JPKI Applet

Protection Profile

Version 1.10
JISEC-C0859

Digital Agency, Government of Japan

Contents

1. PP Introduction 1

1.1. PP reference 1

1.2. Definitions 1

1.3. TOE Description 2

1.3.1. TOE type 2

1.3.2. TOE and non-TOE components 3

1.3.3. Available non-TOE hardware/software/firmware 4

1.3.4. TOE major security features 4

1.4. Life-cycle 5

1.4.1. JPKI provisioning stage 6

1.4.2. JPKI operational stage 6

2. Conformance claims 7

2.1. CC conformance claim 7

2.2. PP claim 7

2.3. Package claim 7

3. Security problem definition 8

3.1. Subjects 8

3.2. Assets 8

3.3. Threats 9

3.4. Organisational security policies 9

3.5. Assumptions 10

4. Security objectives 11

4.1. Security objectives for the TOE 11

4.2. Security objectives for the operational environment 11

4.3. Security objectives rationale 13

5. Security requirements 15

5.1. Security functional requirements 15

5.2. Security assurance requirements 19

5.2.1. Security requirement coverage 21

5.3. Security assurance requirements rationale 23

6. References 25

1. PP Introduction

This document is the Protection Profile (PP) for Common Criteria evaluation of JPKI Applet.

For definitions of the references used in this document, see Chapter 6 References".

1.1. PP reference

Table 1-1 PP identification

PP attribute	
Name	JPKI Applet Protection Profile
Version	1.10
Issue Date	January 2026
Provided by	Digital Agency, Government of Japan
Certification No.	JISEC-C0859

1.2. Definitions

Table 1-2 Definitions

Definition	
Certificate	digital signature used as electronic attestation binding a Public Key (PK) to a person confirming the identity of that person as legitimate signer
Certificate info	information associated with a SK/PK pair that may be stored in a Secure Signature Creation Device (SSCD)
Certificate generation application (CGA)	collection of application components that receive the PK from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate
Data to be signed (DTBS)	all electronic data to be signed including a user message and additional information that is signed together with a user message
Data to be signed or its unique representation (DTBS/R)	data received by a SSCD as input in a single signature creation operation
External device	Devices outside the TOE that interact with the TOE such as contactless card readers, servers and the host controller of a mobile phone.
Individual Number Card	a plastic card issued to residents of Japan that contains an embedded IC chip and displays the holder’s name, address, date of birth, sex, 12-digit Individual Number, and photo.
Japanese Public Key Infrastructure (JPKI)	a safe and secure identity verification service that uses electronic certification installed in My Number Card's IC chips (My Number is not used) to officially authenticate users and confirm that documents such as contracts have not been

	tampered with online.
JPKI Applet	a Java Card applet that is responsible for generating a key pair for digital signature and for user certification
JPKI application	a mobile phone application responsible for CGA and Signature Creation Application (SCA).
Password (PW)	data persistently stored by the TOE for authentication of a user as authorised for a particular role
Public Key (PK)	public cryptographic key that can be used to verify a digital signature. JPKI Applet has two PKs, which are “the public key for digital signature” and “the public key for user certification”.
Secure Signature Creation Device (SSCD)	hardware or software that is used in creating a digital signature
Secure Element Issuer Trusted Service Manager (SEI-TSM)	responsible for managing the end-to-end security of the SE, including the deployment of applications and services.
Service Provide Trusted Service Manager (SP-TSM)	entity that issues certificates or provides other services related to digital signatures
Signature creation application (SCA)	application complementing a SSCD with a user interface with the purpose to create a digital signature
Secret Key (SK)	secret cryptographic key stored in the SSCD under exclusive control by the signatory to create a digital signature. JPKI Applet has two SKs, which are “the secret key for digital signature” and “the private key for user certification”.
Verification authentication data (VAD)	data provided as input to a SSCD for authentication

1.3. **TOE Description**

1.3.1. TOE type

The TOE is an embedded secure element (eSE) on the mobile phone. The TOE acts as a Java Card system that provides a secure signature creation device (SSCD) with key generation for creating a digital signature and authenticating users. The TOE is assumed to be comprised of the JPKI Applet, a Java Card Platform, and an integrated circuit (IC). The IC and the platform can be evaluated and certified separately. The JPKI Applet on top of the IC and the platform are evaluated as composite product evaluation and certification.

