Security Target for TrustyCabinet™ UX V1

Author: Yoichi Kanai, Ricoh Company, Ltd.

Date: November 12, 2002

Version: 1.9

Document Revision History

Version	Date	Author(s)	Description
0.1	2000/10/23	Yoichi Kanai	The first draft sent to TUViT.
0.15	2000/11/9	Yoichi Kanai	Contents of Table 19, 20, 21, and 30 are supplied. Inter-TSF duplication-related issues are erased. Documentation correctness is improved.
0.5	2000/12/15	Yoichi Kanai	Reviewed by Mr. Arnold Abromeit and Mr. Frank Roth in TUViT.
0.6	2001/02/01	Yoichi Kanai	Mismatches between the ST and implementations are corrected.
1.0	2001/05/14	Yoichi Kanai	Revised based on comments from Mr. Abromeit (TUViT) and the evaluation result received from ECSEC. The product name is changed from “TrustyCabinet V2” to “TrustyCabinet UX V1.”
1.01	2001/05/21	Yoichi Kanai	The URL of the reference document is updated.
1.02	2001/06/25	Yoichi Kanai	Revised based on comments from Mr. Abromeit (TUViT).
1.1	2001/09/23	Yoichi Kanai	FIA_AFL.1 (a) is refined based on actual implementation of the TOE. The related parts are also changed. The word “TCAB2” in Figure 3 is corrected. For the password quality metric, “password shall include” is corrected to “password must include”. The detailed version number of the TOE is changed to V1.01. SF.INT.1 and SF.INT.2 are added as functions realized based on permutational mechanism.
1.2	2001/11/15	Yoichi Kanai	Revised based on comments from the certification body (TUViT). Unclarities in the TOE description, section 5.3.1, section 6.1.3, and section 6.1.4 are clarified.
1.3	2001/12/03	Yoichi Kanai	Revised based on the following observation reports from ECSEC evaluators. Observation reports: SEA-EORS-0001-01, SEA-EORS-0002-01, SEA-EORS-0003-01, SEA-EORS-0004-01, and SEA-EORS-0005-01
1.4	2002/03/08	Yoichi Kanai	Revised based on discussion with ECSEC evaluators concerning comments from the certification body in Japan (NITE).
1.45	2002/03/11	Yoichi Kanai	Revised based on comments from ECSEC evaluators.
1.5	2002/05/07	Yoichi Kanai	Version numbers of the assurance measures are updated.
1.6	2002/09/26	Yoichi Kanai	Revised based on comments from ECSEC evaluators. Descriptions in section 7.3 and 7.5.3 are refined. A requirement for authentication failure handling is refined. Requirements for IT environment are refined.
1.7	2002/10/07	Yoichi Kanai	Minimum SOF-level is changed to SOF-Basic.
1.8	2002/10/17	Yoichi Kanai	SF.INT.1 and SF.INT.2 are removed from section 6.1.6 and a Note is added after the assumptions table based on comments from ECSEC.
1.9	2002/11/12	Yoichi Kanai	Version numbers of the assurance measures are updated.

Table of Contents

List of Figures

List of Tables

1 ST Introduction

1.1 ST Identification

Title:	Security Target for TrustyCabinet™ UX V1
Version:	1.9
TOE:	TrustyCabinet UX V1 (Version: V1.01)
Date:	November 12, 2002
Author:	Yoichi Kanai, Ricoh Company, Ltd.
CC version used:	ISO/IEC 15408 (CC Version 2.1)
Keywords:	electronic document management, storage system, data integrity, authenticity, cryptography

1.2 ST Overview

This Security Target (ST) describes security specifications of a secure electronic document storage system TrustyCabinet UX V1 (Version: V1.01) (TrustyCabinet is called TCAB, hereafter).

The TCAB is a server system typically used in an intranet of a corporation or a government. It provides functions for securely storing and managing electronic documents as evidence. The TCAB manages revision history of stored documents and it protects the documents and the revision history from unauthorized modifications by using cryptographic techniques. To store the documents for a long term, the TCAB has a capability to write-out the documents to off-line discs like CD-R or DVD-RAM etc. The TCAB also has a capability to transfer the stored documents to another TCAB via the network. The TCAB intends to support security policies provided by the Management and Coordination Agency of Japan [GOV].

The TOE defined in this ST is the server software only (underlying operating environment of the server software and third party produced modules used with the server software are out of the TOE).

This ST consists of 10 parts listed below:

1) ST Introduction (this part),

2) TOE Description,

3) TOE Security Environment,

4) Security Objectives,

5) IT Security Requirements,

6) TOE Summary Specification,

7) Rationale,

8) Reference,

9) Glossary, and

10) Abbreviation.

1.3 ISO/IEC 15408 Conformance Claim

The TOE is **conformant** to ISO/IEC 15408-2:1999(E) (CC Version 2.1 Part2).

The TOE is **conformant** to ISO/IEC 15408-3:1999(E) (CC Version 2.1 Part3) assurance level **EAL3**.

Conformance to a PP is not claimed.

1.4 Strength of Function Claim

The minimum strength level claimed for the TOE is **SOF-Basic**.

2 TOE Description

In this chapter, the background of the TCAB, the TCAB architecture, the TCAB functions, and the TOE boundary are described. The TOE is a part of server software of a document storage system described in detail hereafter.

In the following sections, the terms TCAB, TCABX1, and TCABW1 is used as defined in Table 1.

Table 1 TrustyCabinet-related term

Term	Definition
TCAB	This term is used as a general term for representing TrustyCabinet (server).
TCABX1	This term is used for representing TrustyCabinet UX V1 (server) that is not the same version of the TOE.
TCABW1	This term is used for representing TrustyCabinet V1 (server, for Windows platform).

2.1 Background

In this section, the background and the design concept of TCAB is described.

TCAB is a server system typically used in an intranet of a corporation or a government. It provides functions for securely storing and managing electronic documents. The TCAB keeps trustworthiness of the stored documents by utilizing cryptographic technologies and document access control functions, therefore, the TCAB is very useful for organizations of government and corporations to store electronic documents as evidence.

Figure 1 shows a reference model of a TCAB-integrated system. The TCAB is generally used from business processing systems rather than from end-users directly. The TCAB may be used/accessed directly via the network (not via business processing systems) only by an administrator or an auditor of the TCAB. To maintain the TCAB, only a customer-engineer uses the local console of the TCAB machine.

In the typical three-layer architecture employed in many of the recent web-based information systems, TCAB occupies the position of the backend data management layer. TCAB is accessed from a business processing system corresponding to the business logic layer, and provides the service of storing and managing electronic documents that are the products of business processes. The documents are first stored on a hard-drive of the TCAB and then they can be written out to off-line discs for long-term storage. As a countermeasure for a system crash, a UPS and a backup device are equipped with the TCAB machine. The TCAB only realizes role-based access control concerning documents, not individual access control, and if individual access control for the whole system including TCAB itself is required, it has to be realized by the business application layer.

When the TCAB-integrated system is used for a company’s document workflow/management, the whole of the integrated system (end-user terminal, business processing system, and TCAB) may be located on the same intranet, which is separated from public network (e.g., the Internet) or protected from public network with firewalls. On the other hand, when the TCAB-integrated system is used for Internet-based governmental administrative procedures, the end-user’s terminal may be located on the Internet, the business processing system may be located on the firewall-protected DMZ (De-Militarized Zone), and the TCAB may be located on the firewall-protected

government intranet.

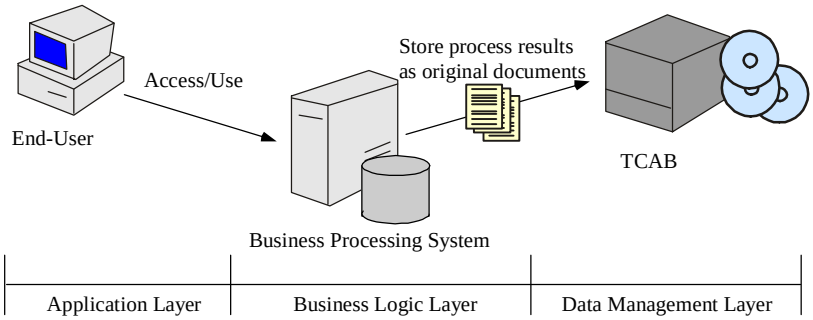

Figure 1 Reference model of a TCAB integrated system

For understanding the usage of the TCAB-integrated system, an example of application system for the governmental administrative procedures using the TCAB-integrated system is described as follows:

(1) The business processing system is a web-server and serves application forms.

(2) The end-user accesses the web-server and sends application documents, which are generated based on the provided application form, to the business processing system via the Internet.

(3) The business processing system checks the format of the application documents, generates search index information for the documents, and stores the index information into databases.

(4) Finally, the business processing system stores the application documents as evidence on the TCAB via the network (intranet).

The stored documents may be used not only by one organization but multiple organizations. For such situations, the TCAB provides document transfer function. The TCAB can transfer stored documents to a distinct TCAB (installed in another organization) via the network using secure communication channel (with mutual authentication, integrity protection, and encryption).

In Japan, a study group arranged by the Management and Coordination Agency summarized a report for realizing the Internet-based governmental administrative procedures [GOV] on March 2000. In the report, criteria for keeping security of electronic documents, which are used for governmental administrative procedures, are provided. The criteria are considered to be security policies provided by the government. TCAB is intended to support these security policies. The essence of the security policies is integrity, confidentiality, and readability of the stored documents (evidence) shall be maintained properly by both technical and operational measures. The detailed security policies are described in section 3.5.

2.2 TCAB Functions

In this section, general functions of TCAB are described.

Figure 2 shows a schematic diagram of the document storage process.

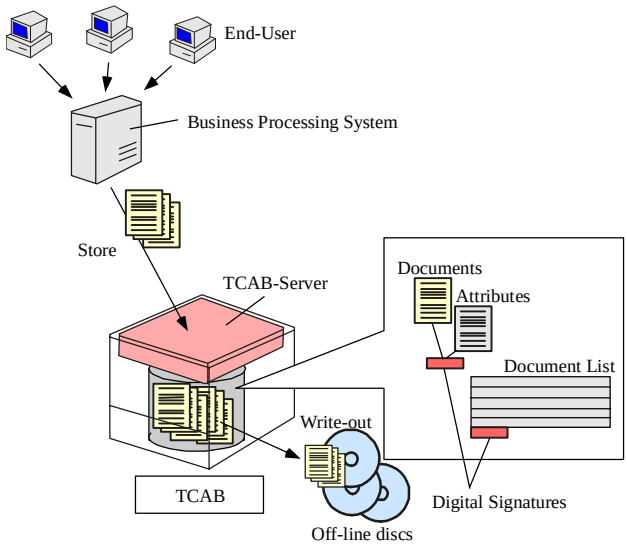

Figure 2 Schematic diagram of the document storage process

Before using all of the following functions, the accessing client has to be authenticated by the TCAB.

(a) Store documents

When a client of a TCAB stores an electronic document via the network, the TCAB generates document attributes, which indicate that the document is an original document or a temporary document, and attaches them to the document. The document and the attributes are protected from unauthorized modifications by data authentication mechanisms, and they are stored on a hard-drive in the TCAB. The TCAB protects communication data between the client and the TCAB by encryption and message authentication mechanisms. A temporary document can be changed to an original document later.

(b) Read documents

A client of a TCAB can read electronic documents stored in the TCAB via the network. When the TCAB receives a read request from the client, the TCAB verifies the document requested to read and sends it to the client if the verification succeeds. If the verification fails, it sends an error to the client.

(c) Transfer documents to other systems

A client of a TCAB can transfer electronic documents stored in the TCAB to another TCAB via the network. When the TCAB receives a transfer request from the client, the TCAB verifies the document requested to transfer, transfers the document to the specified TCAB, and deletes the transferred document on the sender-side. The originator and the receiver perform mutual authentication before starting transfer, and they protect the

communication data between them by encryption and message authentication mechanisms. The receiver also keeps the attributes of the transferred document.

(d) Write out documents onto off-line discs

A client of a TCAB can write out electronic documents stored in a hard-drive of the TCAB onto an off-line disc, such as CD-R or DVD-RAM. When the TCAB receives a write-out request from the client, the TCAB verifies the corresponding document, writes out the document onto an off-line disc and deletes the document on the hard-drive. The TCAB bestows a unique identification number on the off-line disc, and the TCAB internally maintains the mapping information of disc identification numbers and document identification numbers to manage the location of each document.

(e) Create duplicates

A client of a TCAB can create a duplicate of an original document stored in the TCAB. When the TCAB receives a duplicate request from the client, the TCAB verifies the integrity of the document requested to duplicate and checks that the document is an original. If the document is authentic and is an original, the TCAB duplicates the original document. The TCAB explicitly distinguishes the original from its duplicate(s) because original documents must be stored during a retention period (e.g. due to legal reasons). Because the created duplicates are also integrity protected by the TCAB and are ensured that they are just as same as the originals at that time; they can be used as trustworthy backups of original documents and can be used for transferring them to other TCAB as authentic duplicates.

(f) Revise documents

Original documents and temporary documents stored on an internal hard-drive of a TCAB can be revised later. When a client requests to revise an original or a temporary document, the TCAB stores the revised contents data as a new version of the document. The revision history of the document is recorded automatically and cannot be modified or canceled. Old versions of the document can be referred at any time. The TCAB only provides sequential revision management capability and does not provide version branching. Therefore, only the latest version of the document can be revised.

On the other hand, documents written-out on off-line discs cannot be revised at all. Duplicates also cannot be revised at all, to prevent mismatches between duplicates and the original.

(g) Delete documents

Documents stored in the TCAB can be deleted. When a client requests to delete a document, the TCAB determines permit or reject the request based on the targeted document’s attributes. If the targeted document is an original document, then the TCAB checks the retention period of the document and determines permit or reject the request. If the targeted document is a duplicate or a temporary document, then the TCAB permits the

request without further checking.

TCAB also includes functionality supporting the document management related functions described above.

(a) Audit

TCAB records audit data related to system access events, document access events, security management events, and so on. The recorded audit data can be written out onto external media such as CD-R. The audit data, written on the external media, are protected with digital signatures generated by the TCAB. To verify the integrity of the audit data written on the external media, a verification tool is used. The tool verifies the digital signatures and ensures that the audit data are not modified. The verification tool is not a part of the TCAB.

(b) System backup

TCAB has the capability to backup the entire TCAB internal hard-drives to backup media such as DLT. The backup is used for restoring the whole TCAB system. The backup is protected with digital signatures generated by the TCAB, and the digital signatures are verified after restoration by TCAB during a start-up test.

(c) Account management

TCAB has the capability to manage user accounts that are used to identify and authenticate external entities. TCAB manages user account roles such as administrator, auditor, normal user, and so on. In general, an account having a normal user role is used by a business-processing system. On the other hand, an account having an administrator or an auditor role is used by a human user.

2.3 TCAB Architecture

In this section, architecture of TCAB is described.

Figure 3 shows a schematic diagram of TCAB architecture.

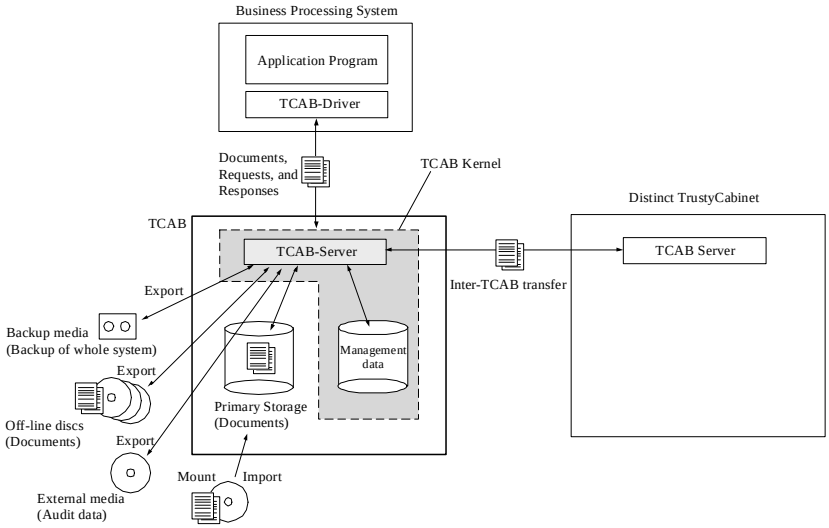

Figure 3 Schematic diagram of the TCAB architecture

TCAB is a network attached server system. A server process named TCAB-Server is working and provides services to clients. A client application (e.g. a business-processing software) accesses the TCAB-Server by using a driver module named TCAB-Driver. The TCAB-Driver accesses the TCAB-Server via the network.

The TCAB-Server and the TCAB-Driver communicate with each other using a Secure Sockets Layer (SSL). SSL communications are also used between a TCAB and a distinct TCAB.

TCAB describes document attributes using eXtensible Markup Language (XML). The document attributes and document contents are protected with digital signatures generated by the TCAB.

TCAB employs several software modules that are used for supporting the TOE to provide services. These software modules are listed in Table 2.

Table 2 Software required for the TOE

Software type	Details
Operating system	Solaris™ 7 for SPARC™ (Sun Microsystems, Inc.) This is used for a platform of the TCAB-Server.
Virtual Machine	Java™ 2 SDK, Standard Edition, v 1.3 for Solaris™/SPARC™ (Sun Microsystems, Inc.) This is used for a platform of the TCAB-Server
Secure communication module	OpenSSL 0.9.4 (OpenSSL Project: http://www.openssl.org) This module is used for securing RMI transport layer protocols.
XML parser	Xerces Java Parser 1.3.1 (Apache XML Project: http://xml.apache.org/xerces-j/) This module is used for processing XML data, such as document attributes.
E-Mail engine	Java™ Mail API 1.1.3 compliant module TCAB uses “Java Mail API 1.1.3 Reference Implementation” provided by Sun Microsystems, Inc.

Software type	Details
	This module is used for sending e-mail messages to a configured e-mail address for notifying security alarms.
Cryptographic module	Java™ Cryptography Architecture (JCA) compliant provider module TCAB uses "SunRsaSign" provider for generation/verification of digital signatures, "SUN" for hashing and keys/certificates storage, "RICOH" for key generation. "SunRsaSign" provider and "SUN" provider are provided in conjunction with Java™ 2 SDK by Sun Microsystems, Inc.
Backup module	tar command TCAB uses a 'tar' command provided in conjunction with the operating system (Solaris™ 7). This module is used to backup TCAB hard-drives.

Hardware modules required for TCAB to provide services are listed in Table 3.

Table 3 Hardware required for the TCAB

Hardware type	Details
Machine	A workstation on which the operating system specified in the Table 2 works (e.g., Sun workstation Ultra-80).
Hard-drive	TCAB requires multiple partitions. System Program Partition: This partition is used for storing operating system environment, virtual machine environment, and TCAB software modules. System Data Partition: This partition is used for storing security management data and audit data. User Data Partition: This partition is used for storing user data such as documents. This partition is also called "primary storage" for the documents.
External storage device	An external storage device, such as a CD-R drive. It can be used for (1) writing out documents to off-line discs, (2) exporting audit data to external media, and (3) importing documents on off-line discs.
Backup device	A backup device, such as DLT, that can be used with the backup module specified in the Table 2.
Power supply	A power supply device, such as UPS, that works on the operating system specified in the Table 2.
Hardware protection	A hardware case that can protect TCAB-Kernel from direct accesses. The TCAB-Kernel consists of System Program Partition, System Data Partition, CPU board, and keyboard/mouse. The purpose of the hardware protection is to reduce possibilities of TCAB system corruption. The level of hardware protection depends on the operational environment. For a well-administered environment, a lock on the hardware case covering a rack-mounted machine is sufficient for satisfying the purpose. In general, whole of the TCAB machine, not only the TCAB-Kernel, is covered with a hardware case.

TCAB-related personnel are defined in Table 4.

Table 4 TCAB-related personnel

Personnel type	Details
TCAB-User	This is one of the user roles managed in TCAB. A user (human or system) having this role is also called a TCAB-User. The TCAB-User has privileges to access documents stored in the TCAB. The TCAB-User can read, store, revise, and delete documents, but cannot use system management functions. In general, a business-processing system uses an account having this role to access a TCAB.
TCAB-RO-User	TCAB-RO-User means TCAB Read Only User. This is one of the user roles managed in TCAB. A user (human or system) having this role is also called a TCAB-RO-User. The TCAB-RO-User only has privileges to read documents stored in the TCAB.
TCAB-Administrator	This is one of the user roles managed in TCAB. A user (generally human) having this role is also called a TCAB-Administrator. The TCAB-Administrator has privileges to perform the following system management: account management, system timer configuration, and system shutdown. The TCAB-Administrator does not have privileges to store and revise documents.
TCAB-Key-Owner	This user role is **not managed in TCAB**. This person possesses a physical key that is used to unlock the hardware protection. The TCAB-Key-Owner can unlock the hardware protection and can directly access to the TCAB-Kernel, however, does not have privileges to login to the operating machine. In general, one person acts as both TCAB-Administrator and TCAB-Key-Owner.
TCAB-Auditor	This is one of the user roles managed in TCAB. A user (generally human) having this role is also called a TCAB-Auditor. The TCAB-Auditor has privileges to execute the following audit functions: viewing audit data and audit data backup/clear. The TCAB-Auditor does not have privileges to store, revise, and delete documents. One person **must not** act as both TCAB-Administrator and TCAB-Auditor.
TCAB-OS-Administrator	This user role is **not managed in TCAB**. This person has privileges to login to the operating machine. The person, however, does not unlock hardware protection of the machine; so, the person has to call a TCAB-Key-Owner to unlock the machine and login to the system. One person **must not** act as both TCAB-Key-Owner and TCAB-OS-Administrator. In general, one person acts as both TCAB-Auditor and TCAB-OS-Administrator.
TCAB-Customer-Engineer	This user role is **not managed in TCAB**. This person is a customer engineer (or, in other words, a service-repair person) who belongs to the developer or a maintenance provider company. Basically, this person does not belong to the organization that is using a TCAB. This person has privileges to install, maintain, and restore a TCAB. To install/maintain/restore the TCAB, the person has to access the TCAB-Kernel directly, however, the person does not have privileges to unlock hardware protection and login to the operating machine. Therefore, to install/maintain/restore, the person has to call a TCAB-Key-Owner and a TCAB-OS-Administrator to unlock and login to the system.

