 2024 TOSHIBA TEC. All rights reserved.

7.4. Storage Encryption (Selective requirements)

The following describes the summary specifications for the requirements D.1 and D.4 selected in Storage Encryption.

FCS_COP.1(f)

The TSF is used for processing the plaintext management header (including the KEK derivation context) and plaintext LUKS data (including the LUKS key), as well as for processing the ciphertext management header (including the KEK derivation context) and ciphertext LUKS data (including the LUKS key) read from the SSD. During TOE installation, the TSF uses the 128-bit key material encryption key generated according to the TSS of FCS_KYC_EXT.1 to encrypt the plaintext management header using AES in CBC mode as specified in ISO/IEC 18033-3 and ISO/IEC 10116. The resulting ciphertext management header is then stored on the SSD. The TSF uses the 128-bit KEK generated in accordance with the TSS of FCS_KYC_EXT.1 during TOE installation to encrypt the plaintext LUKS data using AES in CBC mode as specified in ISO/IEC 18033-3 and ISO/IEC 10116, storing the resulting ciphertext LUKS data on the SSD.
At TOE state start-up, the TSF uses the 128-bit key material encryption key read from FROM in accordance with the TSS of FCS_KYC_EXT.1 to decrypt the ciphertext management header read from the SSD using AES in CBC mode as specified in ISO/IEC 18033-3 and ISO/IEC 10116, storing the resulting plaintext management header in volatile memory.
Additionally, at TOE state start-up, the TSF uses the 128-bit KEK generated in accordance with the TSS of FCS_KYC_EXT.1 to decrypt the ciphertext LUKS data read from the SSD using AES in CBC mode as specified in ISO/IEC 18033-3 and ISO/IEC 10116, storing the resulting plaintext LUKS data in volatile memory.

[Relevant TSFI]

- Control Panel: Power key
- Others: Main switch

FCS_KDF_EXT.1

The TSF utilizes the counter mode KDF defined in NIST SP800-108, employing HMAC-SHA-256 as the PRF, which is specified as the keyed-hash function in FCS_COP.1(h), to derive a 128-bit KEK. The submask for input to the counter mode KDF defined in NIST SP800-108 consists of a 256-bit K_{IN}, which is formed by concatenating the KEK derivation key and the key material encryption key generated as 256-bit random numbers by Hash_DRBG(SHA-512) in accordance with FCS_RBG_EXT.1(a) and split into 128-bit segments. Additionally, a 256-bit KEK derivation context is defined as Context, generated using CTR_DRBG(AES) in accordance with FCS_RBG_EXT.1(b). Therefore, the output meets the conditions for 128-bit security strength. Here, both K_{IN} and Context are submasks generated by the RNG specified in FCS_RBG_EXT.1, thereby satisfying the requirements of the SFR. During TOE setup, a 256-bit value formed by concatenating the KEK derivation key and the key material encryption key, along with the KEK derivation context, is used as the submask for the TSF input. Upon booting after TOE installation, a 256-bit value formed by concatenating the KEK derivation key and the key material encryption key read from FROM, along with the KEK derivation context decrypted from the ciphertext read from the SSD, is used as the submask for the TSF input.
[Relevant TSFI]

- Control Panel: Power key
- Others: Main switch

Copyright© 2024 TOSHIBA TEC. All rights reserved.

FCS_SMC_EXT.1

The TSF generates a 128-bit LUKS key during TOE setup by XORing a 128-bit DEK with a 128-bit submask.

The TSF generates a 128-bit DEK during TOE start-up by XORing a 128-bit LUKS key with a 128-bit submask.

[Relevant TSFI]

- Control Panel: Power key
- Others: Main switch

FCS_COP.1(h)

At the derivation of the KEK from the KEK derivation key, key material encryption key, and KEK derivation context, the TSF uses HMAC-SHA-256 which conforms to ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2” and ISO/IEC 10118 to calculate the keyed-hash message function in FCS_KDF_EXT.1. The HMAC key length is 256 bits, hash function is SHA-256, block length is 512 bits, and outputted MAC output length is 256 bits.

[Relevant TSFI]

- Control Panel: Power key
- Others: Main switch

FCS_COP.1(d)

The TSF transparently encrypts user document data, confidential TSF data, and related data such as core dumps when writing them to the assigned encrypted partitions on the SSD for each data category. To enable transparent encryption of data written to the SSD and decryption of data read from the SSD as the encryption method for storage encryption, encryption and decryption are performed with AES-CBC which is a combination of AES in ISO/IEC 18033-3 and CBC in ISO/IEC 10116 using the 128-bit DEK identified by FCS_KYC_EXT.1 that is generated according to FCS_CKM.1(b) at the time of start-up in TOE state.

The TSF transparently encrypts swap-out data swapped out of the main memory when it is written to the swap partition of the SSD. To enable transparent encryption of data written to the SSD and decryption of data read from the SSD as the encryption method for storage encryption, encryption and decryption are performed with AES-CBC which is a combination of AES in ISO/IEC 18033-3 and CBC in ISO/IEC 10116 using the 128-bit DEK for swap partition that is generated according to FCS_CKM.1(b) at the time of start-up in TOE state.

[Relevant TSFI]

- Control Panel: Login, Home screen, Copy, Simple Copy, Scan, Simple Scan, Fax transmission, Print, Job display and Log display, Admin settings, Power key
- TopAccess: Login, Job status, Account, User management, Admin settings
- Printer Driver: Interface to a Print request
- Others: Main switch, PSTN Fax interface

7.5. Communication Protection (Selective requirements)

The following describes the summary specifications for the selective requirements D.2.