1.3.2. TOE and non-TOE components

The following figure illustrates the physical scope of the TOE (indicated in yellow).

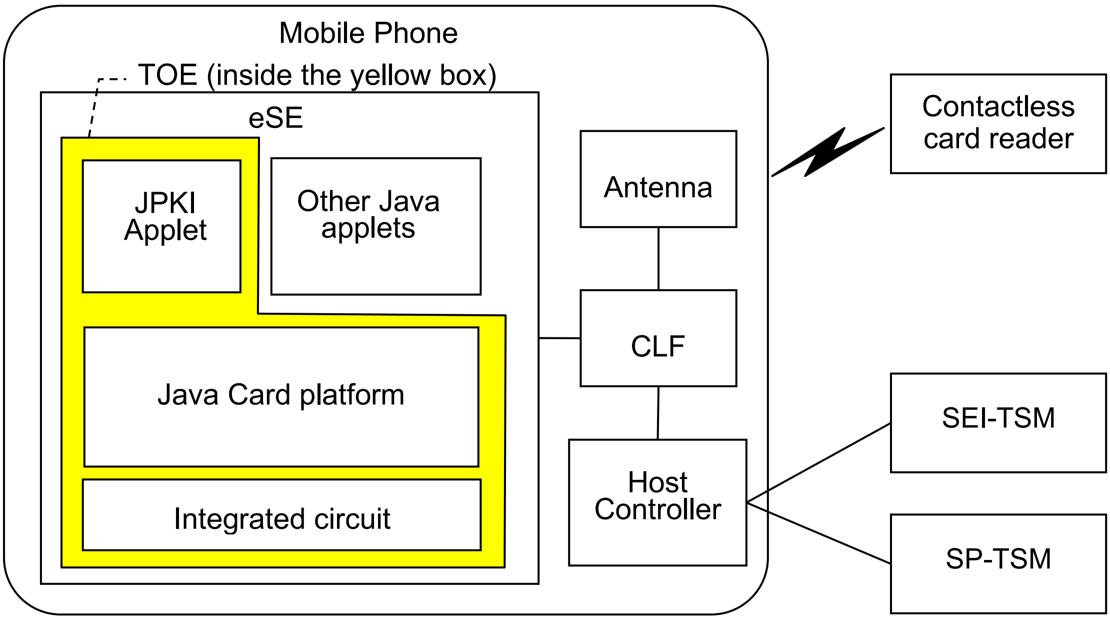


Figure 1-1 TOE physical scope

The components of the TOE are explained as follows:

- JPKI Applet constitutes the part of the TOE that is responsible for generating a key pair for digital signature and for user certification. It manages the access control to use the signature creation function and executes the cryptographic operation for generating a digital signature. The JPKI Applet is installed as a post-issuance in the operational environment.
- Java Card Platform manages and executes applets. It provides APIs for developing applets in accordance with the Java Card specification [JC-SPEC]. Java Card Platform has GlobalPlatform packages providing a common interface to communicate with a smart card and manage applications in a secure way according to the GP specifications [GP].
- Integrated circuit is the hardware platform of the TOE. The hardware platform provides the basic cryptographic functionalities and includes security detectors, sensors, and circuitry to protect the TOE.

The components of the non-TOE are explained as follows:

- Other Java applets can coexist with the JPKI Applet, but they are logically independent of each other.
- Antenna is used to transmit and receive radio waves to communicate with Contactless card reader. It can convert electrical signals into radio waves and vice versa.
- CLF (Contactless Front-end) manages packet rooting between Antenna and Host controller, controlling carrier wave transmission of Antenna, acquiring card (anti-collision) as card function.
- Host controller controls CLF and communication with external servers (such as SEI-TSM and SP-TSM). It is equivalent with main processor of mobile phone.
- The TOE is supposed to run on mobile phone. Therefore, all above non-TOE components are also

part of a mobile phone.

1.3.3. Available non-TOE hardware/software/firmware

Operation of the TOE does not rely on other IT environment, except for power supply from a mobile phone.