2.4 TOE Boundary

As shown in Figure 3, TCAB is a hardware/software combined server system. The TOE is, however, software only. To clarify the physical (software module) boundary of the TOE, a schematic diagram of the software structure is shown in Figure 4.

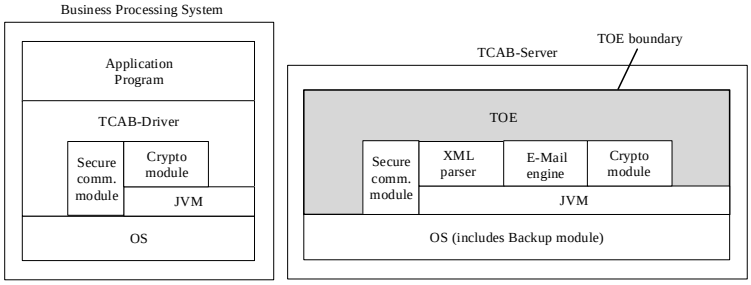

Figure 4 Schematic diagram of the software structure

In Figure 4, the grayed box is the TOE. Software structure of the business processing system side is also shown in the figure; however, this side is not part of the TOE.

The TSC (TSF Scope of Control) includes data and executables stored in System Program Partition, management data and audit data stored in System Data Partition, documents stored in Primary Storage, and documents stored on mounted off-line discs.

Documents stored on un-mounted off-line discs, backup data stored on DLT, audit data on external media are out of the TSC. The TOE can import documents on off-line discs by mounting the corresponding discs. Backup data on DLT, however, is used for restoring whole of the TOE by TCAB-Customer-Engineer, so the TOE itself does not import backup data.

To clarify the logical (functionality) boundary of the TOE, the functionality of each software module is described as follows:

(1) The TOE uses hardware resources of the TCAB, such as hard-drives, external media, off-line discs, memories, networks and so on. The TOE does not directly accesses the hardware resources but via JVM and OS. The underlying JVM and OS provide the capability for managing and handling such hardware resources.

(2) The TOE generates/handles attributes of each document, access history of system, access logs of document, and system timer configuration history. All of them are written in XML and the XML parser module provides the capability to parse/produce XML formatted data. The TOE controls when/how to use the XML parser.

(3) The TOE sends e-mails to a configured e-mail address for notifying security-related events occurred in the TCAB. The TOE generates the e-mail messages and makes the e-mail engine to send the message. The e-mail engine provides capability to send the messages based on SMTP. The TOE controls when/how to use the e-mail engine.

(4) The TOE protects integrity of documents, document lists, system access history, and so on. For the integrity protection, the TOE generates hash values and digital signatures of the protection targets using cryptographic module. The cryptographic module provides capability to calculate hash values, generate/verify digital signatures, store/manage cryptographic keys/certificates, and generate

cryptographic keys. The TOE controls when/how to use the cryptographic module.

(5) The TCAB protects communications between a client and the TCAB (also between the TCAB and a distinct TCAB) using the secure communication module. The secure communication module provides capability to establish secure communication channel based on SSL. The TOE incorporates the secure communication module and realizes RMI communication based on SSL. The TOE controls when/how to use the secure communication module.

(6) The TCAB backups the whole of the internal hard-drives to DLTs using the backup module. The backup module provides capability to archive specified data on hard-drives to DLTs. The TOE controls when/how to use the backup module.

All other functionality of the TCAB-Server, described in section 2.2, is provided by the TOE.

3 TOE Security Environment

3.1 Introduction

This chapter identifies the following:

1) Assets that have to be protected by the TOE,
2) Significant assumptions about the TOE's operational environment,
3) Threats for which this TOE and the TOE's environment should address, and
4) Organizational security policies for which this TOE is appropriate.

By providing the information described above, this section gives the basis for the security objectives described in Chapter 4 and, subsequently, the specific security requirements listed in Chapter 5.

3.2 Assets

Assets that have to be protected by the TOE are listed in Table 5.

Table 5 Assets

1.	ASSET.DOCUMENTS	Documents
		Document contents treated by the TCAB shall be protected by the TOE. The document contents include the following: (1) Document contents stored in document objects on the TCAB internal hard-drives. (2) Document contents stored in document objects on off-line discs that are written out by the TCAB. (3) Document contents or some parts of document contents on the network that are transferred from an authenticated client or a distinct TCAB to the TOE. (4) Document contents or some parts of document contents on the network that are transferred from the TOE to an authenticated client or a distinct TCAB. A document contents consists of multiple "versions". A document object is a container of the document contents. The document-object-related TSF data, document attributes, document access logs, and digital signature data (used for protecting the document except the signature data), are usually handled with the document object. A "version" consists of multiple content-files. Note: The word "document(s)" is used for representing general document(s) if an explicit distinction between document contents and document objects is not required.
2.	ASSET.SYSTEM	System and system data
		The executables of the TCAB and the TSF data shall be protected. The data which shall be protected are the following: (1) System configuration data. (2) Installed programs. (3) TSF data stored within the TOE working machine. (4) Backup data. (5) Audit data written-out to external media.

3.3 Assumptions

The specific conditions listed below are assumed to exist in the TOE environment. These assumptions include essential environmental constraints on the use of the TOE.

Table 6 Assumptions

1.	A.PLATFORM	The platform of the TOE is trusted.
		The platform of TOE is trusted and works correctly and in the expected way (the platform consists of hardware modules listed in Table 3 and software modules listed in Table 2). No viruses and Trojan horses are installed on the machine. The secure communication module is configured to allow usage of high-grade cryptography only. Cryptographic keys used for secure communication and digital signing are generated and updated by a TCAB-Customer-Engineer in a secure manner. The cryptographic keys are destructed on updating them with new keys. The TCAB-Customer-Engineer ensures that the keys are strong enough for their purpose.
2.	A.DEDICATED-MACHINE	The TOE works on a dedicated machine.
		The machine on which the TOE works is used only for the TOE. No components other than that ones listed in Table 2 and the TOE itself are installed on the machine. The machine is configured to terminate all network services other than the services provided by the TOE.
3.	A.PRIVATE-NETWORK	The TOE is located on a private network.
		The TOE does not directly connect to a public network. The TOE is located on a network that is properly protected by a firewall, or on a network that has no connections to a public network. Therefore, it is not assumed that unknown malicious users attack directly to the TOE in a sophisticated manner in the firewall-protected network, e.g. attacks utilizing enormous number of machines.
4.	A.PERSONNEL	Proper persons are assigned to administrators and they are trained.
		For administration and maintenance of the TOE, administrators are properly assigned to trustworthy persons as defined in Table 4. The assigned administrators and users of the TOE who have access rights for the TOE maintain their authentication data used for accessing the TOE properly.

Note:

In A.PERSONNEL, the word “administrators” means administration-related persons of the TOE including TCAB-Administrator, TCAB-Auditor, TCAB-OS-Administrator, TCAB-Key-Owner, and TCAB-Customer-Engineer.

3.4 Threats

Security threats related to the TOE are identified in this section.

Table 7 Threats

1.	T.UNAUTH-ACCESS	Unknown users perform unauthorized access to the TOE.
		Unknown users (users without a TCAB user account) logically perform unauthorized access to the TOE and therefore to the documents stored inside the TOE. Unknown users may use the TOE security functions without identification and authentication. Unknown users or unauthorized users may perform password attacks to impersonate an authorized client.
2.	T.NETWORK-ATTACK	Network communications are attacked.
		Communications between the TOE and a client, or between the TOE and a distinct TCAB, are modified or eavesdropped by malicious users. Malicious users may perform impersonation or man-in-the-middle attacks. Therefore malicious users may access to documents and secrets (e.g., authentication data) on the network.
3.	T.DELETE-DOC	A document, which has to be retained, is deleted via the TSF.
		Regardless of intentionally or un-intentionally, a stored document, which has to be retained, is deleted via the TSF. General write protection and access controlled file system are not enough for addressing this threat. For example, someone who has a right to delete a document may delete the important document that has to be stored during the retention period from a legal point of view. Someone may impersonate a client who has a right to delete, and may delete the important document.
4.	T.OVERWRITE-DOC	A document is modified without traces via the TSF.
		Regardless of intentionally or un-intentionally, a stored document is modified or overwritten without traces (access logs and revision history) via the TSF. General write protection and access controlled file system are not enough for addressing this threat. For example, someone who has a right to modify a document can easily modify/overwrite the document without traces. Someone may impersonate a client who has a right to modify, and may modify/overwrite the important document without traces.
5.	T.MODIFY-DOC-DIRECTLY	A document is modified, deleted, altered or forged directly.
		A stored document is undetectedly modified, deleted, or forged without using the TOE security functions. An Off-line disc storing documents may be thrown away or may be altered with another disc. For example, after creating a copy of an off-line disc storing documents, an authorized client may revise documents on the off-line disc using the TOE. Later, someone may alter the new disc with the old copied disc. Simple digital signature protection is not enough for addressing this threat. For example, someone may easily alter a document with another digitally signed document.
6.	T.CONFUSE-ORIGINAL	Authorized users confuse an original with its duplicates.
		An authorized client duplicates an original document using the TSF, and other clients confuse the duplicates with the original. This leads to other threats, for example, authorized clients may delete the original, which has to be stored during retention period, because they cannot distinguish the original from its duplicates. Additionally, authorized clients may revise duplicates and may confuse the revised duplicates with the original. It leads inconsistencies of document revision controls.
7.	T.CORRUPT-SYSTEM	The TOE system is corrupted directly by malicious users.

		Malicious users corrupt the TOE system directly, not via the TSF. Malicious OS users may modify system configurations or install programs, and it leads to the future insecurities. Malicious users may modify the TSF data stored within the TOE. Malicious users may modify the backup data directly, and it leads to other insecurities such as insecure state of the TOE caused by a restoration. Malicious users may modify audit data written-out to external media.

3.5 Organizational Security Policies

In Japan, a study group arranged by the Management and Coordination Agency summarized a report for realizing the Internet-based government administrative procedures [GOV] on March 2000. In the report, criteria for keeping security of electronic document, which is used for the government administrative procedures, are provided. The criteria are considered to be security policies provided by the government. The TOE and the TOE environment are intended to support the policies.

In the report, following three (3) primary organizational security policies are provided.

(1) Integrity of documents shall be maintained properly.

The organization shall store documents, which are created or acquired from external to the organization, after the documents are authorized to be stored.

The organization shall prevent losses and degradations of the documents.

The organization shall record revision history of the documents for preventing unauthorized modifications of the documents and detecting the fact that the document was fraudulently modified.

(2) Confidentiality of documents shall be maintained properly.

By controlling accesses to the stored documents, or by recording access history of the document, or by other measures, the document shall be protected from unauthorized users' accesses.

The documents shall be stored and managed to prevent unauthorized access, disclosure, and eavesdropping.

(3) Readability of documents shall be maintained properly.

The organizations shall maintain systems for visualizing electronic documents, to prepare situations that those documents are required to view.

These primary organizational security policies are decomposed into more detailed 19 policies by [GOV]. Those policies are summarized as 12 policies listed in Table 8. To clarify the mapping between the policies described in the report [GOV] and the policies listed in the table; the original policies are shown in separately in the right column of the table (highlighted by bold face letters). Each organizational security policy in Table 8 is mapped to security objectives in section 4.

Table 8 Organizational security policies

1.	P.MANAGER	Manager responsible for the document
		To clarify the responsibility and privilege of document management, the organization shall specify a manager who is responsible for the electronic document management.
2.	P.IDENTIFY-AUTHENTICATE	Identification and authentication
		Electronic Document Management and Storage System (EDMSS) shall identify and authenticate users accessing the system.
3.	P.MANAGE-MEDIA	Management of electronic media
		The organization shall specify storage space for electronic media. The electronic media shall be maintained securely (e.g., in the locked shelves). The organization shall record check-out/check-in history of the electronic media.
4.	P.AUDIT	Audit
		System access audit EDMSS shall record accesses. **Document access log** EDMSS shall record access logs of the stored documents. The logs shall contain information about storage date, access date, revision date, deletion date, and the accessing user. The logs shall be maintained securely for a specified period. **System timer setting** System timer configuration history shall be recorded and the history shall be maintained securely for a specified period. **Audit duty** The EDMSS shall be audited properly.
5.	P.ACCESS-CONTROL	Access control
		Accesses to the documents stored in EDMSS shall be controlled properly, based on the document type.
6.	P.MANAGE-REVISION	Document revision management
		Revision history The revision history, including deleted contents and appended contents, of documents shall be maintained. The revision history shall be maintained securely for a specified period. **Document revision management** When revise a document, the original document should be maintained for a specified period, if it is required.
7.	P.PROTECT-CONTENTS	Contents protection
		Contents encryption To prevent and to prepare for steal, disclosure, and modification, the stored documents should be encrypted, if it is required. **Contents signing** The stored documents should be protected with a digital signature having functionality of detecting modifications, if it is required.
8.	P.BACKUP	Backup
		Document backup The stored documents shall be backed-up at regular intervals. The backup data shall be maintained properly. **Management of media** Media with stored documents and backup media shall be checked, that these media are properly maintained, at regular intervals. **Program backup** The programs shall be backed-up, and the backup shall be properly maintained.
9.	P.VIRUS-CHECK	Virus check

		Documents acquired from outside the organization shall be virus-checked before using them.
10.	P.READABILITY	Readability
		The organization shall maintain systems for visualizing electronic documents. The systems include such as computers, programs, networks, display monitors, and printers. When the documents are required to view, the organization shall visualize the documents on a monitor or papers.
11.	P.MAINTAIN-SYSTEM	System maintenance
		EDMSS shall be maintained, checked, and updated[1] systematically. Documents shall be protected during the maintenance.
12.	P.POWER-SUPPLY	Power supply
		To prevent losses and destructions of documents caused by power supply termination, Uninterruptible Power Supplies (UPS), or other measures, shall be applied to the systems.

[1] An update of the system (either the TOE itself or one or more of the platform components) may lead to a configuration which is no longer the evaluated one (such an update procedure is out of scope in this evaluation). If an evaluated system is mandatory for the organization, the update planning has to take this into account.

4 Security Objectives

This section defines the security objectives for the TOE and its environment. The security objectives address or support all of the security environment aspects identified in the previous section.

4.1 Security Objectives for the TOE

Security objectives for the TOE are listed in Table 9.

Table 9 Security objectives for the TOE

1.	O.IDENTIFY-AUTHENTICATE	User identification and authentication
		The TOE shall identify and authenticate clients accessing via the network. The TOE shall reject authentication requests that may lead too many authentication failures. The TOE shall only accept authentication secrets that are strong enough against attacks such as a dictionary attack.
2.	O.PROTECT-NETWORK	Network protection
		The TOE shall protect network communications between the TOE and a remote trusted IT product (a client or a distinct TCAB) from un-detection of modification, eavesdropping and impersonation.
3.	O.LOGICAL-PACKAGE	Logical packaging
		The TOE shall detect modification directly performed on documents stored under control of the TOE. (Documents stored on an off-line disc mounted on the system are under control of the TOE.) The TOE shall not recognize a forged document as an authentic document. The TOE shall protect documents with digital signatures. The TOE shall protect a list of these signatures by providing an additional digital signature for the list.
4.	O.REVISE-CONTROL	Document revision control
		The TOE shall control revising documents. When revising an original document, the TOE shall store the revised document as a new version of the document, without overwriting or deleting any previous versions of the document. The TOE shall not provide capability to delete old versions of documents. The TOE shall not provide capability to revise duplicates to prevent inconsistencies between the duplicates and the original. The TOE shall provide capability to view old versions of each document. The TOE shall not revise documents stored on off-line discs.
5.	O.DUPLICATE-CONTROL	Document duplicate control
		The TOE shall control creating duplicates. The TOE shall distinguish an original document from its duplicates. The TOE shall provide information that it is recognizable for the clients whether a document is an original or a duplicate.
6.	O.DELETE-CONTROL	Document delete control

		The TOE shall control deleting documents. The TOE shall not delete an original document during the specified retention period. The TOE may delete temporary documents and duplicates. The TOE may delete original documents that are out of the specified retention period. The TOE shall only provide capability to delete entire documents, not particular document versions. The TOE shall control retention period configuration so that the retention period can only be changed to a longer one.
7.	O.AUDIT	Auditing
		The TOE shall record access history of the TOE. The TOE shall record document access logs. The document access logs shall contain information about storage date, access date, revision date, deletion date, and the accessing client. The TOE shall record system timer configuration history. The TOE shall provide capability to view the system timer configuration history. The TOE shall provide capability to view the recorded audit data for authorized clients.
8.	O.PROTECT-SYSTEM	System protection
		The TOE shall protect itself by detecting unauthorized modification of the following data: security management data and audit data. The TOE shall detect modification of these data even if they are restored from backup data.
9.	O.MANAGE-SYSTEM	System management
		The TOE shall provide capability to manage the TOE for authorized privileged clients only. The TOE shall provide capability to backup the TOE and documents for authorized privileged clients.

4.2 Security Objectives for the Environment

Some policies and threats are beyond the capability of the TOE to adequately mitigate without support from the TOE operational environment. These policies and threats derive security objectives for the environment that are listed in the following sections.

4.2.1 Security Objectives for the IT Environment

Table 10 Security objectives for the IT environment

1.	OIE.SUPPORT-CRYPTO	Cryptographic operation support
		The cryptographic module shall provide capability of cryptographic operations for the TOE. The secure communication module shall provide capability of secure communication for the TOE.
2.	OIE.OS-LOGIN	OS login control support
		The OS of the machine shall provide capability to control login for restricting direct access to the TOE.

4.2.2 Security Objectives for the Non-IT Environment

Table 11 Security objectives for the Non-IT environment

1.	OE.MANAGE-MEDIA	Media management
		Those responsible for the TOE shall properly manage media. The media are such as off-line discs storing documents, external media storing audit data, backup media, and a primary storage of the TCAB (if the primary storage is not protected in conjunction with the TCAB-Kernel). Those responsible for the TOE shall specify storage space for electronic media. Those responsible for the TOE shall maintain the media in a locked cabinet. Those responsible for the TOE shall record check-out/check-in history of the electronic media. Those responsible for the TOE shall check the condition of the media at regular intervals. Those responsible for the TOE may duplicate media for availability reasons, but those responsible for the TOE shall not confuse duplicates with the original media.
2.	OE.TRAIN	Training
		Those responsible for the security of the organization shall properly assign administrators as defined in Table 4 except the TCAB-Customer-Engineer. Those responsible for the security of the organization shall provide initial and ongoing training for the assigned administrators except the TCAB-Customer-Engineer. Those responsible for maintenance of the TOE shall assign proper person for TCAB-Customer-Engineer. Those responsible for maintenance of the TOE shall provide initial and ongoing training for the assigned customer engineer. Those responsible for the TOE shall train users and administrators who have access rights to the TOE to maintain their authentication data properly. Those responsible for the security of the organization shall provide training for TCAB-Auditor to audit at regular intervals. Those responsible for the security of the organization shall provide training for TCAB-Administrator to backup the system data and documents at regular intervals. Those responsible for the security of the organization shall plan updates of the TOE systematically.
3.	OE.PHYSICAL-PACKAGE	Physical packaging
		Those responsible for the TOE shall protect the security kernel of the TOE (TCAB-Kernel) physically. Those responsible for the TOE shall ensure that only TCAB-Key-Owner can remove (unlock) the physical protection. Those responsible for the TOE shall ensure that only TCAB-OS-Administrator can login to the TOE abstract machine. Those responsible for the TOE shall chose different persons for TCAB-Key-Owner and TCAB-OS-Administrator.
4.	OE.ACCESS-CONTROL	Detailed access control
		Those responsible for the TOE shall ensure that systems providing detailed document access control capability are properly used in conjunction with the TOE. The detailed document access control is such as individual user based access control, workflow status based access control and so on.
5.	OE.PLATFORM	The platform of the TOE

		Those responsible for installation shall ensure that the modules are properly installed and configured. Those responsible for installation shall ensure that the abstract machine is properly installed and configured. Those responsible for installation shall ensure that the secure communication module is configured to allow usage of cryptography that is compatible with the claimed strength of function level only. Those responsible for the TOE installation/maintenance shall apply UPS device to the TOE. Those responsible for installation shall ensure that no viruses and Trojan horses are installed on the machine.
6.	OE.DEDICATED-MACHINE	Dedicated machine
		Those responsible for the TOE installation/maintenance shall ensure that the TOE works on a dedicated machine. Those responsible for the TOE installation/maintenance shall ensure that no components other than that ones listed in Table 2 and the TOE itself are installed in the machine. Those responsible for the TOE installation/maintenance shall terminate all network services other than the services provided by the TOE.
7.	OE.PRIVATE-NETWORK	Located on private network
		Those responsible for the TOE shall locate the TOE on a private network. Those responsible for the TOE shall not connect the TOE directly to a public network. Those responsible for the TOE shall locate the TOE on a network that is properly protected by a firewall, or on a network that has no connections to a public network.
8.	OE.MANAGER	Manager responsible for the document management
		Those responsible for the security of the organization shall specify a manager who is responsible for the electronic document management. This manager is responsible for systematic planning of maintenance, checks, and updates of the system, and he is responsible for ensuring protection of documents during the maintenance.
9.	OE.PROTECT-CONTENTS	Contents protection
		Those responsible for the TOE shall ensure that contents encryption systems are properly used in conjunction with the TOE. Those responsible for the TOE shall ensure that contents signing systems are properly used in conjunction with the TOE.
10.	OE.VIRUS-CHECK	Virus check
		Those responsible for the TOE shall ensure that documents acquired from out of the organization are virus-checked before using them.
11.	OE.READABILITY	Readability
		Those responsible for the TOE shall maintain systems for visualizing electronic documents stored in the TOE. Those responsible for the TOE shall have capability of visualizing the documents on a monitor or papers, when the documents are required to view.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

The TOE's security requirements have exclusively been taken from ISO/IEC 15408 part 2 (i.e. the set is CC part 2 conformant) and can be categorized in the following seven categories:

1) Identification and authentication,
2) Network protection,
3) Document access control,
4) Document protection,
5) Audit,
6) System protection, and
7) System management.

In the following sections, several TOE-specific terms are used for specifying security requirements. Definitions of these terms are summarized as follows:

Registered flag: When a user account is registered (created), the account information is marked as "registered." When a user account is un-registered, the account information is marked as "un-registered." The TSF rejects authentication requests that target the un-registered user account. Once an account is un-registered, the account cannot be re-registered. The registered flag is used for keeping such account status.