FCS_TLS_EXT.1

The TSF supports the TLS communication for communication with each type of servers mentioned in FTP_ITC.1 and communication with the client PC mentioned in FTP_TRP.1(a)/FTP_TRP.1(b). The TLS communication supported by the TSF is TLS1.2 (RFC 5246).

Copyright© 2024 TOSHIBA TEC. All rights reserved.

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

Communication between TSF and Client PC

- The TSF generates the server secret key and public key of the RSA used for the TLS communication according to FCS_RBG_EXT.1(b) and FCS_CKM.1(a). The signature of the server certificate is generated by using the secret key and hash algorithm according to FCS_COP.1(b) and FCS_COP.1(c).
- The following shows how to share the secret random number data.
  - ✧ The TSF decrypts the secret random number encrypted by the RSA public key which was sent from the client PC using the server secret key. The TSF generates the session key and HMAC key from the secret random numbers using the keyed-hash message authentication code (HMAC) according to FCS_COP.1(c) and FCS_COP.1(g).
- The following shows how to encrypt and verify the communication data.
  - ✧ The TSF verifies alteration of the communication data by using the HMAC key according to FCS_COP.1(c) and FCS_COP.1(g).
  - ✧ The TSF encrypts and decrypts the communication data in the AES-CBC mode according to FCS_COP.1 (a).

[Relevant TSFI]
- Conform to TSFI of FTP_TRP.1(a) and FTP_TRP.1(b).

Communication between TSF and Servers

- The following shows how TSF verifies the digital signature of the server certificate sent from various servers.
  - ✧ TSF calculates the hash value for server certificate verification according to FCS_COP.1(c).
  - ✧ TSF decrypts the digital signature of the server certificate by RSA signature verification according to FCS_COP.1 (b), and verifies the tampering of the server certificate by comparing it with the hash value for server certificate verification described above.
- The following shows how to share the secret random number data.
  - ✧ The TSF generates a secret random number according to FCS_RBG_EXT.1(b) for generating the session key and the HMAC key.
  - ✧ The TSF encrypts the secret random number using the RSA public key included in server certificate which was sent from each server. The TSF generates the session key and the HMAC key from the secret random numbers using the keyed-hash message authentication Code (HMAC) according to FCS_COP.1(c) and FCS_COP.1(g).
- The following shows how to encrypt and verify the communication data.
  - ✧ The TSF verifies alteration of the communication data by using the HMAC key according to FCS_COP.1(c) and FCS_COP.1(g).
  - ✧ The TSF encrypts and decrypts the communication data in the AES-CBC mode according to FCS_COP.1 (a).

[Relevant TSFI]
Conform to TSFI of FTP_ITC.1.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Communication between TSF and Client PC using IPPS

- The TSF generates the server secret key and public key of the RSA used for the TLS communication according to FCS_RBG_EXT.1(b) and FCS_CKM.1(a). The signature of the server certificate is generated by using the secret key and hash algorithm according to FCS_COP.1(b) and FCS_COP.1(c).
- The TSF decrypts the secret random number encrypted by the RSA public key which was sent from the client PC using the server secret key. The TSF generates the session key and the HMAC key from the secret random numbers using the keyed-hash message authentication code (HMAC) according to FCS_COP.1(c) and FCS_COP.1(g).
- The TSF verifies alteration of the communication data by using the HMAC key according to FCS_COP.1(c) and FCS_COP.1(g).
- The TSF encrypts and decrypts the communication data in the AES-CBC mode according to FCS_COP.1(a).

[Relevant TSFI]
Printer Driver: Interface to a Print request

FCS_HTTPS_EXT.1

The HTTP protocol which complies with RFC2818 is implemented so as to establish the trusted communication path between the TOE and the remote users. FCS_HTTPS_EXT.1 is realized by enabling the HTTPS communication using the TLS protocol which is specified at FCS_TLS_EXT.1.

[Relevant TSFI]
- TopAccess: Login, Job status, Account, User management, Admin settings

FCS_COP.1(g)

The TSF is used in HMAC which is included in the processing to generate the session key and the HMAC key from a secret random number during the TLS communication. Additionally, the TSF is used in HMAC to verify tampering of communication data in TLS communication. The keyed-hash message authentication is performed according to HMAC-SHA-1 with a message length and key length of 160 bits and HMAC-SHA256 with a message length and key length of 256 bits that satisfy FIPS PUB 198-1 “The Keyed-Hash Message Authentication Code” and FIPS PUB 180-3 “Secure Hash Standard”. The hash function used at this time conforms to FCS_COP.1(c). From the above, FCS_COP.1(g) is realized.

[Relevant TSFI]
- Conform to FTP_TRP.1(a)、FTP_TRP.1(b) and FTP_ITC.1

7.6. Trusted Update (Selective requirements)

The following describes the summary specifications for the selective requirements D.3.

FCS_COP.1(c)

The TSF is used for the following three processes.
A digital signature must be attached to the firmware to verify the authenticity of the firmware during firmware update at FPT_TUD_EXT.1. The cryptographic hash function conforms to SHA-256 which complies with ISO/IEC 10118-3:2004. The TSF performs signature generation or verification of the server certificate for TLS communication according to FCS_TLS_EXT.1. The cryptographic hash function used in that case complies with SHA-1, SHA-256, SHA-384 or SHA-512 conforming to ISO/IEC 10118-3:2004. The TSF authenticates the hash message with a key according to FCS_COP.1(g) during verification of the communication data integrity. The cryptographic hash

Copyright© 2024 TOSHIBA TEC. All rights reserved.

function which is used at that time conforms to SHA-1 and SHA-256 which comply with ISO/IEC 10118-3:2004.
From the above, FCS_COP.1(c) is realized.