1.3.4. TOE major security features

Japanese Public Key Infrastructure (JPKI) is a safe and secure identity verification service that uses electronic certification installed in Individual Number Card (also called as My Number Card) IC chips to officially authenticate users and confirm that documents such as contracts have not been tampered with.

By incorporating the functions of electronic certification in Individual Number Card into an eSE (the TOE) on the mobile phone, it has become possible to apply for and use various Individual Number Card services anytime and anywhere on a single mobile phone without having to carry an Individual Number Card.

The functional overview of the TOE in its distinct operational environments is explained as follows:

- The preparation environment where JPKI application interacts with the SEI-TSM to load the JPKI Applet, and where the TOE interacts with a certification service provider (SP-TSM) to obtain a certificate for the public key (PK) corresponding with the secret key (SK) generated by the TOE.
- The signing environment where it interacts with a signer through JPKI application to sign data after authenticating the signer as its signatory. The signature creation application (SCA) provides the data to be signed, or a unique representation thereof (DTBS/R) as input to the TOE signature creation function and obtains the resulting digital signature.

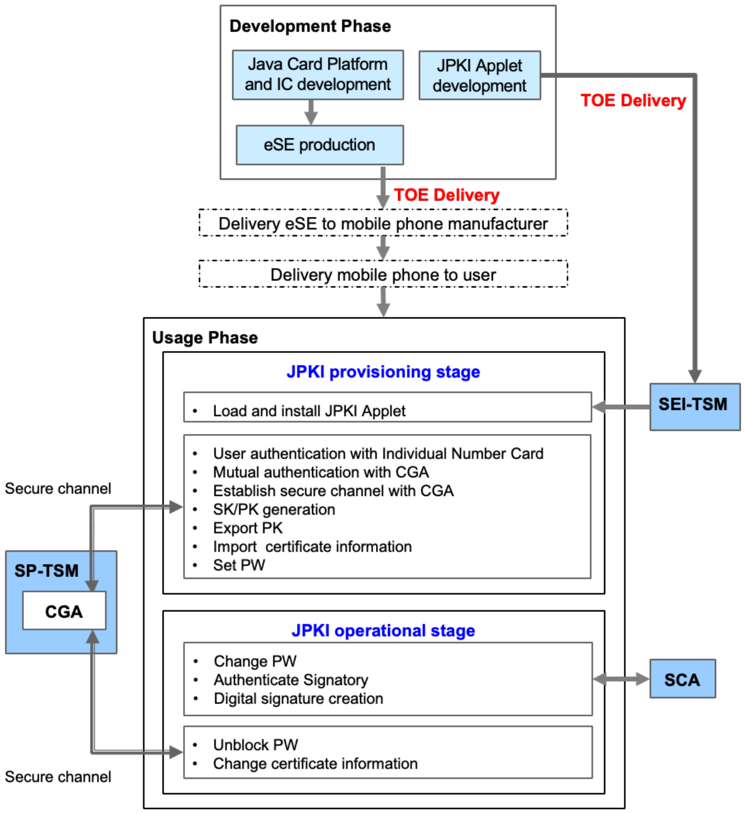
The TOE performs the following functions:

- to generate SK for digital signature and the correspondent PK;
- to generate SK for user certification and the correspondent PK;
- to prove the identity as SSCD to SP-TSM;
- to export the PKs for certification through a secure channel to the CGA;
- to receive and store certificate info;
- to switch the TOE from a non-operational state to an operational state;
- to create digital signatures through the following steps:
  A) authenticate the signatory for digital signature and determine its intent to sign;
  B) select a SK for digital signature in the SSCD;
  C) receive DTBS/R;
  D) apply an appropriate cryptographic signature creation function using the selected SK to the DTBS/R;

- to authenticate user for user certification through the following steps:
  - A) authenticate the signatory for user certification and determine its intent to sign;
  - B) select a SK for user certification in the SSCD;
  - C) receive DTBS/R;
  - D) apply an appropriate cryptographic signature creation function using the selected SK to the DTBS/R;
- to import a public key for external authentication and authenticate a user as its signatory by using the public key;
- to generate random number meeting the quality metric depending on purposes.