Activated flag: When a user account is registered (created), the account information is marked as "activated." When a user account is de-activated, the account information is marked as "de-activated." The TSF rejects authentication requests that target the de-activated user account. The de-activated user account can be re-activated by a privileged authorized user. The activated flag is used for keeping such account status.

5.1.1 Identification and Authentication

This category of security requirements corresponds to the following security objective.

1.	O.IDENTIFY-AUTHENTICATE	User identification and authentication
		The TOE shall identify and authenticate clients accessing via the network. The TOE shall reject authentication requests that may lead too many authentication failures. The TOE shall only accept authentication secrets that are strong enough against attacks such as a dictionary attack.

Security functional requirements for this security function category are listed in Table 12.

Table 12 Identification and authentication security requirements

Security Requirement		Component
Login controls	User authentication before any action	FIA_UAU.2 (a)
	User identification before any action	FIA_UID.2 (a)
	Multiple authentication mechanisms	FIA_UAU.5
Password selection	Verification of secrets	FIA_SOS.1
Failure handling	Authentication failure handling	FIA_AFL.1 (a1) FIA_AFL.1 (a2) FIA_AFL.1 (b)
Security attributes	User attribute definition	FIA_ATD.1
	User-subject binding	FIA_USB.1

FIA_UAU.2 User authentication before any action (a)

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

FIA_UID.2 User identification before any action (a)

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

Note:

The TSF-mediated actions are: access operations to documents and management operations to the TOE.

FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [**account name/password authentication mechanism and SSL client authentication (public-key certificate based) mechanism**] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**following rules:**

(1) If the client uses the account having a role other than TCAB-System, the client must be authenticated by using account name/password authentication mechanism.

(2) If the client uses the account having a role TCAB-System, the client must be authenticated by using both of account name/password authentication mechanism and SSL client authentication (public-key certificate based) mechanism].

Note:

The account having a role TCAB-System is used only by the TOE, a distinct TCAB, a distinct TCABX1, and a distinct TCABW1. These products do not change their account names and passwords; therefore, an additional authentication is required for not weaken the strength of the authentication function.

FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [**authentication secret quality metric defined below**].

Authentication secret quality metric:

1) the length of it is at least eight (8) characters,

2) it contains at least one (1) alphabet character,

3) it contains at least one (1) numeric character, and

4) it contains at least one (1) non-alphanumeric character.

Note:

This metric assumes that the authentication secret is a password (string).

FIA_AFL.1 Authentication failure handling (a1)

FIA_AFL.1.1 The TSF shall detect when [**1**] unsuccessful authentication attempts occur related to [**a wrong combination of account name and password, a de-activated user account or an un-registered user account**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**record audit data**].

FIA_AFL.1 Authentication failure handling (a2)

FIA_AFL.1.1 The TSF shall detect when [**more than 50 times within the recent 5 seconds**] unsuccessful authentication attempts occur related to [**a wrong combination of account name and password, a de-activated user account or an un-registered user account**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**reject the further login requests until the number of detected unsuccessful authentication attempts within the recent 5 seconds becomes less than 50**].

Note:

The TOE assumes that business-processing system accesses the TOE. The business-processing system does not mistype a password, in general.

FIA_AFL.1 Authentication failure handling (b)

FIA_AFL.1.1 The TSF shall detect when [**3 times within 5 minutes**] unsuccessful authentication attempts occur related to [**a wrong combination of account name and password, a de-activated user account or an un-registered user account**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**send an e-mail containing the information about the detected authentication failure to the specified notification address**].

Note:

Authentication failures may be caused by a human user, who uses an account having a role TCAB-Administrator or TCAB-Auditor, or a mis-configured business processing system.

FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**account name, activated flag, registered flag, and role**].

Note:

The activated flag is used for determining whether the account is terminated or not. The registered flag is used for determining whether the account is un-registered or not.

FIA_USB.1 User-subject binding

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

Note:

The subject is an instance (Java RMI server instance) created in the TOE on a success of a client authentication.

5.1.2 Network Protection

This category of security requirements corresponds to the following security objective.

2.	O.PROTECT-NETWORK	Network protection
		The TOE shall protect network communications between the TOE and a remote trusted IT product (a client or a distinct TCAB) from un-detection of modification, eavesdropping and impersonation.

Security functional requirements for this security function category are listed in Table 13.

Table 13 Network protection security requirements

Security Requirement		Component
Initiated by TSF	Inter-TSF trusted channel	FTP_ITC.1 (a1)
	Inter-TSF trusted channel	FTP_ITC.1 (a2)

FTP_ITC.1 Inter-TSF trusted channel (a1)

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [**the TSF**] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**Inter-TCAB document transfer function**].

Note:

The TSF only initiates a trusted channel for the specified functions. The secure communication module realizes the trusted channel functionality.

FTP_ITC.1 Inter-TSF trusted channel (a2)

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [**the remote trusted IT product**] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**all the functions of the TOE that can be invoked from external clients**].

Note:

The TSF only initiates a trusted channel for the specified functions. The secure communication module realizes the trusted channel functionality.

5.1.3 Document Protection

This category of security requirements corresponds to the following security objective.

3.	O.LOGICAL-PACKAGE	Logical packaging
		The TOE shall detect modification directly performed on documents stored under control of the TOE. (Documents stored on an off-line disc mounted on the system are under control of the TOE.) The TOE shall not recognize a forged document as an authentic document. The TOE shall protect documents with digital signatures. The TOE shall protect a list of these signatures by providing an additional digital signature for the list.

Security functional requirements for this security function category are listed in Table 14.

Table 14 Document protection security requirements

Security Requirement		Component
Document protection	Stored data integrity monitoring and action	FDP_SDI.2

FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored within the TSC for [**integrity errors**] on all objects, based on the following attributes: [**digital signatures for document contents, document security attributes, and document lists containing digital signatures for each document contents**].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [

1) Record audit data containing the information about the detected event,

2) Send an e-mail containing the information about the detected event to a configured e-mail address, and

3) If the error is detected during processing a client request, suppress the requested operation and return an error or an exception to the client].

5.1.4 Document Access Control

This category of security requirements corresponds to the following security objectives.

4.	O.REVISE-CONTROL	Document revision control
		The TOE shall control revising documents. When revising an original document, the TOE shall store the revised document as a new version of the document, without overwriting or deleting any previous versions of the document. The TOE shall not provide capability to delete old versions of documents. The TOE shall not provide capability to revise duplicates to prevent inconsistencies between the duplicates and the original. The TOE shall provide capability to view old versions of each document. The TOE shall not revise documents stored on off-line discs.
5.	O.DUPLICATE-CONTROL	Document duplicate control
		The TOE shall control creating duplicates. The TOE shall distinguish an original document from its duplicates. The TOE shall provide information that it is recognizable for the clients whether a document is an original or a duplicate.
6.	O.DELETE-CONTROL	Document delete control
		The TOE shall control deleting documents. The TOE shall not delete an original document during the specified retention period. The TOE may delete temporary documents and duplicates. The TOE may delete original documents that are out of the specified retention period. The TOE shall only provide capability to delete entire documents, not particular document versions. The TOE shall control retention period configuration so that the retention period can only be changed to a longer one.

Security functional requirements for this security function category are listed in Table 15.

Table 15 Access control security requirements

Security Requirement		**Component**
Access control	Complete access control	FDP_ACC.2
	Security attribute based access control	FDP_ACF.1
Access control management	Static attribute initialization	FMT_MSA.3
	Management of security attributes	FMT_MSA.1 (a) FMT_MSA.1 (b)
Export	Export of user data with security attributes	FDP_ETC.2 (a) FDP_ETC.2 (b)

Import	Import of user data with security attributes	FDP_ITC.2 (a) FDP_ITC.2 (b)
	Inter-TSF basic TSF data consistency	FPT_TDC.1 (a) FPT_TDC.1 (b)

FDP_ACC.2 Complete access control

FDP_ACC.2.1 The TSF shall enforce the [**Mandatory Document Access Control SFP**] on [**instances created in the TOE that execute accesses on behalf of clients and document objects**] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Note:

The subject is an instance (Java RMI server instance) created in the TOE on a success of a client authentication.

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the [**Mandatory Document Access Control SFP**] to objects based on [**object attributes document type, document location, retention period and subject attribute role**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**rules specified in the Table 16 and Table 17**].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**The list of document objects can be acquired by any authorized client**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [**following additional rules:**

1) Overwriting document objects is not allowed.

2) An original document object that is in the retention period cannot be deleted.

3) Partial deletion of a document object (e.g. deletion of a part of the object containing an individual version) is not allowed].

Note:

An original document object means a document object having a document type “Original Document.”

Table 16 Access control rules for document objects stored in the internal hard-drives

Role	Document Type		
	Temporary Document	**Original Document**	**Duplicate**
TCAB-User	Create Revise (version up) Read Delete Inter-TCAB transfer	Create Revise (version up) Read Delete Duplicate	Read Delete Inter-TCAB transfer Move to off-line discs

Role	Document Type		
	Temporary Document	**Original Document**	**Duplicate**
	Move to off-line discs	Inter-TCAB transfer Move to off-line discs	
TCAB-RO-User	Read	Read	Read
TCAB-Administrator	Read Delete Inter-TCAB transfer Move to off-line discs Backup	Read Delete Duplicate Inter-TCAB transfer Move to off-line discs Backup	Read Delete Inter-TCAB transfer Move to off-line discs Backup
TCAB-Auditor	None	None	None
TCAB-System	Internal procedure for Inter-TCAB transfer	Internal procedure for Inter-TCAB transfer	Internal procedure for Inter-TCAB transfer
Note: The "TCAB-System" is a role assigned only for the account used by the remote TCAB. When transferring a document from a sender-TCAB to a receiver-TCAB, the sender-TCAB shall be authenticated as a client having a role TCAB-System by the receiver-TCAB. The receiver-TCAB performs internal procedures for the document transferring only if the sender-TCAB is authenticated as a client having a role TCAB-System. The words "Internal procedure for Inter-TCAB transfer" denotes the internal procedures for the document transferring performed by the receiver-TCAB.			

Table 17 Access control rules for document objects stored on off-line discs.

Role	Document Type		
	Temporary Document	**Original Document**	**Duplicate**
TCAB-User	Read Delete	Read Delete	Read Delete
TCAB-RO-User	Read	Read	Read
TCAB-Administrator	Read Delete	Read Delete	Read Delete
TCAB-Auditor	None	None	None
TCAB-System	None	None	None
Note: The "TCAB-System" is a role assigned only for the account used by the remote TCAB.			

Note:

The TOE records and manages a list of document objects, that has been written out to off-line discs, on the internal hard-drive of the TOE. An entry of the list can be deleted even if the corresponding document object (disc) is **not** mounted on the system. Once the entry has been deleted, the corresponding document object no longer can be accessed.

FMT_MSA.3 Static attribute initialisation

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

FMT_MSA.3.2 The TSF shall allow the [**TCAB-User**] to specify alternative initial values to override the default values when an object or information is created.

Note:

The restrictive default value is the document type, “Original Document”. The TOE allows to override the default document type with an alternative initial value, “Temporary Document”, on a document object creation.

FMT_MSA.1 Management of security attributes (a)

FMT_MSA.1.1 The TSF shall enforce the [**Mandatory Document Access Control SFP**] to restrict the ability to [**perform one of the operations listed below on**] the security attributes [**document type and retention period**] to [**TCAB-User**].

Operations:

1) Specify the document type on document object creation (either “Temporary Document” or “Original Document”).

2) Change the document type from “Temporary Document” to “Original Document”.

3) Specify the retention period on document object creation.

4) Lengthen the retention period.

Note:

A document object that has a type of “Original Document” can be duplicated. The duplicate will have a type of “Duplicate”. Therefore this is not managed by the TCAB-User but automatically by the TOE.

FMT_MSA.1 Management of security attributes (b)

FMT_MSA.1.1 The TSF shall enforce the [**Mandatory Document Access Control SFP**] to restrict the ability to [**view**] the security attributes [**document type and retention period**] to [**TCAB-User, TCAB-RO-User, and TCAB-Administrator**].

FMT_MSA.1 Management of security attributes (c)

FMT_MSA.1.1 The TSF shall enforce the [**Mandatory Document Access Control SFP**] to restrict the ability to [**view**] the security attributes [**document access logs**] to [**TCAB-User, TCAB-Administrator, and TCAB-Auditor**].

FDP_ETC.2 Export of user data with security attributes (a)

FDP_ETC.2.1 The TSF shall enforce the [**Mandatory Document Access Control SFP**] when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.2.2 The TSF shall export the user data with the user data’s associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TSC: [**when the TSF transfers (exports) document contents to another product, which is compatible with TrustyCabinet UX V1 document exportation protocol, via the network, the TSF shall export**

the document contents with its security attributes document type and retention period].

Note:

This is a requirement for the TCAB to securely transfer document contents via the network and to keep access control policy for the document object created at the destination.

In this requirement, "another product, which is compatible with TrustyCabinet UX V1 document exportation protocol" is a distinct TCAB or a distinct TCABX1.

FDP_ETC.2 Export of user data with security attributes (b)

FDP_ETC.2.1 The TSF shall enforce the [**Mandatory Document Access Control SFP**] when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TSC: [

1) When document contents are written-out (export) to an off-line disc, the TSF shall export the document contents with its security attributes document type, retention period and digital signature.

2) When the TSF exports document contents to an off-line disc, the TSF shall create a list of the exported (created) document objects and record this list on the off-line disc with a digital signature for the list.

3) The list, described above, shall contain digital signatures of each document object stored on the off-line disc].

Note:

This is a requirement for the TCAB to write-out/mount document objects on off-line discs keeping integrity and keeping consistency of access control policy.

FDP_ITC.2 Import of user data with security attributes (a)

FDP_ITC.2.1 The TSF shall enforce the [**Mandatory Document Access Control SFP**] when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [**when document contents are transferred (imported) from another**

product, which is compatible with TrustyCabinet UX V1 document importation protocol, via the network, the TSF shall import the document contents with its security attributes document type and retention period].

Note:

This is a requirement for the TCAB to securely transfer document contents via the network and to keep access control policy for the created document object.

In this requirement, "another product, which is compatible with TrustyCabinet UX V1 document importation protocol" is a distinct TCAB, a distinct TCABX1, or a distinct TCABW1.

FDP_ITC.2 Import of user data with security attributes (b)

FDP_ITC.2.1 The TSF shall enforce the [**Mandatory Document Access Control SFP**] when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: [

1) When a document object (on off-line disc) is mounted and used (imported), the TSF shall import the document contents of the object with its security attributes document type, retention period and digital signature.

2) When an off-line disc is mounted on the TOE, the TSF shall verify a stored document list, which lists document objects stored on the off-line disc, by using digital signature(s).

3) When a document object, which is stored on an off-line disc, is accessed, the TSF shall verify the document object by using digital signature(s)].

Note:

This is a requirement for the TCAB to write-out/mount document objects on off-line discs keeping integrity and keeping consistency of access control policy.

FPT_TDC.1 Inter-TSF basic TSF data consistency (a)

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [**document type, retention period, and document access logs**] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [**the rule that TSF data received via the network (document type, retention period, and document access logs) are interpreted just as are without further interpretation**] when interpreting the TSF data from another trusted IT product.

Note:

In this requirement, another trusted IT product denotes a distinct TCAB, a distinct TCABX1, or a distinct TCABW1.

FPT_TDC.1 Inter-TSF basic TSF data consistency (b)

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [**document type, retention period, document access logs, a document list, and digital signatures for integrity protection, which are stored on the mounted (importing) off-line disc,**] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [**the rule that the TSF data on the off-line disc (document type, retention period, document access logs, a document list, and digital signatures for integrity protection) are interpreted just as are without further interpretation**] when interpreting the TSF data from another trusted IT product.

Note:

In this requirement, another trusted IT product denotes a distinct TCAB, a distinct TCABX1, or a distinct TCABW1.

5.1.5 Audit

This category of security requirements corresponds to the following security objective.

7.	O.AUDIT	Auditing
		The TOE shall record access history of the TOE. The TOE shall record document access logs. The document access logs shall contain information about storage date, access date, revision date, deletion date, and the accessing client. The TOE shall record system timer configuration history. The TOE shall provide capability to view the system timer configuration history. The TOE shall provide capability to view the recorded audit data for authorized clients.

Security functional requirements for this security function category are listed in Table 18.

Table 18 Audit security requirements

Security Requirement		Component
Audit events	Audit data generation	FAU_GEN.1
	User identity association	FAU_GEN.2
Time stamp	Reliable time stamps	FPT_STM.1
Audit review	Audit review	FAU_SAR.1
Audit protection	Protected audit trail storage	FAU_STG.1
	Action in case of possible audit data loss	FAU_STG.3 (a) FAU_STG.3 (b)

	Prevention of audit data loss	FAU_STG.4

FAU_GEN.1 Audit data generation

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) [**The events listed in Table 19, Table 20, and Table 21**].

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, 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, [**nothing.**]

Table 19 Events recorded as system access history

Event	Description
Start-up of the TOE	On start-up of the TOE, the result of the start-up procedure shall be recorded. The start-up procedure includes integrity check of TSF data. The integrity check success/failure results in a success/failure of the start-up. Corresponds to FAU_GEN.1 and FPT_ITT.3.
Shutdown of the TOE	On shutting down of the TOE, the TOE shall protect TSF data from undetected modifications. Corresponds to FPT_ITT.3.
Login authentication	Corresponds to FIA_AFL.1 (a1), (a2).
Changing password	Corresponds to FIA_SOS.1 and FMT_MTD.1 (a).
User account registration	Corresponds to FMT_MTD.1 (a).
User account un-registration	Corresponds to FMT_MTD.1 (a).
User account de-activation	Corresponds to FMT_MTD.1 (a).
User account re-activation	Corresponds to FMT_MTD.1 (a).
System timer configuration	Corresponds to FMT_MTD.1 (d).
Viewing system timer configuration history	Corresponds to FAU_SAR.1.
Integrity check of document list	On the first access to a DocSpace of the TOE, integrity check shall be performed and the result shall be recorded. The integrity check success/failure results in a success/failure of accessing the DocSpace. Corresponds to FDP_SDI.2 and FDP_ITC.2 (b).
Integrity check of document	On document object access, integrity check shall be performed and the result shall be recorded. The document object access includes creation, revision, read, duplication, deletion, inter-TCAB transfer, write out to off-line disc, viewing attributes, and viewing access logs of document object. The integrity check success/failure results in a success/failure of accessing the document object. Corresponds to FDP_SDI.2 and FDP_ITC.2 (b).
Creation of document	Corresponds to FDP_ACF.1.
Revision of document	Corresponds to FDP_ACF.1.
Read of document	Corresponds to FDP_ACF.1.

Event	Description
Duplication of document	Corresponds to FDP_ACF.1.
Deletion of document	Corresponds to FDP_ACF.1.
Inter-TCAB document transfer	Corresponds to FTP_ITC.1 (a1), FDP_ETC.2 (a) and FDP_ACF.1.
Write out documents onto off-line disc	Corresponds to FDP_ACF.1 and FDP_ETC.2 (b)
Viewing document attributes	Corresponds to FDP_ACF.1.
Viewing document access logs	Corresponds to FDP_ACF.1 and FAU_SAR.1.
Internal procedures for Inter-TCAB transfer	Corresponds to FDP_ACF.1 and FDP_ITC.2 (a).
Acquisition of document list	Corresponds to FDP_ACF.1.
Changing document type	Corresponds to FMT_MSA.1 (a).
Lengthen retention period of document	Corresponds to FMT_MSA.1 (a).
Viewing system access history	Corresponds to FAU_SAR.1
Move system access history onto external media	Corresponds to FMT_MTD.1 (c).
Creation of backup	Corresponds to FMT_MTD.1 (e).
Supplements: The system access history shall be recorded on System Data Partition of the TOE working machine. For each event, the event occurrence time information, the event occurrence identification number, the event type (e.g., method name), client information (if applicable), and the result (success/failure) shall be recorded. The time information consists of a date/time and a timer-identifier. The timer-identifier indicates that how many times the system timer was configured. The client information consists of an account name, an IP address of the client machine.	

Note:

Document accesses are recorded both as system access history (Table 19) and as document access logs (Table 20).

Table 20 Events recorded as document access logs

Event	Description
Integrity check of document	On document object access, integrity check shall be performed and the result shall be recorded. The document object access includes creation, revision, read, duplication, deletion, inter-TCAB transfer, write out to off-line disc, viewing attributes, and viewing access logs of document object. The integrity check success/failure results in a success/failure of accessing the document object. Corresponds to FDP_SDI.2 and FDP_ITC.2 (b).
Creation of document	Corresponds to FDP_ACF.1.
Revision of document	Corresponds to FDP_ACF.1.
Read of document	Corresponds to FDP_ACF.1.
Duplication of document	Corresponds to FDP_ACF.1.
Deletion of document	Corresponds to FDP_ACF.1.
Inter-TCAB document transfer	Corresponds to FTP_ITC.1 (a1), FDP_ETC.2 (a) and FDP_ACF.1.
Write out documents onto off-line disc	Corresponds to FDP_ACF.1 and FDP_ETC.2 (b)
Viewing document attributes	Corresponds to FDP_ACF.1.
Viewing document access logs	Corresponds to FDP_ACF.1 and FAU_SAR.1.
Internal procedures for Inter-TCAB transfer	Corresponds to FDP_ACF.1 and FDP_ITC.2 (a).
Changing document type	Corresponds to FMT_MSA.1 (a).

Event	Description
Lengthen retention period of document	Corresponds to FMT_MSA.1 (a).
Supplements: The document access logs shall be recorded on User Data Partition of the TOE working machine in conjunction with the corresponding document object. The document access logs shall be recorded only for the document objects stored on the User Data Partition. For each event, the event occurrence time information, the event occurrence identification number, the event type (e.g., method name), client information, and the result (success/failure) shall be recorded. The time information consists of a date/time and a timer-identifier. The timer-identifier indicates that how many times the system timer was configured. The client information consists of an account name, an IP address of the client machine.	

Note:

Document object accesses are recorded both as system access history (Table 19) and as document access logs (Table 20).

Table 21 Events recorded as system timer configuration history

Event	Description
System timer configuration	Corresponds to FMT_MTD.1 (d).
Supplements: The system timer configuration history shall be recorded on System Data Partition of the TOE working machine. For each event, the current time information, the configured new time information, and client information shall be recorded. The time information consists of a date/time and a timer-identifier. The timer-identifier indicates that how many times the system timer was configured (i.e., the configured new time information contains an incremented timer-identifier). The client information consists of an account name, an IP address of the client machine.	