[Relevant TSFI]
- Conform to FTP_TRP.1(a), FTP_TRP.1(b) and FTP_ITC.1

7.7. User Data Protection

The following describes the summary specifications for the requirements for Class FDP.

FDP_ACC.1/FDP_ACF.1

The TOE performs access control for the user document data and operation for the user document data. Access control for the user document data allows access only when the user ID linked to the document data matched the user ID of a user who has been identified and authenticated at login. The access control for the user document operation is performed according to the roles retained by the user as shown in **Table 14** and **Table 15**.
FCC_ACC.1 and FDP.AFC.1 are realized by the access control shown in the table below.

Table 24 Print Access Control for D.USER.DOC

User	Access Control Rules
Job Owner	・Assign U.ADMIN(a) and U.NORMAL(a) as the Job owners who submit the documents to be printed. ・Allow browse and output of the documents submitted by the Job Owner. ・Deny modification of the documents submitted by the Job Owner. ・Allow deletion of the documents submitted by the Job Owner.
U.ADMIN(a)	・Allow submission of the documents to be printed. ・Deny browse of the print documents submitted by other users. ・Deny modification of the print documents submitted by other users. ・Allow deletion of the print documents stored by other users.
U.NORMAL(a)	・Allow submission of the documents to be printed. ・Deny browse of the print documents submitted by other users. ・Deny modification of the print documents submitted by other users. ・Deny deletion of the print documents stored by other users.
U.ACCOUNTMANAGER U.FAXOPERATOR U.ADDRESSBOOKOPERATOR	・Deny submission of the documents to be printed. ・Deny browse of all submitted print documents. ・Deny modification of all submitted print documents. ・Deny deletion of all stored print documents.
Unauthorized User	・Allow the print documents submitted by the identified U.ADMIN(a) and U.NORMAL(a). ・Deny browse of all submitted print documents. ・Deny modification of all submitted print documents. ・Deny deletion of all stored print documents.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

[Relevant TSFI]

- Control Panel: Print
- Printer Driver: Interface to a Print request

Table 25 Scan Access Control for D.USER.DOC

User	Access Control Rules
Job Owner	・Assign U.NORMAL(a) as the Job owner who submits the document to be scanned. ・Allow browse of the images scanned by the Job Owner. ・Allow modification and deletion of the image scanned by the Job Owner.
U.ADMIN(a)	・Allow submission of the documents to be scanned. ・Deny browse of the images scanned by other users. ・Deny modification of the images scanned by all users. ・Allow deletion of the images scanned by the self and deny deletion of the images scanned by other users.
U.NORMAL(a)	・Allow submission of the documents to be scanned. ・Deny browse of the images scanned by other users. ・Deny modification and deletion of images scanned by other users.
U.ACCOUNTMANAGER U.FAXOPERATOR U.ADDRESSBOOKOPERATOR	・Deny submission of the documents to be scanned. ・Deny browse of all scanned images. ・Deny modification and deletion of the images scanned by all users.
Unauthorized User	・Deny submission of the documents to be scanned. ・Deny browse of all scanned images. ・Deny modification and deletion of all scanned images.

[Relevant TSFI]

- Control Panel: Scan, Simple Scan

Table 26 Copy Access Control for D.USER.DOC

User	Access Control Rules
Job Owner	・Assign U.ADMIN(a) and U.NORMAL(a) as the Job owners who submit the documents to be copied. ・Allow output of the copied documents printed by the Job Owner. ・Deny modification of images saved by the job owner. ・Allow deletion of images saved by the job owner.
U.ADMIN(a)	・Allow submission of the documents to be copied. ・Deny browse of the images copied by the other users. ・Deny modification of the images copied and saved by the other users. ・Allow deletion of the images copied and saved by the other users.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

User	Access Control Rules
U.NORMAL(a)	・Allow submission of the documents to be copied. ・Deny browse of the images copied by the other users. ・Deny modification of the images copied and saved by the other users. ・Deny deletion of the images copied and saved by the other users.
U.ACCOUNTMANAGER U.FAXOPERATOR U.ADDRESSBOOKOPERATOR	・Deny submission of the documents to be copied. ・Deny browse of all copied images. ・Deny modification of all copied and saved images. ・Deny deletion of all copied and saved images.
Unauthorized User	・Deny submission of the documents to be copied. ・Deny browse of all copied images. ・Deny modification of all copied and saved images. ・Deny deletion of all copied and saved images.

[Relevant TSFI]

・Control Panel: Copy, Simple Copy, Job display and Log display

Table 27 Fax Transmission Access Control for D.USER.DOC

User	Access Control Rules
Job Owner	・Assign U.ADMIN(a), U.NORMAL(a) and U.FAXOPERATOR as the Job owners of Fax transmission documents. ・Allow browse of the images scanned by the Job Owner. ・Allow modification of the images saved by the job owner. ・Allow deletion of the images saved by the job owner.
U.ADMIN(a)	・Allow submission of Fax transmission documents. ・Deny browse of the images scanned by the other users. ・Deny modification of the images saved by the other users. ・Allow deletion of the images saved by the other users.
U.NORMAL(a) U.FAXOPERATOR	・Allow submission of Fax transmission documents. ・Deny browse of the images scanned by other users. ・Deny modification of images saved by the other users. ・Deny deletion of images saved by the other users.
U.ACCOUNTMANAGER U.ADDRESSBOOKOPERATOR	・Deny submission of Fax transmission documents. ・Deny browse of all scanned images. ・Deny modification of all saved images. ・Deny deletion of all saved images.
Unauthorized User	・Deny submission of Fax transmission documents. ・Deny browse of all scanned images. ・Deny modification of all saved images. ・Deny deletion of all saved images.