1.4. Life-cycle

The TOE life-cycle distinguishes phases for development and usage. The development phase is subject of CC evaluation according to ALC class. In this phase, the JPKI Applet, the Java Card Platform and the integrated circuit are developed. The Java Card Platform and the integrated circuit are embedded in the eSE and delivered to mobile phone manufacturers. The Java Card Applet is delivered to SEI-TSM for post-issuance. The development phase ends with the delivery of the TOE (the delivery of the eSE to mobile phone manufacturers and the delivery of the JPKI Applet to SEI-TSM). The TOE embedded in the mobile phone is finally delivered to a mobile phone user. The usage phase has two stages: the JPKI preparation stage and JPKI operational use stage. The TOE life-cycle and the two stages are described in the following figure and sections.



Development Phase
Java Card Platform and IC development
JPKI Applet development
eSE production
TOE Delivery
TOE Delivery
Delivery eSE to mobile phone manufacturer
Delivery mobile phone to user
Usage Phase
JPKI provisioning stage
Load and install JPKI Applet
SEI-TSM
User authentication with Individual Number Card
Mutual authentication with CGA
Establish secure channel with CGA
SK/PK generation
Export PK
Import certificate information
Set PW
Secure channel
SP-TSM
CGA
JPKI operational stage
Change PW
Authenticate Signatory
Digital signature creation
SCA
Unblock PW
Change certificate information
Secure channel

Figure 1-2 TOE lifecycle

1.4.1. JPKI provisioning stage

In JPKI provisioning stage, SEI-TSM loads and installs the JPKI Applet to the eSE embedded in the mobile phone held by the user.

After that, SP-TSM performs the following tasks:

- obtain information on the intended recipient of the device as required for the preparation process and for identification as a legitimate user by authenticating the user's Individual Number Card.
- perform mutual authentication between SP-TSM and the TOE, and establish the secure channel.
- request the TOE to generate SK/PK pairs for digital signature and for user certification.
- request the TOE to export PKs from the TOE and import the certificate information corresponding to each PK to the TOE via the secure channel.
- generate a temporary password for digital signature and for user certification and store them as PWs in the TOE.

Finally, SCA changes PWs to new passwords specified by the legitimate user (signatory).

1.4.2. JPKI operational stage

In JPKI operational stage, the following operations are available:

- The TOE authenticates user as a signatory based on password authentication.
- For password for user certification, external authentication can be added. The external authentication is an alternative for the password authentication. The method of external authentication is public-key cryptography based authentication where the user is authenticated via external biometrics verification device on behalf of password. (See Figure 1-3.)
- The signatory creates digital signatures via SCA.
- PW is locked when wrong VAD is entered specified number of times. Only the administrator can unlock via the secure channel.
- SK/PK and the corresponding certificate information in the TOE permanently can be unusable on demand.

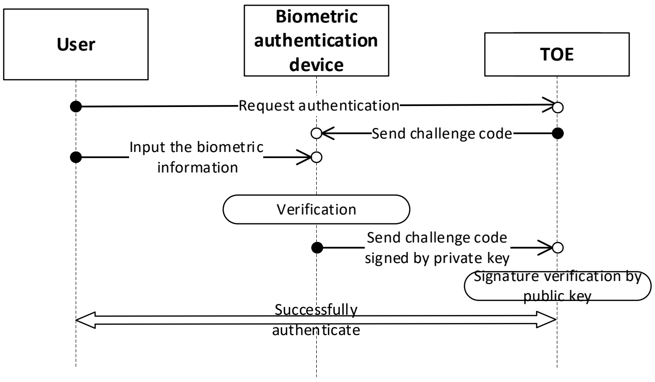

User
Biometric authentication device
TOE
Request authentication
Send challenge code
Input the biometric information
Verification
Send challenge code signed by private key
Signature verification by public key
Successfully authenticate

Figure 1-3 External authentication method

2. Conformance claims

2.1. CC conformance claim

The evaluation is based on the following:

- "Common Criteria for Information Technology Security Evaluation", CC:2022, Release 1 (composed of Part1-5, [CC Part 1], [CC Part 2], [CC Part 3], [CC Part 4], and [CC Part 5])
- "Common Methodology for Information Technology Security Evaluation: Evaluation Methodology", CEM:2022, Release 1 [CC CEM]
- "Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1)", Version 1.1

This PP claims the following conformances:

- [CC Part 2] conformant
- [CC Part 3] conformant
- [CC Part 5] conformant

2.2. PP claim

This PP does not claim conformance to any other PP.