FAU_GEN.2 User identity association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FPT_STM.1 Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide [**TCAB-Auditor**] with the capability to read [**all audit data**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_STG.1 Protected audit trail storage

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

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

FAU_STG.3 Action in case of possible audit data loss (a)

FAU_STG.3.1 The TSF shall take [**the action sending an e-mail containing the information about the detected event to the configured e-mail address**] if the audit trail exceeds [**a warning level configured during the TOE installation/setup procedure**].

FAU_STG.3 Action in case of possible audit data loss (b)

FAU_STG.3.1 The TSF shall take [**the action that sending an e-mail containing the information about the detected event to the configured e-mail address and rejecting requests from clients with a role other than TCAB-Administrator or TCAB-Auditor**] if the audit trail exceeds [**a maximum level configured during the TOE installation/setup procedure**].

FAU_STG.4 Prevention of audit data loss

FAU_STG.4.1 The TSF shall [**prevent auditable events, except those taken by the authorised user with special rights**] and [**shutting down the TOE**] if the audit trail is full.

Note:

If the audit trail is full, the TOE automatically shuts-down the TOE itself and no one can access to the TOE.

To restore the TOE working machine, TCAB-Customer-Engineer shall perform maintenance/restoration procedures.

5.1.6 System Protection

This category of security requirements corresponds to the following security objective.

8.	O.PROTECT-SYSTEM	System protection
		The TOE shall protect itself by detecting unauthorized modification of the following data: security management data and audit data. The TOE shall detect modification of these data even if they are restored from backup data.

Security functional requirements for this security function category are listed in Table 22.

Table 22 System protection security requirements

Security Requirement		Component
TSF protection	Basic internal TSF data transfer protection	FPT_ITT.1
	TSF data integrity monitoring	FPT_ITT.3
	Non-bypassability of the TSP	FPT_RVM.1

	TSF domain separation	FPT_SEP.1
	Management of security functions behaviour	FMT_MOF.1

FPT_ITT.1 Basic internal TSF data transfer protection

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

FPT_ITT.3 TSF data integrity monitoring

FPT_ITT.3.1 The TSF shall be able to detect [**modification of data**] for TSF data transmitted between separate parts of the TOE.

FPT_ITT.3.2 Upon detection of a data integrity error, the TSF shall take the following actions: [

1) Record audit data containing the information about the detected event,

2) Send e-mail containing the information about the detected event to a configured e-mail address, and

3) Terminate the TOE].

Note:

Here "transmission" of data describes the following procedure: integrity-protected storage of these data by the TOE and reading of the formerly stored data by the TOE again. That means that "separate parts of the TOE" here both refer to the TOE (separation in time). This requirement component has been chosen because there is no "Stored data integrity" component applicable to TSF data (FDP_SDI is suitable for user data only).

On start-up of the TOE, the TSF checks the integrity of the stored TSF data; therefore, a detection of a modification of the TSF data results in a failure of the start-up (in Table 19).

FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [**disable and modify the behaviour of**] the functions [**all the TSF(s)**] to [**no one**].

Note:

The TOE shall prohibit the de-activation and modification of any TOE-provided functions.

5.1.7 System Management

This category of security requirements corresponds to the following security objective.

9.	O.MANAGE-SYSTEM	System management
		The TOE shall provide capability to manage the TOE for authorized privileged clients only. The TOE shall provide capability to backup the TOE and documents for authorized privileged clients.

Security functional requirements for this security function category are listed in Table 23.

Table 23 System management security requirements

Security Requirement		Component
Security roles	Restrictions on security roles	FMT_SMR.2
Account management	Management of TSF data	FMT_MTD.1 (a)
Audit management	Management of TSF data	FMT_MTD.1 (b) FMT_MTD.1 (c) FMT_MTD.1 (d)
Backup	Management of TSF data	FMT_MTD.1 (e)

FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 The TSF shall maintain the roles: [**TCAB-User, TCAB-RO-User, TCAB-Administrator, TCAB-Auditor and TCAB-System**].

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions [**one user account has only one role**] are satisfied.

FMT_MTD.1 Management of TSF data (a)

FMT_MTD.1.1 The TSF shall restrict the ability to [**manage**] the [**user account**] to [**TCAB-Administrator and TCAB-Auditor based on the rules specified in the Table 24**].

Table 24 Rules and privileges for account management

Role	Privileges
TCAB-Administrator	Register and un-register accounts having following roles: TCAB-User, TCAB-RO-User, and TCAB-Administrator. De-activate and re-activate accounts having following roles: TCAB-User, and TCAB-RO-User.
TCAB-Auditor	Register and un-register accounts having a TCAB-Auditor role.

Rules:

1) User password can be changed only by the corresponding authorized client.
2) An account of a client currently logged-in to the TCAB cannot be un-registered.

FMT_MTD.1 Management of TSF data (b)

FMT_MTD.1.1 The TSF shall restrict the ability to [**modify**] the [**e-mail address used for notifications**] to [**TCAB-Administrator**].

FMT_MTD.1 Management of TSF data (c)

FMT_MTD.1.1 The TSF shall restrict the ability to [**move**] the [**audit data onto external media**] to [**TCAB-Auditor**].

FMT_MTD.1 Management of TSF data (d)

FMT_MTD.1.1 The TSF shall restrict the ability to [**configure**] the [**system timer**] to [**TCAB-Administrator**].

FMT_MTD.1 Management of TSF data (e)

FMT_MTD.1.1 The TSF shall restrict the ability to [**backup**] the [**TSF data**] to [**TCAB-Administrator**].

Note:

The backup data can be restored by TCAB-Customer-Engineer only.

5.2 TOE Security Assurance Requirements

The assurance components for the TOE are summarized in Table 25. It is the set of components defined by the evaluation assurance level **EAL3**. Besides EAL3 no other requirements have been chosen. Therefore the assurance requirements are conformant to CC part 3.

Table 25 TOE assurance requirement components (EAL3)

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.3	Authorisation controls
	ACM_SCP.1	TOE CM coverage
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation, and start-up procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.2	Security enforcing high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life cycle support	ALC_DVS.1	Identification of security measures
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability	AVA_MSU.1	Examination of guidance

Assurance Class	Component ID	Component Title
assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

5.3 Security Requirements for the IT Environment

In this section, security requirements for the IT environment are identified. These requirements are selected to directly or indirectly satisfy the security objectives for the IT environment.

5.3.1 Cryptographic Operations

This category of security requirements corresponds to the following security objective.

1.	OIE.SUPPORT-CRYPTO	Cryptographic operation support
		The cryptographic module shall provide capability of cryptographic operations for the TOE. The secure communication module shall provide capability of secure communication for the TOE.

Security functional requirements for this security function category are listed in Table 26.

Table 26 Cryptographic operations security requirements

Security Requirement		Component
Secure communication module	Inter-TSF trusted channel	FTP_ITC.1 (b1)
	Inter-TSF trusted channel	FTP_ITC.1 (b2)
	Cryptographic operation	FCS_COP.1 (a)
Cryptographic module	Cryptographic operation	FCS_COP.1 (b)

FTP_ITC.1 Inter-TSF trusted channel (b1)

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [**the TSF**] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**functions required to be initiated by the TOE**].

Note:

In this requirement component, the “TSF” denotes the secure communication module.

The TOE controls when to initiate a trusted channel. The secure communication module realizes the trusted channel functionality. Only for transferring a document between the TOE and a distinct TCAB, the TOE initiates the communication (FTP_ITC.1 (a1)).

FTP_ITC.1 Inter-TSF trusted channel (b2)

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit [**the remote trusted IT product**] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**functions required to be initiated by the remote trusted IT product**].

Note:

In this requirement component, the "TSF" denotes the secure communication module.

The TOE controls when a trusted channel has to be used. The secure communication module realizes the trusted channel functionality. All the functions of the TOE that can be invoked from external clients require to use the trusted channel (FTP_ITC.1 (a2)).

FCS_COP.1Cryptographic operation (a)

FCS_COP.1.1 The TSF shall perform [**cryptographic operations listed in Table 27**] in accordance with a specified cryptographic algorithm [**listed in Table 27**] and cryptographic key sizes [**listed in Table 27**] that meet the following: [**SSL v2/v3 standard**].

Table 27 Cryptographic operations, algorithms, and key sizes

Operation	Algorithm	Key size
Authentication and key exchange	**RSA**	**1024 bits**
Encryption and decryption	**Triple-DES**	**168 bits**
	IDEA	**128 bits**
	RC4	**128 bits**
	RC2	**128 bits**
Hashing	**SHA-1**	**Not applicable**
	MD5	**Not applicable**

Note:

In this requirement component the term "TSF" denotes the cryptographic module.

FCS_COP.1Cryptographic operation (b)

FCS_COP.1.1 The TSF shall perform [**cryptographic operations listed in Table 28**] in accordance with a specified cryptographic algorithm [**listed in Table 28**] and cryptographic key sizes [**listed in Table 28**] that meet the following: [**standards listed in Table 28**].

Table 28 Cryptographic operations, algorithms, key sizes, and standards

Operation	Algorithm	Key size	Standard
Digital signature generation and verification	**RSA**	**1024 bits**	**RSA digital signature: PKCS#1**
Hashing	**MD5**	**Not applicable**	**RFC 1321**

Note:

In this requirement component the term “TSF” denotes the cryptographic module.

5.3.2 OS Login Control

This category of security requirements corresponds to the following security objective.

2.	OIE.OS-LOGIN	OS login control support
		The OS of the machine shall provide capability to control login for restricting direct access to the TOE.

Security functional requirements for this security function category are listed in Table 29.

Table 29 OS login control security requirements

Security Requirement		Component
Login	Timing of identification	FIA_UID.1 (b)
	Timing of authentication	FIA_UAU.1 (b)

FIA_UID.1 Timing of identification (b)

FIA_UID.1.1 The TSF shall allow [**the following TSF-mediated actions**] on behalf of the user to be performed before the user is identified.

(a) select language;

(b) select desktop or console login;

(c) select remote host for login;

(d) help for login function.

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.

Note:

In this requirement component, the “TSF” denotes the OS.

FIA_UAU.1 Timing of authentication (b)

FIA_UAU.1.1 The TSF shall allow [**the following TSF-mediated actions**] on behalf of the user to be performed before the user is authenticated.

(a) select language;

(b) select desktop or console login;

(c) select remote host for login;

(d) help for login function.

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.

Note:

In this requirement component, the “TSF” denotes the OS.

6 TOE Summary Specification

In this section, TOE security functions and TOE security assurance measures provided to meet the security functional requirements in section 5.1 and security assurance requirements in section 5.2 are described.

6.1 TOE Security Functions

6.1.1 Identify and Authenticate Function

SF.I&A.1 User login authentication

Before allowing any other actions, SF.I&A.1 identifies and authenticates the accessing client by account name and password. (Correspondence: FIA_UID.2 (a), FIA_UAU.2 (a))

The authentication fails if a wrong account name/password combination is provided or if a de-activated or an un-registered account name is used. (Correspondence: FIA_AFL.1 (a1), (a2))

If the audit trail exceeds the maximum level, which is configured during the installation/setup procedure, SF.I&A.1 rejects login request from clients with a role other than TCAB-Administrator or TCAB-Auditor. (Correspondence: FAU_STG.3 (b))

If the accessing client has the role TCAB-System, SF.I&A.1 additionally authenticates the client using public key certificates configured during installation or maintenance by TCAB-Customer-Engineer. The public-key certificate based authentication is realized based on SSL protocol. (Correspondence: FIA_UID.2 (a), FIA_UAU.2 (a), FIA_UAU.5)

On success of the client authentication, the TOE creates an instance (Java RMI server instance) and binds the client information including the account name and role to the instance. The TOE returns the instance to the client as a remote reference to the instance. (Correspondence: FIA_USB.1)

If and only if the accessing client is authenticated, a remote reference (Java RMI remote reference) for using other functions such as accessing documents, managing system, and so on, is provided to the client. The remote reference is the only interface for accessing the TOE from external to the TOE and the remote reference only provides function interface (methods) for invoking security functions of the TOE. Therefore, the security functions of the TOE are always invoked. (Correspondence: FPT_RVM.1)

Additionally, the remote reference does not provide methods for disabling and modifying behavior of the security functions. (Correspondence: FMT_MOF.1)

REMARKS:

Client authentication provided by SF.I&A.1 is also used for establishing secure communication channel in conjunction with SF.NET.1. (Correspondence: FTP_ITC.1 (a1), (a2))

SF.I&A.2 Authentication failure handling

If SF.I&A.1 detected an authentication failure; including wrong account name and password combination and use of de-activated or un-registered account name, SF.I&A.2 records audit data and waits for 5 seconds before

responding the authentication request. Additionally, SF.I&A.2 restricts simultaneous authentication processes up to 50 (it results in maximum number of authentication failures within the recent 5 seconds is 50). (Correspondence: FIA_AFL.1 (a1), (a2))

Additionally, SF.I&A.2 counts authentication failures and if 3 authentication failures are detected within 5 minutes, SF.I&A.2 sends an e-mail indicating that continuous authentication failures are detected to the configured notification address. (Correspondence: FIA_AFL.1 (b))

To avoid too much e-mail notifications, SF.I&A.2 does not send an e-mail for 10 minutes after the last notification of continuous authentication failures.

6.1.2 Network Protection Function

SF.NET.1 Network protection

SF.NET.1 provides a communication channel between the TCAB and a client of the TCAB or a distinct TCAB by using secure communication module that provides communication channel based on SSL v2/v3 protocol. SF.NET.1 controls how the secure communication channel is applied. Communication data is encrypted/decrypted and integrity protected/verified during transmission. (Correspondence: FTP_ITC.1 (a1), (a2))

For Inter-TCAB document transfer function, SF.NET.1 initiates the secure communication and identifies and authenticates the communication target. (Correspondence: FTP_ITC.1 (a1))

For using functions provided by TCAB, SF.NET.1 allows an accessing client (including a distinct TCAB as a client) to initiate the secure communication channel. For establishing the secure communication channel, SF.NET.1 sends authentication data to be verified by the client. (Correspondence: FTP_ITC.1 (a2))

REMARKS:

If a client initiates the secure communication, SF.I&A.1 is used to identify and authenticate the accessing client. (Correspondence: FTP_ITC.1.1 (a2))

The secure communication module has to be configured during installation/set-up of TCAB to use algorithms listed in Table 27. (Correspondence: FTP_ITC.1 (b1), (b2), FCS_COP.1 (a))

6.1.3 Access Control Function

SF.ACC.1 Access control

SF.ACC.1 controls all operations between Java RMI server instances accessing on behalf of clients and document objects in the TCAB. (Correspondence: FDP_ACC.2)

SF.ACC.1 authorizes or denies accesses between the instance and document object based on document type, document location, retention period, and role bounded to the instance. The only allowed operations depending on role, document type, and document location are shown in Table 30 and Table 31. (Correspondence: FDP_ACF.1.1, FDP_ACF.1.2)

For checking a retention period of original document object is over or not, SF.ACC.1 acquires a time stamp

from the underlying operating system indirectly via the underlying JVM. (Correspondence: FPT_STM.1)

In addition to Table 30 and Table 31, SF.ACC.1 allows acquiring the list of document objects by any authorized client, and explicitly denies the following accesses: overwriting a document object, deleting an original document object that is in the retention period, and partially deleting a document object (e.g. deleting an individual version contained in a document object). (Correspondence: FDP_ACF.1.3, FDP_ACF.1.4)

SF.ACC.1 restricts the ability to backup whole of hard-drives of the TCAB to TCAB-Administrator. The backup data can include all data stored in the System Program Partition, System Data Partition, and User Data Partition. (Correspondence: FMT_MTD.1 (e), FDP_ACF.1.2)

SF.ACC.1 authorizes viewing document attributes, which include document type and retention period, of each document object for TCAB-User, TCAB-RO-User, and TCAB-Administrator. (Correspondence FMT_MSA.1 (b))

SF.ACC.1 authorizes viewing document access logs of each document object for TCAB-User, TCAB-Administrator, and TCAB-Auditor. (Correspondence: FMT_MSA.1 (c), FAU_SAR.1)

SF.ACC.1 stores the document objects only on the User Data Partition and off-line disc. The executables of the TSF are stored on the System Program Partition (on installation). SF.INT.1 and SF.AUD.1 stores the TSF data on the System Data Partition. By separating the user data area and the system execution area, the TSF's execution is not interfered nor tampered. (Correspondence: FPT_SEP.1)

Table 30 Access control rules for documents stored in the internal hard-drives

Role	Document Type		
	Temporary Document	**Original Document**	**Duplicate**
TCAB-User	Create Revise Read Delete Inter-TCAB transfer Move to off-line discs	Create Revise Read Delete Duplicate Inter-TCAB transfer Move to off-line discs	Read Delete Inter-TCAB transfer Move to off-line discs
TCAB-RO-User	Read	Read	Read
TCAB-Administrator	Read Delete Inter-TCAB transfer Move to off-line discs	Read Delete Duplicate Inter-TCAB transfer Move to off-line discs	Read Delete Inter-TCAB transfer Move to off-line discs
TCAB-Auditor	None	None	None
TCAB-System	Internal procedure for Inter-TCAB transfer	Internal procedure for Inter-TCAB transfer	Internal procedure for Inter-TCAB transfer

Note:
The "TCAB-System" is a role assigned only for the account used by the remote TOE.
When transferring a document from a sender-TCAB to a receiver-TCAB, the sender-TCAB shall be authenticated as a client having a role TCAB-System by the receiver-TCAB. The receiver-TCAB performs internal procedures for the document transferring only if the sender-TCAB is authenticated as a client having a role TCAB-System.
The words "Internal procedure for Inter-TCAB transfer" denotes the internal procedures for the document transferring performed by the receiver-TCAB.

Table 31 Access control rules for documents stored on off-line discs.

Role	Document Type		
	Temporary Document	**Original Document**	**Duplicate**
TCAB-User	Read Delete	Read Delete	Read Delete
TCAB-RO-User	Read	Read	Read
TCAB-Administrator	Read Delete	Read Delete	Read Delete
TCAB-Auditor	None	None	None
TCAB-System	None	None	None
Note: The "TCAB-System" is a role assigned only for the account used by the remote TOE.			

SF.ACC.2 Import/Export control

SF.ACC.2 exports a document contents with its security attributes via the network from the TOE to a distinct TCAB or a distinct TCABX1. The security attributes include a document type and a retention period of the source document object. On exporting a document contents, SF.ACC.2 creates one data archive containing the document contents itself, its security attributes, and its access logs, and transfers it. (Correspondence: FDP_ETC.2.2 (a), FDP_ETC.2.3 (a), FDP_ETC.2.4 (a))

SF.ACC.2 uses SF.NET.1 to protect communications for transferring the data archive from impersonation, eavesdropping and undetected modification. (Correspondence: FDP_ETC.2.3 (a), FDP_ETC.2.4 (a))

SF.ACC.2 receives one data archive that contains a document contents, its security attributes, and its access logs via the network from a distinct TCAB, a distinct TCABX1, or a distinct TCABW1; and SF.ACC.2 imports the document contents with the security attributes. SF.ACC.1 uses the security attributes for enforcing access control policy for the imported and created document object. The security attributes include a document type and a retention period of the imported document object. (Correspondence: FDP_ITC.2.2 (a), FDP_ITC.2.3 (a))

SF.ACC.2 uses SF.NET.1 to protect communications used for receiving the data archive from impersonation, eavesdropping, and undetected modification. (Correspondence: FDP_ITC.2.3 (a), FDP_ITC.2.5 (a))

By using SF.NET.1, SF.ACC.2 ensures that the communicating entity is a distinct TCAB, a distinct TCABX1, or a distinct TCABW1; and the transferred document type, retention period, and access logs can be used by SF.ACC.1 and SF.AUDIT.1 just as are without further interpretation. (Correspondence: FDP_ITC.2.4 (a), FPT_TDC.1 (a))

SF.ACC.3 Document attribute management

For managing security attributes of document objects, SF.ACC.3 provides the following management capabilities:

1) Specifying a document type

   On document object creation, only TCAB-User can specify a document type either "Temporary Document" or "Original Document." If no document type was specified, SF.ACC.3 attaches the default

document type “Original Document” for the document object.

2) Changing the document type

   Only TCAB-User can change document type of a document object that has a document type of “Temporary Document” to “Original Document.”

3) Specifying a retention period

   On document object creation, only TCAB-User shall specify retention period of the document object. Without specifying it, the document object creation process will be failed.

4) Lengthen the retention period

   Only TCAB-User can lengthen retention period of a document object. No one can shorten the retention period.

A document object that has a type of “Original Document” can be duplicated as shown in Table 30. The duplicate will automatically have a type of “Duplicate” (the type is automatically bestowed by the TOE).

(Correspondence: FMT_MSA.1 (a))

SF.ACC.3 has a default security attribute only for document type. The default value is “Original Document.” It is restrictive because the retention-period-based deletion control is performed for the document object. On document object creation, the client (TCAB-User is the only possible role for document object creation) can specify an alternative document type “Temporary Document” for the document object. (Correspondence: FMT_MSA.3)

SF.ACC.4 User account management

SF.ACC.4 manages user account information of the TOE. SF.ACC.4 provides account management capabilities to TCAB-Administrator and TCAB-Auditor based on the rules specified in Table 32. (Correspondence: FMT_MTD.1 (a))

SF.ACC.4 maintains and manages 4 security attributes belonging to individual user account. The attributes are: account name, activated flag, registered flag, and role.

On user account registration (creation), an account name, a password, and a role shall be specified. Both of the activated flag and the registered flag are internally configured by SF.ACC.4. (Correspondence: FIA_ATD.1)

The password shall satisfy a quality metric specified in Table 33. On account registration or on changing password, SF.ACC.4 verifies that the provided password meets the quality metric. If SF.ACC.4 failed in the verification, SF.ACC.4 suppresses the requested operation. (Correspondence: FIA_SOS.1)

SF.ACC.4 maintains 5 roles: TCAB-User, TCAB-RO-User, TCAB-Administrator, TCAB-Auditor, and TCAB-System. Each user account can have only one role. On account registration, one of these roles except TCAB-System shall be specified for the account. The account name and the role of each user account cannot be changed later. (Correspondence: FMT_SMR.2)

On initial installation/set-up, at least one user account having TCAB-Administrator role, one user account having TCAB-Auditor role, and one user account having TCAB-System role are created.

The account having TCAB-System role is used only by a distinct TCAB, a distinct TCABX1, or a distinct TCABW1; therefore, additional registration of an account having TCAB-System role is not permitted.