[Relevant TSFI]

・Control Panel: Fax transmission, Job display and Log display

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Table 28　Fax Reception Access Control for D.USER.DOC

User	Access Control Rules
Job Owner	・Assign U.ADMIN(a) and U.FAXOPERATOR as the Job owners of Fax-received documents. ・Allow browse and print of all Fax-received documents. ・Deny modification of all Fax-received documents. ・Allow deletion of all Fax-received documents.
U.ADMIN(a) U.FAXOPERATOR	・Allow all Fax receptions regardless of the user's operation. ・Allow browse and print of all Fax-received documents. ・Deny modification of all Fax-received documents. ・Allow deletion of all Fax-received documents.
U.NORMAL(a) U.ACCOUNTMANAGER U.ADDRESSBOOKOPERATOR	・Allow all Fax receptions regardless of the user's operation. ・Deny browse and print of all Fax-received images. ・Deny modification of all Fax-received images. ・Deny deletion of all Fax-received images.
Unauthorized User	・Allow all Fax receptions regardless of the user's operation. ・Deny browse and print of all Fax-received images. ・Deny modification of all Fax-received images. ・Deny deletion of all Fax-received images.
None	・All Fax-received images are received from the outside of the TOE regardless of the user's operation.

[Relevant TSFI]

- Control Panel:　Print
- Others:　PSTN Fax Interface

Table 29　Print Access Control for D.USER.JOB

User	Access Control Rules
Job Owner	・Assign U.ADMIN(a) and U.NORMAL(a) as the Job owners of the jobs printed by themselves.
U.ADMIN(a)	・Allow creation of the print jobs. ・Allow browse of all print jobs. ・Deny modification of all print jobs. ・Allow cancel of all print jobs.
U.NORMAL(a)	・Allow creation of the print jobs. ・Allow browse of all print jobs. ・Deny modification of all print jobs. ・Allow cancel of own print jobs, but deny cancel of other users' print jobs.
U.ACCOUNTMANAGER U.FAXOPERATOR U.ADDRESSBOOKOPERATOR	・Deny creation of the print jobs. ・Allow browse of all print jobs. ・Deny modification of all print jobs. ・Deny cancel of all print jobs.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

User	Access Control Rules
Unauthorized User	・ Allow creation of print jobs by the identified U.ADMIN(a) and U.NORMAL(a). ・ Allow creation of the print jobs. ・ Deny browse of all print jobs. ・ Deny modification of all print jobs. ・ Deny cancel of all print jobs.

[Relevant TSFI]

- Control Panel: Print, Job display and Log display
- TopAccess: Job status
- Printer Driver: Interface to a Print request

Table 30 Scan Access Control for D.USER.JOB

User	Access Control Rules
Job Owner	・ Assign U.ADMIN(a) and U.NORMAL(a) as the Job owners of the jobs scanned by themselves.
U.ADMIN(a)	・ Allow creation of the scanned jobs. ・ Allow browse of all scanned jobs. ・ Deny modification of all scanned jobs. ・ Allow cancel of all scanned jobs.
U.NORMAL(a)	・ Allow creation of the scanned jobs. ・ Allow browse of all scanned jobs. ・ Deny modification of all scanned jobs. ・ Allow cancel of own scanned jobs, but deny cancel of other users' scanned job.
U.ACCOUNTMANAGER U.ADDRESSBOOKOPERATOR U.FAXOPERATOR	・ Deny creation of the scanned jobs. ・ Allow browse of all scanned jobs. ・ Deny modification of all scanned jobs. ・ Deny cancel of all scanned jobs.
Unauthorized User	・ Deny creation of the scanned jobs. ・ Deny browse of all scanned jobs. ・ Deny modification of all scanned jobs. ・ Deny cancel of all scanned jobs.

[Relevant TSFI]

- Control Panel: Scan, Simple Scan, Job display and Log display
- TopAccess: Job status

Table 31 Copy Access Control for D.USER.JOB

User	Access Control Rules
Job Owner	・ Assign U.ADMIN(a) and U.NORMAL(a) as the Job owners of the copy jobs executed by themselves.
U.ADMIN(a)	・ Allow creation of the copy jobs. ・ Allow browse of all copy jobs. ・ Deny modification of all copy jobs. ・ Allow cancel of all copy jobs.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

User	Access Control Rules
U.NORMAL(a)	・Allow creation of the copy jobs. ・Allow browse of all copy jobs. ・Deny modification of all copy jobs. ・Allow cancel of own copy jobs, but deny cancel of other users' copy jobs.
U.ACCOUNTMANAGER U.FAXOPERATOR U.ADDRESSBOOKOPERATOR	・Deny creation of the copy jobs. ・Allow browse of all copy jobs. ・Deny modification of all copy jobs. ・Deny cancel of all copy jobs.
Unauthorized User	・Deny creation of the copy jobs. ・Deny browse of all copy jobs. ・Deny modification of all copy jobs. ・Deny cancel of all copy jobs.