This PP requires strict conformance to the PP and ST claiming conformance to this PP.

2.3. Package claim

This PP claims conformance to the assurance packages:

- Evaluation Assurance Level 4 (EAL4) augmented with ALC_DVS.2 and AVA_VAN.5
- Composite product package (COMP)

3. Security problem definition

3.1. Subjects

Table 3-1 Subjects

Subjects	Definition
User	End user of the TOE who can be identified as administrator or signatory. The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.
Administrator	User who is in charge to perform the TOE initialisation, TOE personalisation or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator.
Signatory	User who holds the TOE and use it on their own behalf or on behalf of the natural or legal person or entity they represent. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as signatory.
Attacker	Human or process acting on their behalf located outside the TOE. The main goal of the attacker is to access the SK or to falsify the digital signature. The attacker has got a high attack potential and knows no secret.

3.2. Assets

CC defines assets as entities that the owner of the TOE presumably places value upon. The term “asset” is used to describe the threats in the operational environment of the TOE.

Table 3-2 Assets and objects

Assets	Description
SK	private key used to perform a digital signature operation. The confidentiality, integrity and signatory’s sole control over the use of the SK shall be maintained. In JPKI, SK corresponds “the private key for digital signature” and “the private key for user certification”.
PK	public key linked to the SK and used to perform digital signature verification. The integrity of the PK when it is exported shall be maintained. In JPKI, PK corresponds “the public key for digital signature” and “the public key for user certification”.
DTBS and DTBS/R	set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the digital signature shall be maintained.
Public key for external authentication (PK-EA)	This public key is imported and stored in the TOE, and used to authenticate as user as its signatory.
User data	set of data imported from external devices, that are the certificate, the certificate info, and other information to operate JPKI services.

3.3. **Threats**

Table 3-3 Threats

Threats	Description
T.Illegal_Attack	An unauthorised user accesses the TOE via external interfaces to disclose or modify internal data of the TOE, or to use processing function of the TOE. “An unauthorised user” is the entity that does not have the authentication data needed to access the assets of the TOE.
T.Replay	An attacker masquerades a legitimate external terminal by monitoring, recording and replaying the authentication procedure between the TOE and the external terminal in order to be authenticated by the TOE. The attack causes disclosure or modification of user data of the TOE, or illegal use of processing function of the TOE.
T.Phys_Attack	An attacker attacks components of the TOE – hardware, firmware or software – with physical means. The attack causes disclosure or modification of user data of the TOE, or unauthorised use of processing function of the TOE.

3.4. **Organisational security policies**

Table 3-4 Organisational security policies (OSP)

OSP	Description
P.Multiple_authentication	The TOE provides multiple authentication methods to authenticate users. In addition to the password authentication, users also select cryptography key-based authentication.
P.Secure_messaging	Secure messaging shall be applied to the communication between the TOE and CGA.
P.Cryptography	The TOE provides cryptographic functions which are used for data hashing, data protection, SK/PK generation, signature creation and authentication.
P.RND	The TSF generates random numbers to be used for the TSF itself. The quality of random numbers is sufficient to prevent prediction by an attacker.

3.5. Assumptions

Table 3-5 Assumptions

Assumptions	Description
A.PKI	For the effective operation of the TSF, it is assumed that the PKI environment, where the keys for public key cryptosystem (a pair of public and private keys) of the TOE are assured to be effective, is provided.
A.Administrator	The administrator, who creates, changes or deletes data on the TOE, is assumed to be a trusted user and to operate the TOE properly based on the privileges.
A.Protect_VAD	The confidentiality and integrity of VAD is assumed to be guaranteed when VAD is imported from an external device to the TOE.

4. Security objectives

This chapter describes the security objectives for the TOE and the TOE environment in response to the security needs identified in Chapter 3, "Security problem definition".