Table 32 Rules and privileges for account management

Role	Privileges
TCAB-Administrator	Register and un-register accounts having following roles: TCAB-User, TCAB-RO-User, and TCAB-Administrator. De-activate and re-activate accounts having following roles: TCAB-User, and TCAB-RO-User.
TCAB-Auditor	Register and un-register accounts having a TCAB-Auditor role.
Rules: 1) User password can be changed only by the corresponding authorized client. 2) An account of a client currently logged-in to the TCAB cannot be un-registered.	

Table 33 Password quality metric

Aspect	Metric
Length	At least eight (8) characters
Character type	The password must include: at least one (1) alphabet character, at least one (1) numeric character, and at least one (1) non-alphanumeric character.

6.1.4 Integrity Protection Function

SF.INT.1 Document integrity protection

SF.INT.1 generates a digital signature (called a document signature) for each document object, including its security attributes and its access logs, and stores it with the corresponding document object. If the document object is modified (e.g., by revise operation or by a change in the access logs), the document signature is re-generated. The security attributes include document type and retention period. (Correspondence: FDP_SDI.2.1)

SF.INT.1 creates document lists for each document object repository (called a DocSpace). In the document list, each list entry contains a document signature of the corresponding document object. SF.INT.1 also generates a digital signature (called a list signature) for each document list and stores it with the corresponding document list. The list signature is also re-generated if an authorized change is made within the corresponding DocSpace. (Correspondence: FDP_SDI.2.1)

SF.INT.1 verifies the list signature when a client accesses to the corresponding DocSpace and verifies the document signature when a client accesses to the corresponding document object. If SF.INT.1 fails in verification of these digital signatures, 1) SF.INT.1 passes event information indicating the failure to SF.AUD.1 for recording the detected event, 2) SF.INT.1 sends an e-mail containing the event information to a configured e-mail address, and 3) if the event is detected during processing a client request, SF.INT.1 suppresses the requested operation and

returns an error or an exception to the client. (Correspondence: FDP_SDI.2.2)

The list signature verification error results in a failure in accessing the DocSpace and the document signature verification error results in a failure in accessing the document object (corresponding audit events are described in Table 34).

When document contents contained in document objects, which are stored within the internal hard-drives of the TCAB, are written out (exported) onto an off-line disc, SF.INT.1 generates document signatures for each exporting document object as same as described above, and stores them on the off-line disc with the document objects (with its security attributes and access logs). SF.INT.1 also creates a document list of exported document objects just as same as described above, generates a list signature and stores it with the list on the off-line disc. (Correspondence: FDP_ETC.2 (b))

When an off-line disc is mounted (that corresponds to the first connection to the corresponding DocSpace by a user) on the TCAB, SF.INT.1 verifies a document list stored on the off-line disc by using a list signature (stored on the off-line disc). When a document object, which is stored on an off-line disc, is accessed, SF.INT.1 verifies the document object by using its document signature and a corresponding entry of the document list stored on the disc. If the verification is succeeded, SF.INT.1 imports the document object (with its security attributes and access logs), and SF.ACC.1 uses the security attributes for access control. (Correspondence: FDP_ITC.2 (b))

The list signature verification error results in a failure in accessing the DocSpace and the document signature verification error results in a failure in accessing the document object (corresponding audit events are described in Table 34).

By verifying those signatures, SF.INT.1 ensures that the document objects (including its security attributes and access logs), the document list, and signatures are stored by the TCAB itself, by a distinct TCAB, or by a distinct TCABX1, or a distinct TCABW1, and are not modified at all. Therefore, SF.ACC.1 uses the security attributes and the document list just as are without further interpretation, SF.AUD.1 uses the access logs just as are without further interpretation, and SF.INT.1, like described above, uses the digital signatures just as are without further interpretation. (Correspondence: FPT_TDC.1 (b))

SF.INT.1 uses cryptographic module for generating and verifying digital signatures described above.

REMARKS:

The cryptographic module has to be configured during installation/set-up of TCAB to use cryptographic algorithms listed in Table 28. (Correspondence: FCS_COP.1 (b))

SF.INT.2 System integrity protection

SF.INT.2 generates digital signatures for the following information: system access history, system timer configuration history, user account management data, system configuration data, and TCAB executables. Those

digital signatures, called system signatures, are stored on System Data Partition that is a part of TCAB-Kernel and is protected by hardware protection and login restriction of the underlying operating system. (Correspondence: FPT_ITT.1, FAU_STG.1)

During initial start-up, SF.INT.2 verifies the system signatures to detect unauthorized modifications performed on the information described above. If SF.INT.2 fails in the verification, 1) SF.INT.2 passes event information indicating the failure to SF.AUD.1 for recording the detected event, 2) SF.INT.2 sends an e-mail containing the event information to a configured e-mail address, and 3) SF.INT.2 terminates the TCAB itself. (Correspondence: FPT_ITT.3, FAU_STG.1)

A failure of the system signature verification during the initial start-up appears as a failure of the initial start-up, therefore, the system signature verification failure event is recorded as start-up failure (in Table 34).

The system access history can be moved onto external media. When the system access history is moved onto external media, SF.INT.2 generates a digital signature of the moved system access history and records it on the external media. The system access history on the external media is out of control of the TCAB. (Correspondence: FPT_ITT.1)

SF.INT.2 uses cryptographic module for generating and verifying digital signatures described above.

SF.INT.2 protects the TSF data including system access history, system timer configuration history, user account management data, system configuration data, and TCAB executables. The protected data is stored on the System Program Partition and the System Data Partition. The digital signatures protecting these data are also stored on the System Data Partition. On the other hand, SF.ACC.1 stores document objects only on the User Data Partition and off-line disc. By separating the user data area and the system execution area, the TSF's execution is not interfered nor tampered. (Correspondence: FPT_SEP.1)

REMARKS:

The cryptographic module has to be configured during installation/set-up of TCAB to use cryptographic algorithms listed in Table 28. (Correspondence: FCS_COP.1 (b))

The login restriction of the underlying operating system has to be configured properly so that only TCAB-OS-Administrator is able to login. (Correspondence: FIA_UID.1 (b), FIA_UAU.1 (b))

6.1.5 Audit Function

SF.AUD.1 Auditing function

SF.AUD.1 generates an audit record on detecting an event specified in Table 34, Table 35, and Table 36. (Correspondence: FAU_GEN.1, FAU_GEN.2)

SF.AUD.1 checks disk capacity of System Data Partition before recording system access history and system timer configuration history. If the capacity is in the warning range configured during the installation/set-up procedure and it is the first time after a start-up of the TCAB, SF.AUD.1 sends an e-mail containing the

information about the detected event to a configured e-mail address. (Correspondence: FAU_STG.3 (a))

Additionally, if the capacity exceeds the maximum level, which is configured during the installation/set-up procedure, and it is the first time after a start-up of the TCAB, SF.AUD.1 sends an e-mail containing the information about the detected event to a configured e-mail address and rejects requests from clients with a role other than TCAB-Administrator or TCAB-Auditor. (Correspondence: FAU_STG.3 (b))

If the capacity of the System Data Partition is full, SF.AUD.1 shuts down the TCAB. In such a case, only TCAB-Customer-Engineer can perform recovery procedures without using the TOE. (Correspondence: FAU_STG.4)

The TOE acquires time stamps from the underlying operating system indirectly via the JVM. The underlying operating system is properly maintained by trustworthy persons as defined in Table 4; therefore the time stamps acquired from the operating system are reliable. The time stamps are used in audit data and used for checking retention period of original documents. (Correspondence: FPT_STM.1)

SF.AUD.1 stores the TSF data including system access history, system timer configuration history on the System Data Partition. On the other hand, SF.ACC.1 stores document objects only on the User Data Partition and off-line disc. By separating the user data area and the system execution area, the TSF's execution is not interfered nor tampered. (Correspondence: FPT_SEP.1)

Table 34 Events recorded as system access history

Event	Description
Start-up of the TOE	On start-up of the TOE, the result of the start-up procedure shall be recorded. The start-up procedure includes integrity check of TSF data. The integrity check success/failure results in a success/failure of the start-up. Corresponds to FAU_GEN.1 and FPT_ITT.3.
Shutdown of the TOE	On shutting down of the TOE, the TOE shall protect TSF data from undetected modifications. Corresponds to FPT_ITT.3.
Login authentication	Corresponds to FIA_AFL.1 (a1), (a2).
Changing password	Corresponds to FIA_SOS.1 and FMT_MTD.1 (a).
User account registration	Corresponds to FMT_MTD.1 (a).
User account un-registration	Corresponds to FMT_MTD.1 (a).
User account de-activation	Corresponds to FMT_MTD.1 (a).
User account re-activation	Corresponds to FMT_MTD.1 (a).
System timer configuration	Corresponds to FMT_MTD.1 (d).
Viewing system timer configuration history	Corresponds to FAU_SAR.1.
Integrity check of document list	On the first access to a DocSpace of the TOE, integrity check shall be performed and the result shall be recorded. The integrity check success/failure results in a success/failure of accessing the DocSpace. Corresponds to FDP_SDI.2 and FDP_ITC.2 (b).

Event	Description
Integrity check of document	On document object access, integrity check shall be performed and the result shall be recorded. The document object access includes creation, revision, read, duplication, deletion, inter-TCAB transfer, write out to off-line disc, viewing attributes, and viewing access logs of document object. The integrity check success/failure results in a success/failure of accessing the document object. Corresponds to FDP_SDI.2 and FDP_ITC.2 (b).
Creation of document	Corresponds to FDP_ACF.1.
Revision of document	Corresponds to FDP_ACF.1.
Read of document	Corresponds to FDP_ACF.1.
Duplication of document	Corresponds to FDP_ACF.1.
Deletion of document	Corresponds to FDP_ACF.1.
Inter-TCAB document transfer	Corresponds to FTP_ITC.1 (a1), FDP_ETC.2 (a) and FDP_ACF.1.
Write out documents onto off-line disc	Corresponds to FDP_ACF.1 and FDP_ETC.2 (b)
Viewing document attributes	Corresponds to FDP_ACF.1.
Viewing document access logs	Corresponds to FDP_ACF.1 and FAU_SAR.1.
Internal procedures for Inter-TCAB transfer	Corresponds to FDP_ACF.1 and FDP_ITC.2 (a).
Acquisition of document list	Corresponds to FDP_ACF.1.
Changing document type	Corresponds to FMT_MSA.1 (a).
Lengthen retention period of document	Corresponds to FMT_MSA.1 (a).
Viewing system access history	Corresponds to FAU_SAR.1
Move system access history onto external media	Corresponds to FMT_MTD.1 (c).
Creation of backup	Corresponds to FMT_MTD.1 (e).
Supplements: The system access history shall be recorded on System Data Partition of the TOE working machine. For each event, the event occurrence time information, the event occurrence identification number, the event type (e.g., method name), client information (if applicable), and the result (success/failure) shall be recorded. The time information consists of a date/time and a timer-identifier. The timer-identifier indicates that how many times the system timer was configured. The client information consists of an account name, an IP address of the client machine.	

Table 35 Events recorded as document access logs

Event	Description
Integrity check of document	On document object access, integrity check shall be performed and the result shall be recorded. The document object access includes creation, revision, read, duplication, deletion, inter-TCAB transfer, write out to off-line disc, viewing attributes, and viewing access logs of document object. The integrity check success/failure results in a success/failure of accessing the document object. Corresponds to FDP_SDI.2 and FDP_ITC.2 (b).
Creation of document	Corresponds to FDP_ACF.1.
Revision of document	Corresponds to FDP_ACF.1.
Read of document	Corresponds to FDP_ACF.1.
Duplication of document	Corresponds to FDP_ACF.1.
Deletion of document	Corresponds to FDP_ACF.1.
Inter-TCAB document transfer	Corresponds to FTP_ITC.1 (a1), FDP_ETC.2 (a) and FDP_ACF.1.
Write out documents onto off-line disc	Corresponds to FDP_ACF.1 and FDP_ETC.2 (b)

Event	Description
Viewing document attributes	Corresponds to FDP_ACF.1.
Viewing document access logs	Corresponds to FDP_ACF.1 and FAU_SAR.1.
Internal procedures for Inter-TCAB transfer	Corresponds to FDP_ACF.1 and FDP_ITC.2 (a).
Changing document type	Corresponds to FMT_MSA.1 (a).
Lengthen retention period of document	Corresponds to FMT_MSA.1 (a).
Supplements: The document access logs shall be recorded on User Data Partition of the TOE working machine in conjunction with the corresponding document object. The document access logs shall be recorded only for the document objects stored on the User Data Partition. For each event, the event occurrence time information, the event occurrence identification number, the event type (e.g., method name), client information, and the result (success/failure) shall be recorded. The time information consists of a date/time and a timer-identifier. The timer-identifier indicates that how many times the system timer was configured. The client information consists of an account name, an IP address of the client machine.	

Table 36 Events recorded as system timer configuration history

Event	Description
System timer configuration	Corresponds to FMT_MTD.1 (d).
Supplements: The system timer configuration history shall be recorded on System Data Partition of the TOE working machine. For each event, the current time information, the configured new time information, and client information shall be recorded. The time information consists of a date/time and a timer-identifier. The timer-identifier indicates that how many times the system timer was configured (i.e., the configured new time information contains an incremented timer-identifier). The client information consists of an account name, an IP address of the client machine.	

SF.AUD.2 Audit management

SF.AUD.2 provides capability of read-access to the system access history and the system timer configuration history for TCAB-User, TCAB-Administrator, and TCAB-Auditor.

The system access history, document access logs, and system timer configuration history are described in XML (i.e. text format); therefore, the client can easily interpret them. (Correspondence: FAU_SAR.1)

REMARKS:

SF.ACC.1 controls read-access to the document access logs for each document object.

TCAB sends e-mail messages on detecting severe events, such as continuous authentication failures, documents modifications and system corruptions (integrity errors on the TSF data). To send e-mail messages, an e-mail address and an IP-address (or a host name) of a SMTP server have to be configured. SF.AUD.2 provides capability to manage those configurations only for TCAB-Administrator. (Correspondence: FMT_MTD.1 (b))

The system access history recorded on System Data Partition by SF.AUD.1. SF.AUD.2 provides capability of

moving the system access history onto external media only for TCAB-Auditor. (Correspondence: FMT_MTD.1 (c))

TCAB acquires time stamps from the underlying operating system indirectly via the underlying JVM. The time stamps are used in audit data and used for checking retention period of original document objects. SF.AUD.2 provides capability of changing the system timer configuration only for TCAB-Administrator. If a TCAB-Administrator changes the system timer configuration, SF.AUD.2 changes the system timer of the operating system and passes the information about the event to SF.AUD.1 for recording system timer configuration history. (Correspondence: FMT_MTD.1 (d))

By restricting the ability to change the system timer configuration only to TCAB-Administrator, the time stamps acquired from the underlying operating system become reliable. (Correspondence: FPT_STM.1)

6.1.6 Probabilistic or Permutational Mechanisms

The TOE contains security function SF.I&A.1 that is realized by a probabilistic or permutational mechanism (account name/password based authentication). The strength of function level for the function is **SOF-Basic**.

6.2 Assurance Measures

TCAB provides assurance measures shown in Table 37. Assurance components listed in the table correspond to the EAL3 assurance package.

Table 37 Assurance measures

Assurance Component (EAL3)		Assurance Measure (TCAB document)
ACM_CAP.3	Authorisation controls	Configuration Management Manual for TrustyCabinet UX V1 Version 1.1
ACM_SCP.1	TOE CM coverage	Configuration Management Manual for TrustyCabinet UX V1 Version 1.1
ADO_DEL.1	Delivery procedures	Delivery Procedures for TrustyCabinet UX V1 Version 1.1
ADO_IGS.1	Installation, generation, and start-up procedures	Installation/Maintenance Manual for TrustyCabinet UX V1 Version 2.1 (en)
ADV_FSP.1	Informal functional specification	Security Functional Specification for TrustyCabinet UX V1 Version 1.3
ADV_HLD.2	Security enforcing high-level design	Security High Level Design for TrustyCabinet UX V1 Version 1.2
ADV_RCR.1	Informal correspondence demonstration	Correspondence Demonstration for TrustyCabinet UX V1 Version 1.3
AGD_ADM.1	Administrator guidance	Administration Manual for TrustyCabinet UX V1 Version 2.4 (en)
AGD_USR.1	User guidance	System Development Manual for TrustyCabinet UX V1 Version 2.2 (en)
ALC_DVS.1	Identification of security measures	Development Security Plan for TrustyCabinet UX V1 Version 1.21

Assurance Component (EAL3)		Assurance Measure (TCAB document)
ATE_COV.2	Analysis of coverage	Security Tests for TrustyCabinet UX V1 Version 1.2
ATE_DPT.1	Testing: high-level design	Security Tests for TrustyCabinet UX V1 Version 1.2
ATE_FUN.1	Functional testing	Security Tests for TrustyCabinet UX V1 Version 1.2
ATE_IND.2	Independent testing – sample	TrustyCabinet UX V1 TOE TrustyCabinet UX V1 Test Tools
AVA_MSU.1	Examination of guidance	Administration Manual for TrustyCabinet UX V1 Version 2.4 (en) System Development Manual for TrustyCabinet UX V1 Version 2.2 (en) Installation/Maintenance Manual for TrustyCabinet UX V1 Version 2.1 (en)
AVA_SOF.1	Strength of TOE security function evaluation	Strength of Function Analysis for TrustyCabinet UX V1 Version 1.1
AVA_VLA.1	Developer vulnerability analysis	Vulnerability Analysis for TrustyCabinet UX V1 Version 1.2

7 Rationale

7.1 Security Objectives Rationale

7.1.1 Rationale for Security Objectives Supporting Assumptions

In this section, the rationale for security objectives supporting assumptions is provided.

The following rationale statements show that the each assumption is supported straightforwardly by one environmental security objective.

1.	A.PLATFORM	The platform of the TOE is trusted.
		The platform of TOE is trusted and works correctly and in the expected way (the platform consists of hardware modules listed in Table 3 and software modules listed in Table 2). No viruses and Trojan horses are installed on the machine. The secure communication module is configured to allow usage of high-grade cryptography only. Cryptographic keys used for secure communication and digital signing are generated and updated by a TCAB-Customer-Engineer in a secure manner. The cryptographic keys are destructed on updating them with new keys. The TCAB-Customer-Engineer ensures that the keys are strong enough for their purpose.
	Rationale: OE.PLATFORM directly and straightforwardly supports this assumption.	

2.	A.DEDICATED-MACHINE	The TOE works on a dedicated machine.
		The machine on which the TOE works is used only for the TOE. No components other than that ones listed in Table 2 and the TOE itself are installed on the machine. The machine is configured to terminate all network services other than the services provided by the TOE.
	Rationale: OE.DEDICATED-MACHINE directly and straightforwardly supports this assumption.	

3.	A.PRIVATE-NETWORK	The TOE is located on a private network.
		The TOE does not directly connect to a public network. The TOE is located on a network that is properly protected by a firewall, or on a network that has no connections to a public network. Therefore, it is not assumed that unknown malicious users attack directly to the TOE in a sophisticated manner.
	Rationale: OE.PRIVATE-NETWORK directly and straightforwardly supports this assumption.	

4.	A.PERSONNEL	Proper persons are assigned to administrators and they are trained.
		For administration and maintenance of the TOE, administrators are properly assigned to trustworthy persons as defined in Table 4. The assigned administrators and users of the TOE who have access rights for the TOE maintain their authentication data used for accessing the TOE properly.
	Rationale: OE.TRAIN directly and straightforwardly supports this assumption.	

7.1.2 Rationale for Security Objectives Addressing Threats

In this section, rationale for security objective addressing security threats is provided.

The following rationale statements show that each security threat is addressed by at least one security objective.

1.	T.UNAUTH-ACCESS	Unknown users perform unauthorized access to the TOE.
		Unknown users (users without a TCAB user account) logically perform unauthorized access to the TOE and therefore to the documents stored inside the TOE. Unknown users may use the TOE security functions without identification and authentication. Unknown users or unauthorized users may perform password attacks to impersonate an authorized client.
	Rationale: O.IDENTIFY-AUTHENTICATE directly and straightforwardly addresses this threat. O.MANAGE-SYSTEM supports O.IDENTIFY-AUTHENTICATE by providing user account management capability only for authorized privileged user.	

2.	T.NETWORK-ATTACK	Network communications are attacked.
		Communications between the TOE and a client, or between the TOE and a distinct TCAB, are modified or eavesdropped by malicious users. Malicious users may perform impersonation or man-in-the-middle attacks. Therefore malicious users may access to documents and secrets (e.g., authentication data) on the network.
	Rationale: O.PROTECT-NETWORK directly and straightforwardly addresses this threat. OIE.SUPPORT-CRYPTO supports O.PROTECT-NETWORK by providing secure communication capability.	

3.	T.DELETE-DOC	A document, which has to be retained, is deleted via the TSF.
		Regardless of intentionally or un-intentionally, a stored document, which has to be retained, is deleted via the TSF. General write protection and access controlled file system are not enough for addressing this threat. For example, someone who has a right to delete a document may delete the important document that has to be stored during the retention period from a legal point of view. Someone may impersonate a client who has a right to delete, and may delete the important document.
	Rationale: O.DELETE-CONTROL directly and straightforwardly addresses this threat. O.REVISE-CONTROL addresses an aspect of deletion of previous document versions by preventing overwriting and deleting previous document versions.	

4.	T.OVERWRITE-DOC	A document is modified without traces via the TSF.
		Regardless of intentionally or un-intentionally, a stored document is modified or overwritten without traces (access logs and revision history) via the TSF. General write protection and access controlled file system are not enough for addressing this threat. For example, someone who has a right to modify a document can easily modify/overwrite the document without traces. Someone may impersonate a client who has a right to modify, and may modify/overwrite the important document without traces.
	Rationale: O.REVISE-CONTROL directly and straightforwardly addresses this threat. O.DELETE-CONTROL supports O.REVISE-CONTROL by not providing capability of deletion of particular document versions.	