[Relevant TSFI]

- Control Panel: Copy, Simple Copy, Job display and Log display
- TopAccess: Job status

Table 32 Fax Transmission Access Control for D.USER.JOB

User	Access Control Rules
Job Owner	・Assign U.ADMIN(a), U.NORMAL(a), and U.FAXOPERATOR as the Job owners of the fax transmission jobs executed by themselves.
U.ADMIN(a)	・Allow creation of Fax transmission jobs. ・Allow browse of all Fax transmission jobs. ・Deny modification of all Fax transmission jobs. ・Allow cancel of all Fax transmission jobs.
U.NORMAL(a)	・Allow creation of Fax transmission jobs. ・Allow browse of all Fax transmission jobs. ・Deny modification of all Fax transmission jobs. ・Allow cancel of own Fax transmission jobs, but deny cancel of other users' Fax transmission jobs.
U.ACCOUNTMANAGER U.ADDRESSBOOKOPERATOR	・Deny creation of Fax transmission jobs. ・Allow browse of all Fax transmission jobs. ・Deny modification of all Fax transmission jobs. ・Deny cancel of all Fax transmission jobs.
U.FAXOPERATOR	・Allow creation of Fax transmission jobs. ・Allow browse of all Fax transmission jobs. ・Deny modification of all Fax transmission jobs. ・Allow cancel of own Fax transmission jobs, but deny cancel of other users' Fax transmission jobs.
Unauthorized User	・Deny creation of Fax transmission jobs. ・Deny browse of all Fax transmission jobs. ・Deny modification of all Fax transmission jobs. ・Deny cancel of all Fax transmission jobs.

[Relevant TSFI]

- Control Panel: Fax transmission, Job display and Log display
- TopAccess: Job status

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Table 33　Fax Reception Access Control for D.USER.JOB

User	Access Control Rules
Job Owner	・Assign U.ADMIN(a) and U.FAXOPERATOR as the Job owners of the fax reception jobs executed by themselves.
U.ADMIN(a) U.FAXOPERATOR	・Allow creation of all Fax-received Jobs regardless of the user's operation. ・Allow browse of all Fax-received Jobs. ・Deny modification of all Fax-received Jobs. ・Deny cancellation of all incoming fax jobs.
U.NORMAL(a) U.ACCOUNTMANAGER U.ADDRESSBOOKOPERATOR	・Allow creation of all Fax-received Jobs regardless of the user's operation. ・Deny browse of all Fax-received Jobs. ・Deny modification of all Fax-received Jobs. ・Deny cancel of all Fax-received Jobs.
Unauthorized User	・Allow creation of all incoming fax jobs regardless of user operation. ・Deny browse of all Fax-received Jobs. ・Deny modification of all Fax-received Jobs. ・Deny cancel of all Fax-received Jobs.

[Relevant TSFI]

- Control Panel:　Job display and Log display
- TopAccess:　Job status
- Others:　PSTN Fax Interface

7.8.　PSTN Fax-Network Separation

The following describes the summary specifications for the conditional requirements B.2.

FDP_FXS_EXT.1

Fax transmission and reception are only the functions of the Fax modem.
The Fax interface of the TOE is used only for transmission and reception of the Fax document data with the external Fax machines, and is not used for other purposes.
The Fax interface of the TOE supports only ITU-T-compliant G3 as the transmission/reception protocol.　Thus, only transmission and reception using the Fax protocol are accepted in communication between the TOE and PSTN.　However, communication in which the negotiation with Phase B is not established does not move to the subsequent phase and fails in the communication error, so the TOE disconnects the communication line.
From the above, bridge connection between the PSTN and LAN is prohibited.

[Relevant TSFI]

- Control Panel:　Fax transmission
- Others:　PSTN Fax Interface

7.9.　Identification and Authentication

The following describes the summary specifications for the requirements for Class FIA.

FIA_AFL.1

- When the user logs in from the control panel and TopAccess, the TOE locks out the user ID for a predetermined time when the number of authentication failures counted from the last successful

Copyright© 2024 TOSHIBA TEC. All rights reserved.

authentication or login after account unlocking reaches the number of times (1 to 30) set by U.ADMIN (a).
- The function which releases the locked-out state of a user is provided for the U.ADMIN(a) and U.ACCOUNTMANAGER.

[Relevant TSFI]
- Control Panel: Login
- TopAccess: Login, Admin settings

FIA_ATD.1

- The TOE associates the user ID and role with a user as the security attributes and registers and maintains them.

[Relevant TSFI]
- TopAccess: User management

FIA_PMG_EXT.1

The TOE provides the function to investigate the user password at registration and change of the password. Any combination of the following characters is allowed as a password: Upper and lower case letters, numbers, punctuation marks (+ , - . / : ; = ? ¥ _ ` { | } ~ space), special characters (! @#$^ *()), and European special characters (characters with the German umlauts and French cedilla: See **Table 16** for details.). It is also possible to set the minimum number of digits for a password to more than 15 letters by the U.ADMIN(a).

[Relevant TSFI]
- Control Panel: Home screen, Login, Admin settings
- TopAccess: Login, Account

FIA_UAU.7

If a user enters a password on the control panel, the TOE displays "●" as dummy characters on the control panel instead of the entered characters. Similarly, in the case that a user enters a password from the web browser, alternative characters are displayed instead of the entered characters. The alternative characters depend on the browser used by the user.

[Relevant TSFI]
- Control Panel: Login
- TopAccess: Login

FIA_UAU.1/FIA_UID.1

The TOE requires identification and authentication of a user. Identification and authentication of a user are executed to the user account database. If the user ID and password do not match the credential data which is internally saved, login is denied and an input prompt is displayed again for the user. The user ID of a job owner is associated with a print job performed from the client PC through the printer driver. The TOE identifies the user ID upon reception of a print job, and stores the print job in the print hold queue.
Also, the TOE saves a fax-received job internally without performing identification and authentication of the job.

[Relevant TSFI]
- Control Panel: Login
- TopAccess: Login
- Printer driver: Interface to a Print request

Copyright© 2024 TOSHIBA TEC. All rights reserved.