5.	T.MODIFY-DOC-DIRECTLY	A document is modified, deleted, altered or forged directly.
		A stored document is undetectedly modified, deleted, or forged without using the TOE security functions. An Off-line disc storing documents may be thrown away or may be altered with another disc. For example, after creating a copy of an off-line disc storing documents, an authorized client may revise documents on the off-line disc using the TOE. Later, someone may alter the new disc with the old copied disc. Simple digital signature protection is not enough for addressing this threat. For example, someone may easily alter a document with another digitally signed document.
	Rationale: O.LOGICAL-PACKAGE directly and straightforwardly addresses this threat. O.LOGICAL-PACKAGE ensures that the TSF can protect documents from alteration of them with other digitally signed documents by providing capability of creating a integrity-protected list containing digital signatures of each document. O.REVISE-CONTROL explicitly denies revising documents on off-line discs to eliminate inconsistencies between an original off-line disc and a copied off-line disc. OIE.SUPPORT-CRYPTO supports O.LOGICAL-PACKAGE by providing cryptographic operation capability. OE.MANAGE-MEDIA properly manages direct accesses to the primary storage and the off-line discs to minimize this threat.	

6.	T.CONFUSE-ORIGINAL	Authorized users confuse an original with its duplicates.
		An authorized client duplicates an original document using the TSF, and other clients confuse the duplicates with the original. This leads to other threats, for example, authorized clients may delete the original, which has to be stored during retention period, because they cannot distinguish the original from its duplicates. Additionally, authorized clients may revise duplicates and may confuse the revised duplicates with the original. It leads inconsistencies of document revision controls.
	Rationale: O.DUPLICATE-CONTROL directly and straightforwardly addresses this threat. O.DELETE-CONTROL prevents deleting an original document that is in its retention period. O.REVISE-CONTROL in conjunction with O.DUPLICATE-CONTROL addresses an aspect of this threat by eliminating inconsistencies of document revision control.	

7.	T.CORRUPT-SYSTEM	The TOE system is corrupted directly by malicious users.
		Malicious users corrupt the TOE system directly, not via the TSF. Malicious OS users may modify system configurations or install programs, and it leads to the future insecurities. Malicious users may modify the TSF data stored within the TOE. Malicious users may modify the backup data directly, and it leads to other insecurities such as insecure state of the TOE caused by a restoration. Malicious users may modify audit data written-out to external media.
	Rationale: O.PROTECT-SYSTEM directly and straightforwardly addresses this threat concerning security management data and audit data stored by the system. OIE.SUPPORT-CRYPTO supports O.PROTECT-SYSTEM by providing cryptographic operation capability. OE.PHYSICAL-PACKAGE and OIE.OS-LOGIN prevent direct access to the system internals, to minimize possibilities of the threat occurrence concerning the TSF data stored within the system. OE.MANAGE-MEDIA minimizes possibilities of the threat occurrence concerning backup media and audit data on external media.	

7.1.3 Rationale for Security Objectives Supporting Policies

In this section, rationale for security objective supporting organizational security policies is provided.

The following rationale statements show that each policy is supported by at least one security objective.

1.	P.MANAGER	Manager responsible for the document
		To clarify the responsibility and privilege of document management, the organization shall specify a manager who is responsible for the electronic document management.
	Rationale: OE.MANAGER directly and straightforwardly supports this policy. O.MANAGE-SYSTEM supports OE.MANAGER by providing system management capability only for authorized and privileged user.	

2.	P.IDENTIFY-AUTHENTICATE	Identification and authentication
		Electronic Document Management and Storage System (EDMSS) shall identify and authenticate users accessing the system.
	Rationale: O.IDENTIFY-AUTHENTICATE directly and straightforwardly supports this policy. O.MANAGE-SYSTEM supports O.IDENTIFY-AUTHENTICATE by providing user account management capability only for authorized privileged user.	

3.	P.MANAGE-MEDIA	Management of electronic media
		The organization shall specify storage space for electronic media. The electronic media shall be maintained securely (e.g., in the locked shelves). The organization shall record check-out/check-in history of the electronic media.
	Rationale: OE.MANAGE-MEDIA directly and straightforwardly supports this policy.	

4.	P.AUDIT	Audit
		System access audit EDMSS shall record accesses. **Document access log** EDMSS shall record access logs of the stored documents. The logs shall contain information about storage date, access date, revision date, deletion date, and the accessing user. The logs shall be maintained securely for a specified period. **System timer setting** System timer configuration history shall be recorded and the history shall be maintained securely for a specified period. **Audit duty** The EDMSS shall be audited properly.
	Rationale: O.AUDIT directly and straightforwardly supports system access audit, document access log, and system timer setting aspects of this policy. OE.TRAIN directly supports audit duty aspect of this policy. O.MANAGE-SYSTEM supports this policy by ensuring that only TCAB-Auditor can manage audit data (e.g. export them to external media).	

5.	P.ACCESS-CONTROL	Access control
		Accesses to the documents stored in EDMSS shall be controlled properly, based on the document type.

	Rationale: The combination of access control objectives; O.REVISE-CONTROL, O.DUPLICATE-CONTROL, and O.DELETE-CONTROL, provides capability of access control based on document attributes and user attributes to directly support this policy. OE.ACCESS-CONTROL is a supplement to the access control capability above, and provides more detailed access control capability to support this policy, if it is required. O.MANAGE-SYSTEM supports this policy concerning user account management that only authorized privileged user can manage user accounts.	

6.	P.MANAGE-REVISION	Document revision management
		Revision history The revision history, including deleted contents and appended contents, of documents shall be maintained. The revision history shall be maintained securely for a specified period. **Document revision management** When revise a document, the original document should be maintained for a specified period, if it is required.
	Rationale: O.REVISE-CONTROL directly and straightforwardly supports this policy.	

7.	P.PROTECT-CONTENTS	Contents protection
		Contents encryption To prevent and to prepare for steal, disclosure, and modification, the stored documents should be encrypted, if it is required. **Contents signing** The stored documents should be protected with a digital signature having functionality of detecting modifications, if it is required.
	Rationale: O.LOGICAL-PACKAGE directly supports contents signing aspect of this policy concerning integrity protection of the stored documents within the system. OIE.SUPPORT-CRYPTO supports O.LOGICAL-PACKAGE by providing cryptographic operation capability. OE.PROTECT-CONTENTS directly and straightforwardly supports this policy concerning contents encryption and additional signing performed by a user or a business processing system, if it is required.	

8.	P.BACKUP	Backup
		Document backup The stored documents shall be backed-up at regular intervals. The backup data shall be maintained properly. **Management of media** Media with stored documents and backup media shall be checked, that these media are properly maintained, at regular intervals. **Program backup** The programs shall be backed-up, and the backup shall be properly maintained.
	Rationale: OE.TRAIN supports duty related aspects of this policy. OE.MANAGE-MEDIA supports media management aspects of this policy. O.MANAGE-SYSTEM supports backup related aspects of this policy by providing backup capability to authorized privileged users.	

9.	P.VIRUS-CHECK	Virus check
		Documents acquired from outside the organization shall be virus-checked before using them.
	Rationale: OE.VIRUS-CHECK directly and straightforwardly supports this policy.	

10.	P.READABILITY	Readability
		The organization shall maintain systems for visualizing electronic documents. The systems include such as computers, programs, networks, display monitors, and printers. When the documents are required to view, the organization shall visualize the documents on a monitor or papers.
	Rationale: OE.READABILITY directly and straightforwardly supports this policy.	

11.	P.MAINTAIN-SYSTEM	System maintenance
		EDMSS shall be maintained, checked, and updated systematically. Documents shall be protected during the maintenance.
	Rationale: OE.TRAIN supports the systematic update related aspect of this policy. OE.MANAGER supports the protection during the maintenance related aspect of this policy.	

12.	P.POWER-SUPPLY	Power supply
		To prevent losses and destructions of documents caused by power supply termination, Uninterruptible Power Supplies (UPS), or other measures, shall be applied to the systems.
	Rationale: OE.PLATFORM directly and straightforwardly supports this policy.	

7.1.4 Summary of Security Objectives Rationale

In Table 38, cross-references the threats, policies, and assumptions against the security objectives are shown.

According to this table, each security objective covers at least one threat, policy, or assumption, therefore, each security objective is necessary. Additionally, each threat, policy, and assumption is covered by at least one security objective, as shown in Section from 7.1.1 to 7.1.3 and Table 38, therefore, the security objectives are sufficient to meet the security needs. Each security objective for the TOE is traced back to threats or policies only and is not traced back to assumptions.

Table 38 Mapping of security environment and security objectives

	O.IDENTIFY-AUTHENTICATE	O.PROTECT-NETWORK	O.LOGICAL-PACKAGE	O.REVISE-CONTROL	O.DUPLICATE-CONTROL	O.DELETE-CONTROL	O.AUDIT	O.PROTECT-SYSTEM	O.MANAGE-SYSTEM	OIE.SUPPORT-CRYPTO	OIE.OS-LOGIN	OE.MANAGE-MEDIA	OE.TRAIN	OE.PHYSICAL-PACKAGE	OE.ACCESS-CONTROL	OE.PLATFORM	OE.DEDICATED-MACHINE	OE.PRIVATE-NETWORK	OE.MANAGER	OE.PROTECT-CONTENTS	OE.VIRUS-CHECK	OE.READABILITY
A.PLATFORM																X						
A.DEDICATED-MACHINE																	X					
A.PRIVATE-NETWORK																		X				
A.PERSONNEL													X									
T.UNAUTH-ACCESS	X								X													
T.NETWORK-ATTACK		X								X												
T.DELETE-DOC				X		X																
T.OVERWRITE-DOC				X		X																
T.MODIFY-DOC-DIRECTLY			X	X						X		X										
T.CONFUSE-ORIGINAL				X	X	X																
T.CORRUPT-SYSTEM								X		X	X	X		X								
P.MANAGER									X										X			
P.IDENTIFY-AUTHENTICATE	X								X													
P.MANAGE-MEDIA												X										
P.AUDIT							X		X				X									
P.ACCESS-CONTROL				X	X	X			X						X							
P.MANAGE-REVISION				X																		
P.PROTECT-CONTENTS			X							X										X		
P.BACKUP									X			X	X									
P.VIRUS-CHECK																					X	
P.READABILITY																						X
P.MAINTAIN-SYSTEM													X						X			
P.POWER-SUPPLY																X						

7.2 Rationale for Functional Requirements

In this section, rationale for functional requirements is provided.

The following rationale statements show that each security objective for the TOE is addressed by at least one security requirement. The justifications provided for each security functional requirement (SFR) component explicitly show that the component selections are appropriate.

<table>
<tr><td rowspan="4">1.</td><td rowspan="2">O.IDENTIFY-AUTHENTICATE</td><td>User identification and authentication</td></tr>
<tr><td>The TOE shall identify and authenticate clients accessing via the network.
The TOE shall reject authentication requests that may lead too many authentication failures.
The TOE shall only accept authentication secrets that are strong enough against attacks such as a dictionary attack.</td></tr>
<tr><td colspan="2">Requirements:
FIA_UID.2 (a)
FIA_UAU.2 (a)
FIA_UAU.5
FIA_SOS.1
FIA_AFL.1 (a1), (a2), (b)
FIA_ATD.1
FIA_USB.1

Justification:
These requirements ensure that the TSF can identify and authenticate users accessing via the network.
FIA_UID.2 (a) ensures that the users accessing via the network are identified before any TSF-mediated actions.
FIA_UAU.2 (a) ensures that the users accessing via the network are authenticated before any TSF-mediated actions.
FIA_UAU.5 ensures that the account name/password of the account having a role TCAB-System does not become an easily exploitable one.
FIA_SOS.1 ensures that the secrets used in the TSF are properly strong against attacks.
FIA_AFL.1 (a1) is recording attacks, FIA_AFL.1 (a2) is delaying attackers, and FIA_AFL.1 (b) is notifying attacks to ensure that authentication failures are handled properly against attacks.
FIA_ATD.1 ensures that the TSF can distinguish one user from another for identification and can associate a role specified in FMT_SMR.1.
FIA_USB.1 ensures that the authenticated client is correctly bound to the client’s security attributes.</td></tr>
<tr><td colspan="2"><table>
<tr><th>Requirement</th><th>Dependency</th><th>Fulfilled by</th></tr>
<tr><td>FIA_UID.2 (a)</td><td>FIA_UAU.1</td><td>FIA_UAU.2 (a) that is hierarchical to FIA_UAU.1</td></tr>
<tr><td>FIA_UAU.2 (a)</td><td>FIA_UID.1</td><td>FIA_UID.2 (a) that is hierarchical to FIA_UAU.1</td></tr>
<tr><td>FIA_UAU.5</td><td>No CC defined dependency</td><td>FIA_UAU.5 depends on secure communication capability provided by components FTP_ITC.1 (b2) and FCS_COP.1 (a) required for OIE.SUPPORT-CRYPTO.</td></tr>
<tr><td>FIA_SOS.1</td><td>No CC defined dependency</td><td>-</td></tr>
<tr><td>FIA_AFL.1 (a1)</td><td>FIA_UAU.1</td><td>FIA_UAU.2 (a) that is hierarchical to FIA_UAU.1</td></tr>
<tr><td>FIA_AFL.1 (a2)</td><td>FIA_UAU.1</td><td>FIA_UAU.2 (a) that is hierarchical to FIA_UAU.1</td></tr>
<tr><td>FIA_AFL.1 (b)</td><td>FIA_UAU.1</td><td>FIA_UAU.2 (a) that is hierarchical to FIA_UAU.1</td></tr>
<tr><td>FIA_ATD.1</td><td>No CC defined dependency</td><td>-</td></tr>
<tr><td>FIA_USB.1</td><td>FIA_ATD.1</td><td>FIA_ATD.1</td></tr>
</table></td></tr>
</table>

<table>
<tr><td rowspan="2">2.</td><td rowspan="2">O.PROTECT-NETWORK</td><td>Network protection</td></tr>
<tr><td>The TOE shall protect network communications between the TOE and a remote trusted IT product (a client or a distinct TCAB) from un-detection of modification, eavesdropping and impersonation.</td></tr>
</table>

	Requirements: FTP_ITC.1 (a1) FTP_ITC.1 (a2) Justification: This requirement ensures that the TSF can protect network communications between the TOE and the remote trusted IT products properly. FTP_ITC.1 (a1) ensures that the communications initiated by the TSF are protected properly. FTP_ITC.1 (a2) ensures that the communications initiated by the remote trusted IT product are protected properly.	

Requirement	Dependency	Fulfilled by
FTP_ITC.1 (a1)	No CC defined dependency	FTP_ITC.1 (a1) depends on secure communication capability provided by components FTP_ITC.1 (b1) and FCS_COP.1 (a) required for OIE.SUPPORT-CRYPTO.
FTP_ITC.1 (a2)	No CC defined dependency	FTP_ITC.1 (a2) depends on secure communication capability provided by components FTP_ITC.1 (b2) and FCS_COP.1 (a) required for OIE.SUPPORT-CRYPTO.

3.	O.LOGICAL-PACKAGE	Logical packaging
		The TOE shall detect modification directly performed on documents stored under control of the TOE. (Documents stored on an off-line disc mounted on the system are under control of the TOE.) The TOE shall not recognize a forged document as an authentic document. The TOE shall protect documents with digital signatures. The TOE shall protect a list of these signatures by providing an additional digital signature for the list.
	Requirements: FDP_SDI.2 Justification: The requirement ensures that the TSF can detect modifications directly performed on documents stored in the TSC. FDP_SDI.2 ensures that the TSF can detect modifications directly performed on documents stored in the TSC, and the documents and document lists containing digital signatures of each document are protected with digital signatures.	

Requirement	Dependency	Fulfilled by
FDP_SDI.2	No CC defined dependency	FDP_SDI.2 depends on cryptographic operation capability provided by a component FCS_COP.1 (b) required for OIE.SUPPORT-CRYPTO.

4.	O.REVISE-CONTROL	Document revision control
		The TOE shall control revising documents. When revising an original document, the TOE shall store the revised document as a new version of the document, without overwriting or deleting any previous versions of the document. The TOE shall not provide capability to delete old versions of documents. The TOE shall not provide capability to revise duplicates to prevent inconsistencies between the duplicates and the original. The TOE shall provide capability to view old versions of each document. The TOE shall not revise documents stored on off-line discs.

Requirements:
FDP_ACC.2
FDP_ACF.1
FDP_ETC.2 (a), (b)
FDP_ITC.2 (a), (b)
FPT_TDC.1 (a), (b)
FMT_MSA.1 (a)
FMT_MSA.1 (c)

Justification:
These requirements ensure that the TSF can control revising documents properly.
FDP_ACC.2 ensures that access control is enforced on all operations between all subjects (users) and all objects (documents) including revising operations.

FDP_ACF.1 provides a version-up operation to ensure that the TSF stores revised document as a new version of the document when an original document is revised.
FDP_ACF.1 ensures that the TSF does not provide capability of overwriting any documents by specifying a dedicated explicitly deny rule.
FDP_ACF.1 ensures that the TSF does not provide capability of deleting old versions of documents by specifying a dedicated explicitly deny rule.
FDP_ACF.1 ensures that the TSF does not provide capability of revising duplicates by definition of access rules in Table 14 and Table 15.
FDP_ACF.1 ensures that the TSF provides capability of reading old versions of each document by allowing read document operation for authorized privileged users specified in Table 14 and Table 15.
FDP_ACF.1 ensures that the TSF does not provide capability of revising documents stored on off-line discs by not allowing such operation to any user as shown in Table 15.
FDP_ETC.2 (a), FDP_ITC.2 (a), and FPT_TDC.1 (a) ensure that the policy for revising documents is properly enforced on exported/imported documents via the network.
FDP_ETC.2 (b), FDP_ITC.2 (b), and FPT_TDC.1 (b) ensure that the policy for revising documents is properly enforced on exported/imported documents via off-line discs.
FMT_MSA.1 (a) ensures that the security attributes are properly managed for enforcing security function policy specified by FDP_ACC.2.
FMT_MSA.1 (c) ensures that document access logs (revision logs) can be viewed by proper clients.

Requirement	Dependency	Fulfilled by
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 that is hierarchical to FDP_ACC.1 FMT_MSA.3 that is a component required for O.DELETE-CONTROL.
FDP_ETC.2 (a)	FDP_ACC.1	FDP_ACC.2 that is hierarchical to FDP_ACC.1
FDP_ETC.2 (b)	FDP_ACC.1	FDP_ACC.2 that is hierarchical to FDP_ACC.1
FDP_ITC.2 (a)	FDP_ACC.1 FPT_TDC.1 FTP_ITC.1	FDP_ACC.2 that is hierarchical to FDP_ACC.1 FPT_TDC.1 (a) FTP_ITC.1 (a1) and (b1) that are components required for O.PROTECT-NETWORK and OIE.SUPPORT-CRYPTO
FDP_ITC.2 (b)	FDP_ACC.1 FPT_TDC.1 FTP_ITC.1 or FTP_TRP.1	FDP_ACC.2 that is hierarchical to FDP_ACC.1 FPT_TDC.1 (b) The source of the importation is an off-line disc mounted on the system, thus the source is unambiguously identified. Confidentiality of the security attributes to be imported is not required. Documents and the security attributes to be imported are integrity protected by a component FDP_SDI.2 required for O.LOGICAL-PACKAGE. Therefore, the dependencies on FTP_ITC.1 and FTP_TRP.1 are not necessary to be fulfilled.
FPT_TDC.1 (a)	No CC defined dependency	-
FPT_TDC.1 (b)	No CC defined dependency	-

	FMT_MSA.1 (c)	FDP_ACC.1 FMT_SMR.1	FDP_ACC.2 that is hierarchical to FDP_ACC.1 FMT_SMR.2 that is hierarchical to FMT_SMR.1 that is a component required for O.MANAGE-SYSTEM
	FMT_MSA.1 (a)	FDP_ACC.1 FMT_SMR.1	FDP_ACC.2 that is hierarchical to FDP_ACC.1 FMT_SMR.2 that is hierarchical to FMT_SMR.1 that is a component required for O.MANAGE-SYSTEM

5.	O.DUPLICATE-CONTROL	Document duplicate control
		The TOE shall control creating duplicates. The TOE shall distinguish an original document from its duplicates. The TOE shall provide information that it is recognizable for the clients whether a document is an original or a duplicate.

Requirements:
FDP_ACC.2
FDP_ACF.1
FDP_ETC.2 (a), (b)
FDP_ITC.2 (a), (b)
FPT_TDC.1 (a), (b)
FMT_MSA.1 (a)
FMT_MSA.1 (b)

Justification:
These requirements ensure that the TSF can control creating duplicates properly.
FDP_ACC.2 ensures that access control is enforced on all operations between all subjects (users) and all objects (documents) including duplicate operations.
Distinguishing duplicates from the original is realized by the security attribute document type, which is used in access control policy enforcement FDP_ACF.1.
FDP_ACF.1 ensures that authorized privileged users can view attributes of each document containing document type.
FDP_ETC.2 (a), FDP_ITC.2 (a), and FPT_TDC.1 (a) ensure that the policy for creating duplicates is properly enforced on exported/imported documents via the network.
FDP_ETC.2 (b), FDP_ITC.2 (b), and FPT_TDC.1 (b) ensure that the policy for creating duplicates is properly enforced on exported/imported documents via off-line discs.
FMT_MSA.1 (a) ensures that the security attributes are properly managed for enforcing security function policy specified by FDP_ACC.2.
FMT_MSA.1 (b) ensures that a client can recognize whether the document is an original or a duplicate by providing ability to view the document type to the client.

Requirement	Dependency	Fulfilled by
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 that is hierarchical to FDP_ACC.1 FMT_MSA.3 that is a component required for O.DELETE-CONTROL.
FDP_ETC.2 (a)	FDP_ACC.1	FDP_ACC.2 that is hierarchical to FDP_ACC.1
FDP_ETC.2 (b)	FDP_ACC.1	FDP_ACC.2 that is hierarchical to FDP_ACC.1
FDP_ITC.2 (a)	FDP_ACC.1 FPT_TDC.1 FTP_ITC.1	FDP_ACC.2 that is hierarchical to FDP_ACC.1 FPT_TDC.1 (a) FTP_ITC.1 (a1) and (b1) that are components required for O.PROTECT-NETWORK and OIE.SUPPORT-CRYPTO

	FDP_ITC.2 (b)	FDP_ACC.1 FPT_TDC.1 FTP_ITC.1 or FTP_TRP.1	FDP_ACC.2 that is hierarchical to FDP_ACC.1 FPT_TDC.1 (b) The source of the importation is an off-line disc mounted on the system, thus the source is unambiguously identified. Confidentiality of the security attributes to be imported is not required. Documents and the security attributes to be imported are integrity protected by a component FDP_SDI.2 required for O.LOGICAL-PACKAGE. Therefore, the dependencies on FTP_ITC.1 and FTP_TRP.1 are not necessary to be fulfilled.
	FPT_TDC.1 (a)	No CC defined dependency	-
	FPT_TDC.1 (b)	No CC defined dependency	-
	FMT_MSA.1 (a)	FDP_ACC.1 FMT_SMR.1	FDP_ACC.2 that is hierarchical to FDP_ACC.1 FMT_SMR.2 that is hierarchical to FMT_SMR.1 that is a component required for O.MANAGE-SYSTEM
	FMT_MSA.1 (b)	FDP_ACC.1 FMT_SMR.1	FDP_ACC.2 that is hierarchical to FDP_ACC.1 FMT_SMR.2 that is hierarchical to FMT_SMR.1 that is a component required for O.MANAGE-SYSTEM

6.	O.DELETE-CONTROL	Document delete control
		The TOE shall control deleting documents. The TOE shall not delete an original document during the specified retention period. The TOE may delete temporary documents and duplicates. The TOE may delete original documents that are out of the specified retention period. The TOE shall only provide capability to delete entire documents, not particular document versions. The TOE shall control retention period configuration so that the retention period can only be changed to a longer one.

Requirements:
FDP_ACC.2
FDP_ACF.1
FDP_ETC.2 (a), (b)
FDP_ITC.2 (a), (b)
FPT_TDC.1 (a), (b)
FMT_MSA.3
FMT_MSA.1 (a)

Justification:
These requirements ensure that the TSF can control deleting document properly.
FDP_ACC.2 ensures that access control is enforced on all operations between all subjects (users) and all objects (documents) including deletion operations.

FDP_ACF.1 ensures that the TSF does not provide capability of deleting an original document during the specified retention period by specifying dedicated explicitly deny rule.
FDP_ACF.1 ensures that the TSF does not provide capability of deleting old versions of documents by specifying a dedicated explicitly deny rule.
FMT_MSA.1 (a) supports the TSF to protect original documents from deletion by restricting the ability to change the specified document type (document type can only be changed from Temporary Document to Original Document).
As specified in FDP_ACF.1, the TSF provides capability of deleting temporary documents and duplicates.
As specified in FDP_ACF.1, the TSF provides capability of deleting original documents that are not in the specified retention period.
FMT_MSA.1 (a) ensures that the TSF restricts the ability to change the security attribute retention period to a longer one only.
FDP_ETC.2 (a), FDP_ITC.2 (a), and FPT_TDC.1 (a) ensure that the policy for deleting documents is properly enforced on exported/imported documents via the network.
FDP_ETC.2 (b), FDP_ITC.2 (b), and FPT_TDC.1 (b) ensure that the policy for deleting documents is properly enforced on exported/imported documents via off-line discs.
FMT_MSA.3 ensures that the security attributes are secure even if the client does not specify the initial value on document object creation by specifying the default value to be restrictive.
FMT_MSA.1 (a) ensures that the security attributes are properly managed for enforcing security function policy specified by FDP_ACC.2.

Requirement	Dependency	Fulfilled by
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 that is hierarchical to FDP_ACC.1 FMT_MSA.3 FDP_ACF.1 depends on FPT_STM.1, reliable time stamps, for checking whether the retention period is over or not. The component is required for O.AUDIT.
FDP_ETC.2 (a)	FDP_ACC.1	FDP_ACC.2 that is hierarchical to FDP_ACC.1
FDP_ETC.2 (b)	FDP_ACC.1	FDP_ACC.2 that is hierarchical to FDP_ACC.1
FDP_ITC.2 (a)	FDP_ACC.1 FPT_TDC.1 FTP_ITC.1	FDP_ACC.2 that is hierarchical to FDP_ACC.1 FPT_TDC.1 (a) FTP_ITC.1 (a1) and (b1) that are components required for O.PROTECT-NETWORK and OIE.SUPPORT-CRYPTO

	FDP_ITC.2 (b)	FDP_ACC.1 FPT_TDC.1 FTP_ITC.1 or FTP_TRP.1	FDP_ACC.2 that is hierarchical to FDP_ACC.1 FPT_TDC.1 (b) The source of the importation is an off-line disc mounted on the system, thus the source is unambiguously identified. Confidentiality of the security attributes to be imported is not required. Documents and the security attributes to be imported are integrity protected by a component FDP_SDI.2 required for O.LOGICAL-PACKAGE. Therefore, the dependencies on FTP_ITC.1 and FTP_TRP.1 are not necessary to be fulfilled.
	FPT_TDC.1 (a)	No CC defined dependency	-
	FPT_TDC.1 (b)	No CC defined dependency	-
	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 (a) FMT_SMR.2 that is hierarchical to FMT_SMR.1 that is a component required for O.MANAGE-SYSTEM
	FMT_MSA.1 (a)	FDP_ACC.1 FMT_SMR.1	FDP_ACC.2 that is hierarchical to FDP_ACC.1 FMT_SMR.2 that is hierarchical to FMT_SMR.1 that is a component required for O.MANAGE-SYSTEM

7.	O.AUDIT	Auditing
		The TOE shall record access history of the TOE. The TOE shall record document access logs. The document access logs shall contain information about storage date, access date, revision date, deletion date, and the accessing client. The TOE shall record system timer configuration history. The TOE shall provide capability to view the system timer configuration history. The TOE shall provide capability to view the recorded audit data for authorized clients.

Requirements:
FAU_GEN.1
FAU_GEN.2
FPT_STM.1
FAU_SAR.1
FAU_STG.1
FAU_STG.3 (a)
FAU_STG.3 (b)
FAU_STG.4

Justification:
These requirements ensure that the TSF can record audit data properly.
FAU_GEN.1 ensures that audit data including TOE access history, document access logs, and system timer configuration history, are properly recorded.
FAU_GEN.1 ensures that the TSF records access history of the TOE.
FAU_GEN.1 ensures that the TSF records document access logs.
FAU_GEN.1 in conjunction with FAU_GEN.2 ensures that the TSF records document access logs containing storage date, access date, revision date, deletion date, and the accessing user.
FAU_GEN.1 ensures that the TSF records system timer configuration history.
FPT_STM.1 ensures that reliable time stamps are provided for the TOE.
FAU_SAR.1 ensures that the TSF provides a capability to read system timer configuration history.
FAU_SAR.1 ensures that the TSF provides a capability to read all the recorded audit data for authorized privileged users.
FAU_STG.1 ensures that the TSF protects the recorded audit data to support FAU_SAR.1.
FAU_STG.3 (a) supports FAU_SAR.1 by providing capability to warn before audit trail exceeds a maximum level.
FAU_STG.3 (b) supports FAU_SAR.1 by providing capability to warn and reject requests before audit trail is full.
FAU_STG.4 supports FAU_SAR.1 by providing capability to prevent audit data loss.

Requirement	Dependency	Fulfilled by
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2 (a) that is a component required for O.IDENTIFY-AUTHENTICATE and is hierarchical to FIA_UID.1
FPT_STM.1	No CC defined dependency	-
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3 (a)	FAU_STG.1	FAU_STG.1
FAU_STG.3 (b)	FAU_STG.1	FAU_STG.1
FAU_STG.4	FAU_STG.1	FAU_STG.1

8.	O.PROTECT-SYSTEM	System protection
		The TOE shall protect itself by detecting unauthorized modification of the following data: security management data and audit data. The TOE shall detect modification of these data even if they are restored from backup data.

Requirements:
FPT_ITT.1
FPT_ITT.3
FPT_RVM.1
FPT_SEP.1
FMT_MOF.1

Justification:
These requirements ensure that the TSF can protect its TSF data by detecting un-authorized modifications of these including restored backup data.
These requirements also ensure that the TSF(s) are always functioning.
FPT_ITT.1 ensures that the TSF applies modification protection to its TSF data including security management data, audit data, and restored backup data.
FPT_ITT.3 ensures that the TSF can detect modifications of TSF data and takes actions when such modifications are detected.
FPT_RVM.1 ensures that the TSF(s) are always invoked from the clients.
FPT_SEP.1 ensures that the TSF(s) can work properly even if a client performs malicious actions (invocations) to the TOE.
FMT_MOF.1 ensures that the TSF(s) never be disabled nor modified.

Requirement	Dependency	Fulfilled by
FPT_ITT.1	No CC defined dependency	FPT_ITT.1 depends on cryptographic operation capability provided by a component FCS_COP.1 (b) (digital signature generation) required for OIE.SUPPORT-CRYPTO.
FPT_ITT.3	FPT_ITT.1	FPT_ITT.1 FPT_ITT.3 depends on cryptographic operation capability provided by a component FCS_COP.1 (b) (digital signature verification) required for OIE.SUPPORT-CRYPTO.
FPT_RVM.1	No CC defined dependency	-
FPT_SEP.1	No CC defined dependency	-
FMT_MOF.1	FMT_SMR.1	The requirement component specifies “no one” for the assignment; therefore, the role related dependency is not required be fulfilled.

9.	O.MANAGE-SYSTEM	System management
		The TOE shall provide capability to manage the TOE for authorized privileged users only. The TOE shall provide capability to backup the TOE and documents for authorized privileged users.

Requirements:
FMT_SMR.2
FMT_MTD.1 (a), (b), (c), (d), (e)
FDP_ACF.1

Justification:
These requirements ensure that authorized privileges users can manage the TSF properly.
FMT_SMR.2 ensures that the TSF can restrict privileges for each user by assigning a role for each user.
FMT_MTD.1 (a) ensures that only authorized privileged users can manage user accounts and attributes.
FMT_MTD.1 (b) ensures that only authorized privileged users can modify an e-mail address used for notification.
FMT_MTD.1 (c) ensures that only authorized privileged users can move audit data onto external media.
FMT_MTD.1 (d) ensures that only authorized privileged users can modify system timer configuration.
FMT_MTD.1 (e) ensures that only authorized privileged users can backup the TSF data.
FDP_ACF.1 ensures that only authorized privileged users can backup the documents.

Requirement	Dependency	Fulfilled by

	FMT_SMR.2	FIA_UID.1	FIA_UID.2 (a) that is a component required for O.IDENTIFY-AUTHENTICATE and is hierarchical to FIA_UID.1
	FMT_MTD.1(a)	FMT_SMR.1	FMT_SMR.2 that is hierarchical to FMT_SMR.1
	FMT_MTD.1(b)	FMT_SMR.1	FMT_SMR.2 that is hierarchical to FMT_SMR.1
	FMT_MTD.1(c)	FMT_SMR.1	FMT_SMR.2 that is hierarchical to FMT_SMR.1
	FMT_MTD.1(d)	FMT_SMR.1	FMT_SMR.2 that is hierarchical to FMT_SMR.1
	FMT_MTD.1(e)	FMT_SMR.1	FMT_SMR.2 that is hierarchical to FMT_SMR.1
	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 that is a component required for O.REVISE-CONTROL, O.DELETE-COTROL, O.DUPLICATE-CONTROL and is hierarchical to FDP_ACC.1 FMT_MSA.3 that is a component required for O.DELETE-CONTROL.

The following rationale statements show that each security objective for the IT environment is addressed by at least one security requirement. The justifications provided for each SFR component explicitly show that the component selections are appropriate.

1.	OIE.SUPPORT-CRYPTO	Cryptographic operation support	
		The cryptographic module shall provide capability of cryptographic operations for the TOE. The secure communication module shall provide capability of secure communication for the TOE.	
	Requirements: FTP_ITC.1 (b1) FTP_ITC.1 (b2) FCS_COP.1 (a) FCS_COP.1 (b) Justification: These requirements ensure that the other modules out of the TOE provide cryptographic operation capability and secure communication capability for the TOE. FTP_ITC.1 (b1) ensures that capability of secure communication is provided for the TOE on initiating the communication by the TOE. FTP_ITC.1 (b2) ensures that capability of secure communication is provided for the TOE on communication initiated by the remote trusted IT product. FCS_COP.1 (a) ensures that the TOE uses the strong enough algorithms and protocols for securing communication. FCS_COP.1 (b) ensures that the TOE uses the strong enough algorithms for digital signature generation and verification.		
	Requirement	Dependency	Fulfilled by
	FTP_ITC.1 (b1)	No CC defined dependency	-
	FTP_ITC.1 (b2)	No CC defined dependency	-
	FCS_COP.1 (a)	FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	As assumed in A.PLATFORM, cryptographic keys are generated and updated by a TCAB-Customer-Engineer in a secure manner. The cryptographic keys are destructed on updating them with new keys. The TCAB-Customer-Engineer ensures that the keys are strong enough for secure communication. Thus, all the dependencies defined by the CC are satisfied by secure operational procedures. Therefore, the dependencies are not necessary to be fulfilled.

	FCS_COP.1 (b)	FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	As assumed in A.PLATFORM, cryptographic keys are generated and updated by a TCAB-Customer-Engineer in a secure manner. The cryptographic keys are destructed on updating them with new keys. The TCAB-Customer-Engineer ensures that the keys are strong enough for digital signing. Thus, all the dependencies defined by the CC are satisfied by secure operational procedures. Therefore, the dependencies are not necessary to be fulfilled.

2.	OIE.OS-LOGIN	OS login control support The OS of the machine shall provide capability to control login for restricting direct access to the TOE.		
	Requirements: FIA_UID.1 (b) FIA_UAU.1 (b) Justification: These requirements ensure that the OS provides capability of controlling direct login access for the TOE. FIA_UID.1 ensures that the OS provides capability of identifying accessing user before any action except for language selection, desktop/console selection, login host selection, and login help. FIA_UAU.1 ensures that the OS provides capability of authenticating accessing user before any action except for language selection, desktop/console selection, login host selection, and login help.			
	Requirement	Dependency	Fulfilled by	
	FIA_UID.1 (b)	No CC defined dependency	-	
	FIA_UAU.1 (b)	FIA_UID.1	FIA_UID.1 (b)	

7.3 Rationale for Assurance Requirements

The TOE is used for systems, such as electronic government systems, that require high confidence in IT security functions. Therefore, a high assurance level is required for security design of the TOE.

As described in the assumptions, however, it is assumed that the TOE is used in a properly managed private network. Therefore, an attacker who attacks the TOE using vulnerabilities of the TOE is limited to an internal user. The internal user, however, cannot search for a potential vulnerability of the TOE because the TOE records the activities as logs. Thus, unlike Web servers for example, unknown malicious users cannot attack the TOE in a high-grade sophisticated way. Therefore, the EAL3 assurance package that provides assurance of high-level design by ADV_HLD.2 and ATE_DPT.1 is appropriate for the TOE.

Furthermore direct physical and logical access to the system is protected and limited to TCAB-Key-Owner and TCAB-OS-Administrator, respectively. These two roles always have to be realized by separate trusted individuals. Taking this into account, the only possible point to attack the TOE is the extremely limited interface, TCAB-Driver, i.e. the security functions themselves. The interface can be used only by invocating the API methods of the TCAB-Driver, and all the vulnerabilities of the API methods are obvious. For such a limited interface, appropriate tests via the interface provide enough assurance. Therefore, it is not required to perform

vulnerability analysis concerning exploitation of vulnerabilities and the choice of AVA_VLA.1 (included in EAL3 assurance package) is appropriate.

7.4 Rationale for Mutually Supportive Requirements

All the CC defined dependencies for security functional requirements are fulfilled except FDP_ITC.2 (b), FCS_COP.1 (a), and FCS_COP.1 (b), and justifications explaining why the dependencies are not fulfilled are provided for all of those requirements. Additionally, as described in Section 7.2, some security functional requirements depend on other requirements and such dependencies are also fulfilled.

The EAL3 assurance package is applied for the TOE, therefore, all the CC defined dependencies for security assurance requirements are fulfilled.

For the aspect of protection of the TSF itself, FPT_RVM.1, FPT_SEP.1, and FMT_MOF.1 are included. Furthermore, the TOE works on a trusted platform (OE.PLATFORM), the platform is dedicated to the TOE (OE.DEDICATED-MACHINE), and the TSF is protected from direct tampering by environmental security objectives OE.PHYSICAL-PACKAGE and OIE.OS-LOGIN. Therefore, the TOE environment fulfills the major part of the TSF protection aspect.

Taking these into account, all the security requirements are mutually supportive.

7.5 TOE Summary Specification Rationale

The TOE summary specification rationale is intended to show that the TOE security functions and assurance measures are suitable to meet the TOE security requirements.

7.5.1 Suitability of IT Security Functions Rationale

This section is intended to provide a demonstration that the TOE security functions are suitable to meet all security functional requirements for the TOE. Additionally, this section is intended to provide a demonstration that the combination of the TOE security functions work together so as to satisfy the TOE security functional requirements.

Table 39 Suitability of TOE security functions rationale

Security Functional Requirement		Fulfilled by Security Function(s)
Identification and authentication		
	FIA_UAU.2 (a)	SF.I&A.1: “Before allowing any other actions, SF.I&A.1 … authenticates the accessing user …”
	FIA_UID.2 (a)	SF.I&A.1: “Before allowing any other actions, SF.I&A.1 identifies … the accessing user …”

	FIA_UAU.5	SF.I&A.1: "… SF.I&A.1 identifies and authenticates the accessing user by account name and password." "If the accessing user has the role TCAB-System, SF.I&A.1 additionally authenticates the user using public key certificates … The public-key certificate based authentication is realized based on SSL protocol."
	FIA_SOS.1	SF.ACC.4 "The password shall satisfy a quality metric specified in Table 33." "… SF.ACC.4 verifies that the provided password meets the quality metric. If SF.ACC.4 failed in the verification, SF.ACC.4 suppresses the requested operation." Justification: Contents of Table 33 are the same as the authentication secret quality metric specified in FIA_SOS.1.1.
	FIA_AFL.1 (a1)	SF.I&A.1 "The authentication fails if a wrong account name/password combination is provided or if a de-activated or an un-registered account name is used." SF.I&A.2 "If SF.I&A.1 detected an authentication failure; including wrong account name and password combination and use of de-activated or un-registered account name, SF.I&A.2 records audit data …"
	FIA_AFL.1 (a2)	SF.I&A.1 "The authentication fails if a wrong account name/password combination is provided or if a de-activated or an un-registered account name is used." SF.I&A.2 "If SF.I&A.1 detected an authentication failure; including wrong account name and password combination and use of de-activated or un-registered account name, SF.I&A.2 … waits for 5 seconds before responding the authentication request. Additionally, SF.I&A.2 restricts simultaneous authentication processes up to 50 …"
	FIA_AFL.1 (b)	SF.I&A.2 "Additionally, SF.I&A.2 counts authentication failures and if 3 authentication failures are detected within 5 minutes, SF.I&A.2 sends an e-mail indicating that continuous authentication failures are detected to the configured notification address."
	FIA_ATD.1	SF.ACC.4 "SF.ACC.4 maintains 4 security attributes belonging to individual user account. The attributes are: account name, activated flag, registered flag, and role."
	FIA_USB.1	SF.I&A.1 "On success of the client authentication, the TOE creates an instance (Java RMI server instance) and binds the client information including the account name and role to the instance. The TOE returns the instance to the client as a remote reference to the instance."
Network protection		

	FTP_ITC.1 (a1)	SF.NET.1 "SF.NET.1 provides a communication channel between the TCAB and a client of the TCAB or a distinct TCAB by using secure communication module that provides communication channel … Communication data is encrypted/decrypted and integrity protected/verified during transmission." "For establishing the secure communication channel, SF.NET.1 sends authentication data to be verified by the client." "For Inter-TCAB document transfer function, SF.NET.1 … identifies and authenticates the communication target." Justification: As cited above, SF.NET.1 provides secure communication channel that protects communication data from undetected modification and disclosure, and sends authentication data to be verified. These functionalities are realized by secure communication module, which is out of the TOE. SF.NET.1 controls when and how the secure communication channel is applied. For establishing secure communication channel, client authentication provided by SF.I&A.1 is used in conjunction with SF.NET.1.
	FTP_ITC.1 (a2)	SF.NET.1 "SF.NET.1 provides a communication channel between the TCAB and a client of the TCAB or a distinct TCAB by using secure communication module that provides communication channel … Communication data is encrypted/decrypted and integrity protected/verified during transmission." "For establishing the secure communication channel, SF.NET.1 sends authentication data to be verified by the client." "For using functions provided by TCAB, SF.NET.1 allows an accessing client (including a distinct TCAB as a client) to initiate the secure communication channel." Justification: As cited above, SF.NET.1 provides secure communication channel that protects communication data from undetected modification and disclosure, and sends authentication data to be verified. These functionalities are realized by secure communication module, which is out of the TOE. SF.NET.1 controls when and how the secure communication channel is applied. For establishing secure communication channel, client authentication provided by SF.I&A.1 is used in conjunction with SF.NET.1.
Document protection		
	FDP_SDI.2	SF.INT.1 "SF.INT.1 generates a digital signature for each document object, including its security attributes …" "SF.INT.1 creates document lists … each list entry contains a document signature …" "SF.INT.1 verifies the list signature …" "SF.INT.1 … verifies the document signature …" "If SF.INT.1 fails in verification … SF.INT.1 passes event information indicating the failure to SF.AUD.1 for recording the detected event …" "If SF.INT.1 fails in verification … SF.INT.1 sends an e-mail containing the event information to a configured e-mail address …" "If SF.INT.1 fails in verification … SF.INT.1 suppresses the requested operation and returns an error or an exception to the client."
Document access control		
	FDP_ACC.2	SF.ACC.1 "SF.ACC.1 controls all operations between Java RMI server instances accessing on behalf of clients and document objects in the TCAB."
	FDP_ACF.1	