- Others: PSTN Fax Interface

FIA_USB.1

The TOE associates a user with the user ID and role if identification and authentication are successfully finished.

[Relevant TSFI]
- Control Panel: Login
- TopAccess: Login

7.10. Security Management

The following describes the summary specifications for the requirements for Class FMT.

FMT_MOF.1

The TOE provides the U.ADMIN(a) only with the function which switches the Enable/Disable settings for secure channel function.

[Relevant TSFI]
- Control Panel: Admin settings
- TopAccess: Admin settings

FMT_MSA.1

The TOE provides the U.ADMIN(a) with the following functions.

- Creation, change, inquiry, deletion, and export of all user IDs
- Creation, change, inquiry, deletion, and export of all roles

The TOE provides the U.ACCOUNTMANAGER with the following functions.

- Inquiry and export of all user IDs
- Creation, change, and deletion of the user IDs except for the U.ADMIN(a)
- Creation, change and deletion of the roles except for the U.ADMIN(a)

The TOE provides the U.NORMAL and U.ADDRESSBOOKOPERATOR with the following functions.

- Inquiry of own user ID
- Inquiry of own role

[Relevant TSFI]
- TopAccess: User management

FMT_MSA.3

When a new D.USER.DOC and D.USER.JOB are created, the TOE assigns the user ID of the user who created them as the initial value of the security attribute.
The TOE does not provide the function which overwrites the initial value of the user ID which is the security attribute when the D.USER.DOC and D.USER.JOB are created.

[Relevant TSFI]
- Control Panel: Copy, Simple Copy, Scan, Simple Scan, Fax transmission
- TopAccess: User management
- Printer Driver: Interface to a Print request

FMT_MTD.1

The TOE provides the U.ADMIN(a) with the following operation functions.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

- Change and export of the user password for the U.ADMIN(a).
- Change and export of the user password for the U.ACCOUNTMANAGER.
- Change and export of the user password for the U.ADDRESSBOOKOPERATOR.
- Change and export of the user password for the U.NORMAL.
- Change of the Allowable Number of entry for Login Password.
- Change of the lockout time.
- Status clear for all locked-out accounts.
- Change of the auto logout time.
- Change of the date and time information.
- Change of the minimum password length.
- Creation, change, and deletion of the address book.
- Change of the SYSLOG server settings.
- Change of the FTP server settings.
- Software version check and update

The TOE provides the U.ACCOUNTMANAGER with the following operation functions.

- Change and export of the user password for the U.ACCOUNTMANAGER.
- Change and export of the user password for the U.ADDRESSBOOKOPERATOR.
- Change and export of the user password for the U.NORMAL.
- Status clear for the locked-out accounts other than the U.ADMIN(a).

The TOE provides the U.NORMAL with the following operation functions.

Change of the own user password.

The TOE provides the U.ADDRESSBOOKOPERATOR with the following operation functions.

- Change of the own user password.

[Relevant TSFI]
- Control Panel: Login, Home screen, Job display and Log display, Admin settings
- TopAccess: Login, Account, User management, Admin settings

FMT_SMF.1

The TOE provides the following security management functions to realize FMT_SMF.1.

Time Stamp Settings Management:

- Change operation of the date and time information by the U.ADMIN(a).

User ID Management:

- Change operation of the user ID by the U.ADMIN(a) or U.ACCOUNTMANAGER.

User Password Management:

- Change and export operation of the user password for U.ACCOUNTMANAGER, U.NORMAL, U.ADMIN(a) and U.ADDRESSBOOKOPERATOR by the U.ADMIN(a).
- Change and export operation of the user password for the U.ACCOUNTMANAGER, U.NORMAL, and U.ADDRESSBOOKOPERATOR by the U.ACCOUNTMANAGER.
- Change operation of the own user password by the U.NORMAL.
- Change operation of the user password by the U.ADDRESSBOOKOPERATOR.

Unsuccessful User Authentication Processing Management:

Copyright© 2024 TOSHIBA TEC. All rights reserved.

- Change operation of the number of entries of the login password by the U.ADMIN(a).
- Change operation of the lockout time by the U.ADMIN(a).
- Locked-out account status clear operation by the U.ADMIN(a) or U.ACCOUNTMANAGER.

Minimum Password Length Management:

- Change operation of the minimum password length by the U.ADMIN(a).

Specification of the inactive predetermined time for the user after the session is finished:

- Change operation of the auto logout time by the U.ADMIN(a).

Secure Channel Settings:

- Change operation of the Enable/Disable settings for TLS communication by the U.ADMIN(a).

Address Book Management:

- Change operation of the Address Book by the U.ADMIN(a).

SYSLOG Server:

- Change operation of the SYSLOG server settings by the U.ADMIN(a).

FTP Server:

- Change operation of the FTP server settings by the U.ADMIN(a).

Software:

- Software version confirmation and update by U.ADMIN(a).

[Relevant TSFI]
- Control Panel: Login, Home screen, Job display and Log display, Admin settings
- TopAccess: Login, Account, User management, Admin settings

FMT_SMR.1

The TOE retains a role related to the U.ADMIN(a), U.ACCOUNTMANAGER, U.NORMAL, and U.ADDRESSBOOKOPERATOR, and associates the role with the applicable user when a user is registered.

[Relevant TSFI]
- Control Panel: Login
- TopAccess: Login, User management

7.11. Protection of the TSF

The following describes the summary specifications for the requirements for Class FPT.

FPT_SKP_EXT.1

- The TSF stores the server secret keys described in the TSS of FCS_CKM.1(a) in volatile memory in plaintext, but does not provide access to all users. Additionally, these server secret keys are cleared when the power is turn off.
- When the TSF stores the server secret keys described in the TSS of FCS_CKM.1(a) in Field-Replaceable Nonvolatile storage (SSD), it encrypts them in ciphertext using AES-CBC with a 128-bit DEK, in accordance with FCS_COP.1(d) and FDP_DSK_EXT.1. The TSF does not provide

Copyright© 2024 TOSHIBA TEC. All rights reserved.

access to all users for the DEK necessary for decryption. These DEKs are also cleared when the power is turned off.

- The TSF stores the keys and key materials (KEK derivation key, key material encryption key, context for KEK derivation, KEK, DEK, submask, LUKS key) described in the TSS of FCS_KYC_EXT.1 in volatile memory in plaintext, but does not provide access to all users. These CSPs are cleared when the power is turned off.
- The TSF stores the DEK for the swapping partition in volatile memory in plaintext, but does not provide access to all users. These CSPs are cleared when the power is turned off.
- The TSF stores the KEK derivation key and key material encryption key described in the TSS of FCS_CKM.1(b) in plaintext within the FROM, but does not provide access to all users.
- The TSF stores the session keys for TLS communication and HMAC keys described in the TSS of FCS_CKM.1(b) in volatile memory in plaintext, but does not provide access to all users. These symmetric keys are cleared when the power is turned off.

From the above, FPT_SKP_EXT.1 is realized.

[Relevant TSFI]

- none

FPT_STM.1

The TOE uses “Year”, “Month”, “Day”, “Hour”, “Minute”, and “Second”, which are provided by the real clock IC embedded in the TOE for registration of the audit log, as a stamp to realize FPT_STM.1.

[Relevant TSFI]

- Conform to relevant TSFI of FAU_GEN.1, FAU_GEN.2

FPT_TST_EXT.1

The TOE conducts the following self-tests at power on.

- Verification of TSF Images
  The TSF is implemented by software that controls the MFP (SYSTEM FIRMWARE, SYSTEM SOFTWARE). To ensure the integrity of the TSF, the system performs verification on the image files of both the system firmware and system software using an electronic signature method, employing RSA for public key cryptography and SHA-256 for hashing. Additionally, the firmware for the printer unit (ENGINE FIRMWARE), scanner unit (SCANNER FIRMWARE), and fax unit (FAX1 FIRMWARE) calculates a 16-bit checksum for self-verification of the firmware images to detect implementation failures. If any anomalies are detected during the verification of the image files, the affected image files will not be executed, a service call message will be displayed in the TOE's panel message area, and the TOE will halt its start-up process, rendering it unusable to the user.
- Health test of the entropy source
  Software that controls the MFP (SYSTEM SOFTWARE) starts the rngd process at power on and gets 4096 bytes from /dev/random of Linux PRNG to perform self verification according to NIST SP 800-90B. rngd calls the RDRAND instruction several times by retrying tight loop because entropy is supplied to Linux PRNG at this time. The SYSTEM SOFTWARE outputs a log of the abnormal detection and terminates the rngd process upon detection of the continuous error (CF=0) 10 times during the call. If the constant monitoring of the process monitoring task detects the termination of the rngd process, Service Call is displayed on the panel, and the TOE

Copyright© 2024 TOSHIBA TEC. All rights reserved.

stops operation. The purpose of this health test is to detect unexpected software failures related to the entropy source of the random number generator.

In addition, when the CPU's RDRAND instruction is called, a Built-In Self Test (BIST) is automatically performed to verify that the SoC's built-in Online Health Test (OHT) is conducting continuous health tests correctly, ensuring that the noise source in the entropy source is not faulty. If an anomaly is detected during the BIST, the RDRAND instruction will always return an error with CF=0, and software controlling the MFP will detect a failure in the noise source. If an anomaly is detected in the above health test, an error code will be displayed on the control panel, the TOE will stop operating, and the user will no longer be able to use the TOE.

- Health test of the DRBG
  The DRBG's FCS_RBG_EXT.1(a) and FCS_RBG_EXT.1(b) are both in compliance with NIST SP 800-90A, and when each TSF is first called after the TOE start-up, the health test in Section 11.3 of NIST SP 800-90A rev.1 is automatically executed. If an anomaly is detected in the above health test, an error code will be displayed on the control panel, the TOE will stop operating, and the user will no longer be able to use the TOE.

[Relevant TSFI]
- Control Panel: Power key
- Others: Main switch

FPT_TUD_EXT.1

The TSF provides the U.ADMIN(a) with the Admin settings screen on the Home screen of the control panel as an interface to confirm the current software version information of the TOE, and the Admin settings screen on the control panel and the admin settings screen in TopAccess as the interfaces to update software.
Also, the TSF provides the digital signature verification function which verifies the authenticity of software to be updated before starting update. The verification method is as follows: Compare the hash value which is decrypted from the digital signature provided in the files of each firmware to be updated (SYSTEM SOFTWARE, SYSTEM FIRMWARE, ENGINE FIRMWARE, SCANNER FIRMARE, and FAX1 FIRMWARE) by RSASSA-PSS according to FCS_COP.1(b) and the hash value which is derived from each firmware to be updated by SHA-256 according to FCS_COP.1(c). If the values match, it can be verified that the firmware is correct.

[Relevant TSFI]
- Control Panel: Home screen, Admin settings
- TopAccess: Admin settings

7.12. TOE Access

The following describes the summary specifications for the requirements for Class FTA.

FTA_SSL.3

The TOE forcibly logs the user out if the user does not operate the control panel for a certain period of time. The time can be set from 15 through 150 seconds. Also, a session is forcibly terminated and a user is logged out when the user does not operate for a certain period of time after accessing the TOE though the web browser. The time can be set from 5 through 999 minutes. The TOE does not create an interactive session when submitting a print job from the printer driver, but ends the session immediately after processing a print request.