	FDP_ACF.1.1	SF.ACC.1 "SF.ACC.1 authorizes or denies accesses between the instance and document object based on document type, document location, retention period, and role bounded to the instance."
	FDP_ACF.1.2	SF.ACC.1 "The only allowed operations depending on role, document type, and document location are shown in Table 30 and Table 31." "SF.ACC.1 restricts the ability to backup whole of hard-drives of the TCAB to TCAB-Administrator. The backup data can include all data stored in the System Program Partition, System Data Partition, and User Data Partition." Justification: Table 30 is identical to Table 16 except for backup, and Table 31 is identical to Table 17 except for backup.
	FDP_ACF.1.3	SF.ACC.1 "… SF.ACC.1 allows acquiring the list of document objects by any authorized client …"
	FDP_ACF.1.4	SF.ACC.1 "… SF.ACC.1 … denies the following accesses: overwriting a document object, deleting an original document object that is in the retention period, and partially deleting a document object (e.g. deleting an individual version contained in a document object)."
FMT_MSA.3		SF.ACC.3 "SF.ACC.3 has a default security attribute only for document type. The default value is "Original Document." It is restrictive because the retention-period-based deletion control is performed for the document object. On document object creation, the client (TCAB-User is the only possible role for document object creation) can specify an alternative document type "Temporary Document" for the document object."
FMT_MSA.1 (a)		SF.ACC.3 "On document object creation, only TCAB-User can specify a document type …" "Only TCAB-User can change document type of a document object that has a document type of "Temporary Document" to "Original Document."" "On document object creation, only TCAB-User shall specify retention period of the document object." "Only TCAB-User can lengthen retention period of a document object."
FMT_MSA.1 (b)		SF.ACC.1 "SF.ACC.1 authorizes viewing document attributes, which include document type and retention period, of each document object for TCAB-User, TCAB-RO-User, and TCAB-Administrator."
FMT_MSA.1 (c)		SF.ACC.1 "SF.ACC.1 authorizes viewing document access logs of each document object for TCAB-User, TCAB-Administrator, and TCAB-Auditor."
FDP_ETC.2 (a)		
	FDP_ETC.2.1	SF.ACC.1 As shown in Table 30, the operation "Inter-TCAB transfer" is access controlled by SF.ACC.1
	FDP_ETC.2.2	SF.ACC.2 "SF.ACC.2 exports a document contents with its security attributes …"
	FDP_ETC.2.3	SF.ACC.2 "… SF.ACC.2 creates one data archive containing the document contents itself, its security attributes …" "SF.ACC.2 uses SF.NET.1 to protect communications used for transferring the data archive …"
	FDP_ETC.2.4	SF.ACC.2 "SF.ACC.2 exports a document contents with its security attributes via the network from a TOE to a distinct TCAB or a distinct TCABX1." "… The security attributes include a document type and a retention period …"
FDP_ETC.2 (b)		

		FDP_ETC.2.1	SF.ACC.1 As shown in Table 30, the operation “Move to off-line discs” is access controlled by SF.ACC.1.
		FDP_ETC.2.2	SF.INT.1 “SF.INT.1 … stores … with the document objects (with its security attributes …”
		FDP_ETC.2.3	SF.INT.1 “SF.INT.1 generates a digital signature for each document object, including its security attributes …” “SF.INT.1 generates document signatures for each exporting document … and stores them … with the document objects (with its security attributes …”
		FDP_ETC.2.4	SF.INT.1 “The security attributes include document type and retention period.” “In the document list, each list entry contains a document signature …” “When document contents … are written out onto an off-line disc, SF.INT.1 generates document signatures … and stores them on the off-line disc with the document objects (with its security attributes …” “SF.INT.1 also creates a document list … generates a list signature and stores it with the list on the off-line disc.”
	FDP_ITC.2 (a)		
		FDP_ITC.2.1	SF.ACC.1 As shown in Table 30, the operation “Internal procedure for Inter-TCAB transfer” is access controlled by SF.ACC.1.
		FDP_ITC.2.2	SF.ACC.2 “… SF.ACC.2 imports the document contents with the security attributes. SF.ACC.1 uses the security attributes for enforcing access control policy …”
		FDP_ITC.2.3	SF.ACC.2 “SF.ACC.2 receives one data archive that contains a document contents, its security attributes …” “SF.ACC.2 uses SF.NET.1 to protect communications used for receiving the data archive from the distinct TCAB …”
		FDP_ITC.2.4	SF.ACC.2 “… SF.ACC.2 ensures that … transferred document type, retention period, … can be used by SF.ACC.1 … without further interpretation.”
		FDP_ITC.2.5	SF.ACC.2 “SF.ACC.2 receives one data archive that contains a document contents, its security attributes, and its access logs via the network from a distinct TCAB, a distinct TCABX1, or a distinct TCABW1; and SF.ACC.2 imports the document contents with the security attributes.” “… The security attributes include a document type and a retention period …”
	FDP_ITC.2 (b)		
		FDP_ITC.2.1	SF.ACC.1 As shown in Table 31, documents on imported off-line discs are access controlled by SF.ACC.1.
		FDP_ITC.2.2	SF.INT.1 “… SF.INT.1 imports the document object (with its security attributes … and SF.ACC.1 uses the security attributes for access control.”
		FDP_ITC.2.3	SF.INT.1 “By verifying those signatures, SF.INT.1 ensures that the document objects (including its security attributes … are not modified at all.”
		FDP_ITC.2.4	SF.INT.1 “By verifying those signatures, SF.INT.1 ensures that the document objects (including its security attributes … are stored by the TCAB itself, by a distinct TCAB, or by a distinct TCABX1, or a distinct TCABW1 …

		FDP_ITC.2.5	SF.INT.1 "The security attributes include document type and retention period." "When an off-line disc is mounted on the TCAB, SF.INT.1 verifies a document list stored on the off-line disc by using a list signature …" "When a document, which is stored on an off-line disc, is accessed, SF.INT.1 verifies the document object by using its document signature …" "… SF.INT.1 imports the document object (with its security attributes …" "… SF.INT.1 … uses the digital signatures just as are …"
	FPT_TDC.1 (a)		SF.ACC.2 "… SF.ACC.2 ensures that the communicating entity is a distinct TCAB, a distinct TCABX1, or a distinct TCABW1; and the transferred document type, retention period, and access logs can be used … just as are without further interpretation."
	FPT_TDC.1 (b)		SF.INT.1 "… SF.INT.1 ensures that the document objects (including its security attributes and access logs), the document list, and signatures are stored by the TCAB itself, by a distinct TCAB, or by a distinct TCABX1, or a distinct TCABW1 …" "… the security attributes and the document list just as are without further interpretation …" "… the access logs just as are without further interpretation …" "… the digital signatures just as are without further interpretation …"
Audit			
	FAU_GEN.1		SF.AUD.1 "SF.AUD.1 generates an audit record on detecting an event specified in Table 34, Table 35, and Table 36." Justification: Table 34, Table 35, and Table 36 are identical to Table 19, Table 20, and Table 21 respectively. In Table 34, "Start-up of the TOE" is recorded on start-up of the TCAB (i.e. start-up of SF.AUD.1). In Table 34, "Shutdown of the TOE" is recorded on shutdown of the TCAB (i.e. shutdown of SF.AUD.1).
	FAU_GEN.2		SF.AUD.1 "… the event occurrence time information, … the event type … , the client information … , and the result (success/failure) shall be recorded …" (in Table 34 and Table 35) "Client information consists of an account name, …" (in Table 34 and Table 35) Justification: In the system timer configuration history (Table 36), results (success or failure) are not recorded, however, they are recorded as an event of "System timer configuration" in the system access history (in Table 34).
	FPT_STM.1		SF.AUD.1 "The TOE acquires time stamps from the underlying operating system … the time stamps acquired from the operating system are reliable." SF.AUD.2 "By restricting the ability to change the system timer configuration … the time stamps acquired from the underlying operating system become reliable." SF.ACC.1 "SF.ACC.1 acquires a time stamp from the underlying operating system …"

	FAU_SAR.1	SF.AUD.2 “SF.AUD.2 provides capability to read-access to the system access history and the system timer configuration history for … TCAB-Auditor. The system access history, document access logs, and system timer configuration history are described in XML … the client can easily interpret them.” SF.ACC.1 “SF.ACC.1 authorizes viewing document access logs of each document object for TCAB-User, TCAB-Administrator, and TCAB-Auditor.”
	FAU_STG.1	SF.INT.2 “SF.INT.2 generates digital signatures for … system access history, system timer configuration history …” “… SF.INT.2 verifies the system signatures to detect unauthorized modifications performed on the information described above.” SF.INT.1 “SF.INT.1 generates a digital signature (called a document signature) for each document, including … its access logs …” “SF.INT.1 … verifies the document signature …”
	FAU_STG.3 (a)	SF.AUD.1 “SF.AUD.1 checks disk capacity … If the capacity is in the warning range configured during the installation/set-up procedure … SF.AUD.1 sends an e-mail containing the information about the detected event to a configured e-mail address.”
	FAU_STG.3 (b)	SF.AUD.1 “… if the capacity exceeds the maximum level, … SF.AUD.1 sends an e-mail containing the information about the detected event to a configured e-mail address and rejects requests from clients with a role other than TCAB-Administrator or TCAB-Auditor.” SF.I&A.1 “If the audit trail exceeds the maximum level, … SF.I&A.1 rejects login request from users with a role other than TCAB-Administrator or TCAB-Auditor.”
	FAU_STG.4	SF.AUD.1 “If the capacity of the System Data Partition is full, SF.AUD.1 shuts down the TCAB.”
System protection		
	FPT_ITT.1	SF.INT.2 “SF.INT.2 generates digital signatures for the following information: system access history, system timer configuration history, user account management data, system configuration data, and TCAB executables.” “… SF.INT.2 generates a digital signature of the moved system access history and records it on the external media.”
	FPT_ITT.3	SF.INT.2 “… SF.INT.2 verifies the system signatures to detect unauthorized modifications performed on the information described above.” “If SF.INT.2 fails in the verification, … SF.INT.2 passes event information indicating the failure to SF.AUD.1 for recording the detected event …” “If SF.INT.2 fails in the verification, … SF.INT.2 sends an e-mail containing the event information to a configured e-mail address …” “If SF.INT.2 fails in the verification, … SF.INT.2 terminates the TCAB itself.”
	FPT_RVM.1	SF.I&A.1 “If and only if the accessing client is authenticated, a remote reference (Java RMI remote reference) for using other functions ... is provided to the client. The remote reference is the only interface for accessing the TOE … and the remote reference only provides function interface (methods) for invoking security functions of the TOE. Therefore, the security functions of the TOE are always invoked.”

	FPT_SEP.1	SF.ACC.1 "SF.ACC.1 stores the document objects only on the User Data Partition and off-line disc. … By separating the user data area and the system execution area, the TSF's execution is not interfered nor tampered." SF.INT.2 "… The digital signatures protecting these data are also stored on the System Data Partition. … By separating the user data area and the system execution area, the TSF's execution is not interfered nor tampered." SF.AUD.1 "SF.AUD.1 stores the TSF data including system access history, system timer configuration history on the System Data Partition. … By separating the user data area and the system execution area, the TSF's execution is not interfered nor tampered."
	FMT_MOF.1	SF.I&A.1 "… the remote reference does not provide methods for disabling and modifying behavior of the security functions."
System management		
	FMT_SMR.2	SF.ACC.4 "SF.ACC.4 maintains … 4 security attributes belonging to individual user account. The attributes are: … and role." "SF.ACC.4 maintains 5 roles: TCAB-User, TCAB-RO-User, TCAB-Administrator, TCAB-Auditor, and TCAB-System. Each user account can have only one role."
	FMT_MTD.1 (a)	SF.ACC.4 "SF.ACC.4 provides account management capabilities to TCAB-Administrator and TCAB-Auditor based on the rules specified in Table 32." Justification: Table 32 is identical to Table 24.
	FMT_MTD.1 (b)	SF.AUD.2 "… an e-mail address … have to be configured. SF.AUD.2 provides capability to manage those configurations only for TCAB-Administrator."
	FMT_MTD.1 (c)	SF.AUD.2 "SF.AUD.2 provides capability of moving the system access history onto external media only for TCAB-Auditor."
	FMT_MTD.1 (d)	SF.AUD.2 "SF.AUD.2 provides capability of changing the system timer configuration only for TCAB-Administrator."
	FMT_MTD.1 (e)	SF.ACC.1 "SF.ACC.1 restricts the ability to backup whole of hard-drives of the TCAB to TCAB-Administrator. The backup data can include all data stored in the System Program Partition, System Data Partition, and User Data Partition."

Table 40 Justifications to additional information provided in TOE security functions

Security Function	Additional Information / Justification
SF.I&A.1	Additional Information: Nothing.
	Justification: N/A
SF.I&A.2	Additional Information: "To avoid too much e-mail notifications, **SF.I&A.2 does not send an e-mail for 10 minutes** after the last notification of continuous authentication failures."

	Justification: Without the additional information, continuous authentication failures result in too much e-mail notifications (40 notifications per a 10-minutes). With the additional information, notification interval becomes reasonable without decreasing chances for recognizing the continuous authentication failures. Therefore, the inclusion of the additional information introduces no potential security weaknesses, such as possibilities to bypass, tamper with, or deactivate other TOE security functions.
SF.NET.1	Additional Information: Nothing.
	Justification: N/A
SF.ACC.1	Additional Information: Nothing.
	Justification: N/A
SF.ACC.2	Additional Information: Nothing.
	Justification: N/A
SF.ACC.3	Additional Information: Nothing.
	Justification: N/A
SF.ACC.4	Additional Information: "On initial installation/set-up, **at least one user account having TCAB-Administrator role, one user account having TCAB-Auditor role, and one user account having TCAB-System role are created.**"
	Justification: Built-in accounts having roles TCAB-Administrator, TCAB-Auditor, and TCAB-System matches the account management rules defined in Table 32. Using the built-in account having TCAB-Administrator role can register another account having a role TCAB-User, TCAB-RO-User, or TCAB-Administrator. Using the built-in account having TCAB-Auditor role can register another account having a role TCAB-Auditor. Additionally, the built-in account having TCAB-System role is required for receiving documents from other TCAB, because no one can register/un-register an account having TCAB-System role. Therefore, the inclusion of the additional information introduces no potential security weaknesses, such as possibilities to bypass, tamper with, or deactivate other TOE security functions.
SF.INT.1	Additional Information: Nothing.
	Justification: N/A
SF.INT.2	Additional Information: Nothing.
	Justification: N/A
SF.AUD.1	Additional Information: "If the capacity is in the warning range configured during the installation/set-up procedure and **it is the first time after a start-up of the TCAB**, SF.AUD.1 sends an e-mail containing the information about the detected event to a configured e-mail address."

	Justification: Without the additional information, continuous e-mail notifications may be performed once the capacity is in the warning range. By the additional information, such continuous notifications are avoided. Additionally, the notification is performed not only the first detection but also every time the TCAB starts-up; thus, the administrator (those responsible for the TCAB administration) has multiple chances to recognize the capacity-related warning. Therefore, the inclusion of the additional information introduces no potential security weaknesses, such as possibilities to bypass, tamper with, or deactivate other TOE security functions.
SF.AUD.2	Additional Information: "SF.AUD.2 provides capability of read-access … for **TCAB-User, TCAB-Administrator,** and TCAB-Auditor."
	Justification: The SFR FAU_SAR.1 in this ST requires the TOE to provide capability of read-access to the audit data for TCAB-Auditor. SF.AUD.2 provides capability of read-access not only for TCAB-Auditor but also TCAB-User and TCAB-Administrator. The recorded audit data contains no confidential information. Even if a user having a role TCAB-User or TCAB-Administrator reads the audit data and feels uncomfortable with the recorded audit data, the user cannot change, delete, or move the audit data. Therefore, the inclusion of the additional information introduces no potential security weaknesses, such as possibilities to bypass, tamper with, or deactivate other TOE security functions.

7.5.2 Summary of Security Functions Rationale

In Table 41, cross-references the security functional requirements against the TOE security functions are shown.

According to this table, each TOE security function corresponds to at least one SFR component; therefore, each TOE security function is necessary. Additionally, each SFR component is satisfied by at least one TOE security function as shown in Section 7.5.1 and Table 41; therefore, the TOE security functions are sufficient to meet the security functional requirements for the TOE.

Table 41 Cross reference of TOE security functions and SFRs

	SF.I&A.1	SF.I&A.2	SF.NET.1	SF.ACC.1	SF.ACC.2	SF.ACC.3	SF.ACC.4	SF.INT.1	SF.INT.2	SF.AUD.1	SF.AUD.2
FIA_UAU.2(a)	X										
FIA_UID.2(a)	X										
FIA_UAU.5	X										
FIA_SOS.1							X				
FIA_AFL.1(a1)	X	X									
FIA_AFL.1(a2)	X	X									
FIA_AFL.1(b)		X									
FIA_ATD.1							X				
FIA_USB.1	X										
FTP_ITC.1(a1)			X								
FTP_ITC.1(a2)			X								
FDP_SDI.2								X			
FDP_ACC.2				X							
FDP_ACF.1				X							

FMT_MSA.3						x					
FMT_MSA.1(a)						x					
FMT_MSA.1(b)				x							
FMT_MSA.1(c)				x							
FDP_ETC.2(a)				x	x						
FDP_ETC.2(b)				x				x			
FDP_ITC.2(a)				x	x						
FDP_ITC.2(b)				x				x			
FPT_TDC.1(a)					x						
FPT_TDC.1(b)								x			
FAU_GEN.1										x	
FAU_GEN.2										x	
FPT_STM.1				x						x	x
FAU_SAR.1				x							x
FAU_STG.1								x	x		
FAU_STG.3(a)										x	
FAU_STG.3(b)										x	
FAU_STG.4	X									x	
FPT_ITT.1									x		
FPT_ITT.3									x		
FPT_RVM.1	X										
FPT_SEP.1				x					x	x	
FMT_MOF.1	X										
FMT_SMR.2							x				
FMT_MTD.1(a)							x				
FMT_MTD.1(b)											x
FMT_MTD.1(c)											x
FMT_MTD.1(d)											x
FMT_MTD.1(e)				x							

7.5.3 Minimum Strength of Function Level Rationale

The mechanism used for authenticating external entities is account name/password authentication. In general, account name/password authentication mechanism is not so strong. By applying the metric specified in the FIA_SOS.1, however, the TOE rejects use of simple passwords, and authentication rejection provided by FIA_AFL.1 (a2) rejects a continuous authentication challenge. Furthermore, the authentication protocols are protected by trusted channel provided by FTP_ITC.1 (a1), (a2), (b1), and (b2).

As assumed in A.PRIVATE-NETWORK, it is **not** assumed that the TOE shall be resistant for organizational high-grade sophisticated attacks. If such resistance is required, TOE environmental objectives must be provided.

For the functions based on cryptographic algorithms, major standardized algorithms are used and attackers not having high-grade sophisticated attack potential cannot overcome them.

Therefore, the required minimum SOF-level, **SOF-Basic**, is appropriate for the security objectives of the TOE.

7.5.4 Assurance Measures Rationale

This section of the ST rationale is intended to provide a demonstration that the specified assurance measures satisfy all security assurance requirements in the ST.

In Table 37, each security assurance requirement of the **EAL3** is mapped to at least one assurance measure provided by the TCAB. Therefore, it is clear that the assurance measures satisfy all security assurance

requirements in the ST.

8 Reference

[GOV]: Report for realizing the Internet-based governmental administrative procedures summarized by the Management and Coordination Agency arranged study group, March 2000, http://www.soumu.go.jp/gyoukan/kanri/000316a.htm

9 Glossary

TCAB	It denotes TrustyCabinet UX V1. In general, the term corresponds to the server part of the product only.
TCAB product	It denotes whole product of TrustyCabinet UX V1. The product consists of server software, software that is used in the business processing systems, and utilities.
TCABX1	It denotes TrustyCabinet UX V1 having a version different from the TOE. The TCABX1 may not be security evaluated/certified. Same as the term TCAB, this term corresponds to the server part of the product only.
TCABW1	It denotes TrustyCabinet V1 for Windows platform. The TCABW1 may not be security evaluated/certified. Same as the term TCAB, this term corresponds to the server part of the product only.
TCAB-Server	It denotes a server process working in the TCAB server machine. TCAB-Server is the TOE and does not include OS, JVM, cryptographic module, E-mail engine, XML parser, and secure communication module.
TCAB-Driver	It denotes a driver module used in the business processing systems for accessing the TCAB-Server.
TCAB-Kernel	TCAB-Kernel consists of at least System Program Partition, System Data Partition, CPU-board, and keyboard/mouse. The TCAB-Kernel is protected with hardware case from direct accesses.
Data management layer	It corresponds to the backend layer of three-layer system architecture. Databases and large capacity storage systems providing data storage and management service correspond to this layer.
Business logic layer	It corresponds to the middle layer of three-layer system architecture. Web-servers and application servers providing services correspond to this layer.
Application layer	It corresponds to the front-end layer of three-layer system architecture. Client applications and web-browsers correspond to this layer.
Business processing system	It denotes the system of business logic layer providing business-processing services.
System timer configuration history	If the system timer of the TCAB is changed by a client's request (i.e., a TCAB-Administrator's request), the TCAB records the history of the changes to the system timer. The recorded history is called system timer configuration history.
System access history	If a client accesses to the TCAB-Server, the TCAB records the history of the access on System Data Partition of the TCAB. The recorded history is called system access history.
Document access logs	If a client accesses to a document stored in the TCAB internal hard-drives, the TCAB records the log of the access on the hard-drive associated with the document as well as system access history. The recorded log is called document access logs.
Document instance	It denotes an object of a document temporarily kept on a memory.
DocSpace	It denotes a document repository of the TOE. It can store multiple documents. One TOE can have multiple DocSpaces. One DocSpace corresponds to one partition of a hard-drive or one sheet of off-line disc.
Mount of off-line disc	Mount of off-line disc corresponds to the first connection (access) to the corresponding DocSpace by a client. On mounting the off-line disc, the TOE checks the integrity of the off-line disc. If the integrity-check is successful, the off-line disc is mounted as a DocSpace of the TOE.
Unmount of off-line disc	Unmount of off-line disc corresponds to the disconnection of the last connection (access) to the corresponding DocSpace. No client is using the off-line disc, the TOE automatically unmount the off-line disc.
Inter-TCAB transfer	It denotes a document transferring between the TCAB and a distinct TCAB.

10 Abbreviation

API	Application Programming Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
DES	Data Encryption Standard
DLT	Digital Linear Tape
DMZ	De-Militarized Zone
EAL	Evaluation Assurance Level
EDMSS	Electronic Document Management and Storage System
IDEA	International Data Encryption Algorithm
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
JCA	Java Cryptography Architecture
MD5	Message Digest 5
OS	Operating System
PP	Protection Profile
RC2	Rivest's Cipher 2
RC4	Rivest's Cipher 4
RMI	Remote Method Invocation
RSA	Rivest, Shamir, Adleman (public key algorithm)
SAR	Security Assurance Requirement
SDK	Software Development Kit
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA-1	Secure Hash Algorithm 1
SMTP	Simple Mail Transfer Protocol
SOF	Strength of Function
SSL	Secure Sockets Layer
ST	Security Target
TCAB	TrustyCabinet
TCABX1	TrustyCabinet UX V1 (different version of this TOE)
TCABW1	TrustyCabinet V1 (for Windows platform)
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UPS	Uninterruptible Power Supplies
XML	eXtensible Markup Language