[Relevant TSFI]
- Control Panel: Login
- TopAccess: Login

Copyright© 2024 TOSHIBA TEC. All rights reserved.

7.13. Trusted Path/Channel

The following describes the summary specifications for the requirements for Class FTP.

FTP_ITC.1

The TOE starts communication using TLS1.2 to protect data during communication between each server. In the case that the TOE accesses the mail server, SYSLOG server, and FTP server through the trusted channel, start of the TLS communication is requested to each server.

[Relevant TSFI]

- Control Panel: Power key, Login, Home screen, Copy, Simple Copy, Scan, Simple Scan, Print, Fax transmission, Job display and Log display, Admin settings
- TopAccess: Login, Job status, Account, User management, Admin settings
- Printer Driver: Interface to a Print request
- Others: Main switch, PSTN Fax interface

FTP_TRP.1(a)、FTP_TRP.1(b)

The TSF provides the following functions in order to prevent the communication data from leakage and provide the trusted path which detects alteration of the communication data in the communication path among the TOE, remote administrators, and remote users.

Communication with the WEB page:

- Connection is made by the HTTPS network protocol so as to establish the trusted path from the client PC to the web page of the TOE.
- Communication starts only in the case that the connection is made by the HTTPS protocol when a remote administrator and remote user connect to the web page of the TOE from the client PC using the web browser.
- The first administrator authentication, user authentication, and all remote user actions from the client PC are executed only for connection using the HTTPS protocol.

Print from the client PC:

- For printing from the client PC using the printer driver, connection should be made by the TLS communication protocol for establishing the trusted path during connection to the TOE.

[Relevant TSFI]

- TopAccess: Login, Job status, Account, User management, Admin settings
- Printer Driver: Interface to a Print request

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Table 34 defines the TSFI related to this Chapter.

Table 34 Definition of TSFI

TSFI Name		Details
Control Panel		
	Power key	An interface which starts up and shuts down the MFP by turning off and on the main switch.
	Login	An interface which identifies and authenticates a user who accesses the MFP from the control panel.
	Home Screen	An interface which changes the user password and confirms the TOE version.
	Copy	An interface which copies a document.
	Simple Copy	An interface which copies a document.
	Scan	An interface which scans an original as the image data, and previews, deletes, replaces, and inserts the scanned image data, saves the data to the folder in the FTP server, and sends the data to the specified email address.
	Simple Scan	An interface which scans an original as the image data, and previews and deletes the scanned image data, and sends the data to the specified email address as an attached file.
	Print	An interface which prints an original which was sent from the client PC and stored in the hold queue of the MFP and fax-received data.
	Fax Transmission	An interface which scans an original as the image data, and previews, deletes, replaces, and inserts the scanned image data, and performs Fax transmission.
	Job Display and Log Display	An interface which operates the execution status of Print and Scan and the Address Book data.
	Admin Settings	An interface by which the Admin performs Security operations, such as change of the Admin password and Address Book data operation.
TopAccess		
	Login	An interface which identifies and authenticates a user who accesses the MFP from the client PC.
	Job Status	An interface which operates the active print job and scan job.
	Account	An interface which changes the own password and displays the set role information.
	User Management	An interface which executes management related to a user, such as registration of the user information.
	Admin Settings	An interface which performs the MFP settings, such as the Auto Clear setting, and MFP management, such as the password policy setting and import of the Address Book.
Printer Driver		
	Interface to a Print Request	An interface which holds (saves) the print data from the client PC to the MFP.
Others		
	PSTN Fax Interface	An interface which receives the Fax data from the external Fax machines.
	Main Switch	An interface which turns on the MFP and starts log collection to use the TOE.

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Apendix

This Appendix describes the definition of acronyms and reference documents.

Table 35 Definition of Acronyms

Abbreviation	Definition
AES	Advanced Encryption Standard
BEV	Border Encryption Value
CBC	Cipher Block Chaining
CC	Common Criteria
cPP	Collaborative Protection Profile
CPU	Central Processing Unit
DRAM	Dynamic Random Access Memory
DRBG	Deterministic Random Bit Generator
EE	Encryption Engine
FDE	Full Drive Encryption
FIPS PUB	Federal Information Processing Standards Publication
FRAM	Ferroelectric Random Access Memory
FROM	Flash ROM
FTP	File Transfer Protocol
GCM	Galois Counter Mode
HCD	Hardcopy Device
SSD	Solid State Drive
HMAC	Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol over SSL
IPP	Internet Printing Protocol
IPPS	IPP over SSL
IT	Information Technology
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
LAN	Local Area Network
LCD	Liquid crystal display
LED	light emitting diode
MFP	Multifunction Product
NCU	Network control unit
NIC	Network Interface Controller
NIST	National Institute of Standards and Technology
PC	Personal Computer
PP	Protection Profile
PSTN	Public Switched Telephone Network
RFC	Request for Comments
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
Soc	System-on-a-chip
TLS	Transport Layer Security

Copyright© 2024 TOSHIBA TEC. All rights reserved.

Abbreviation	Definition
TOE	Target of Evaluation
TSF	TOE Security Functionality

- Reference Documents
  - [Rambus 2012]
    - Analysis of Intel's Ivy Bridge Digital Random Number Generator, Cryptography Research a division of Rambus, 2012.
    - Available: https://www.rambus.com/intel-ivy-bridge-random-number-generator/.

Copyright© 2024 TOSHIBA TEC. All rights reserved.