Security objectives for the TOE are to be satisfied by technical countermeasures implemented by the TOE. Security objectives for the environment are to be satisfied either by technical measures implemented by the IT environment, or by non-IT measures.

4.1. Security objectives for the TOE

Table 4-1 Security objectives for the TOE

Security objectives for the TOE	Description
O.I&A	The TOE shall identify/authenticate a user of the TOE and authorise the user who has been authenticated successfully to perform the actions corresponding to the role of the user. The TOE prevents the reuse of authentication data and provides multiple authentication methods to users. In addition to the password authentication, users also select cryptography key-based authentication.
O.Access_Control	The TOE shall permit the subjects controlled under the TOE to access the objects controlled under the TOE based on privileges of each subject. The other accesses shall be prohibited.
O.Secure_messaging	The TOE shall apply secure messaging for communication between the TOE and CGA. Secure messaging shall protect the confidentiality and integrity of the transferred data.
O.Cryptography	The TOE shall provide cryptographic operational function and cryptographic key management function for data hashing, SK/PK generation, signature creation and authentication.
O.Phys_Attack	The TSF shall protect data inside of the TOE from disclosure and modification, or functions of the TOE from unauthorised use, with physical attacks to the elements of the TOE (hardware/firmware/software).
O.RND	The TSF shall generate random numbers meeting the quality metric depending on purposes.

4.2. Security objectives for the operational environment

Table 4-2 Security objectives for the operational environment

Security objectives for the operational environment	Description
OE.PKI	The PKI system is provided to assure validity of keys of the public key cryptosystem of the TOE in the operational environment of the TOE.
OE.Administrator	The administrator who initialises, modifies and deletes the data within the TOE is a trusted user, and operate the TOE properly based on their privileges.

OE.Protect_VAD	External device shall ensure the confidentiality and integrity of VAD when VAD is imported from an external device to the TOE.

4.3. **Security objectives rationale**

The following table provides an overview for security objectives coverage.

Table 4-3 Mapping of security problem definition to security objectives

	O.I&A	O.Access_Control	O.Secure_messaging	O.Cryptography	O.Phys_Attack	O.RND	OE.PKI	OE.Administrator	OE.Protect_VAD
T.Illegal_Attack	X	X							
T.Replay	X								
T.Phys_Attack					X				
P.Multiple_authentication	X								
P.Secure_messaging			X						
P.Cryptography				X					
P.RND						X			
A.PKI							X		
A.Administrator								X	
A.Protect_VAD									X

The following explanation shows that the chosen security objectives are sufficient and suitable to address the identified threats, policies, and assumptions.

T.Illegal_Attack

O.I&A provides that the TOE identifies and authenticates a user of the TOE and grants only the user, who has been authenticated successfully, the privilege corresponding to the role assigned to the user. O.Access_Control limits the extent of accessing to objects to what is limited by the privileges associated with the identification information. These security objectives prevent users from disclosing or modifying data beyond their privileges, or using the service functions illegally. These security objectives diminish sufficiently the threat T.Illegal_Attack.

T.Replay

When an attacker monitors and records data of authentication procedures of an external terminal and makes an authentication attempt to the TOE by impersonating the external terminal, O.I&A will invalidate the authentication data which has been used once and reject the request of authentication. O.I&A removes the threat of impersonation by replaying the same authentication procedures shown in T.Replay.

T.Phys_Attack

Security violation of the assets by physical attacks to the TOE will be prevented by O.Phys_Attack. Therefore, the threat T.Phys_Attack is diminished sufficiently.

P.Multiple_authentication

O.I&A provides the multiple authentication methods to authenticate users.

P.Secure_messaging

O.Secure_messaging protects communication data between the TOE and CGA from disclosure and modification. Therefore, P.Secure_messaging is enforced properly.

P.Cryptography

O.Cryptography is suitable as it directly corresponds to P.Cryptography.

P.RND

If O.RND is enforced, random numbers with a quality sufficient for the TSF will be generated, and also it will prevent an attacker from retrieving information helpful to guess random numbers. O.RND prevents an attacker from guessing random numbers generated. Therefore, P.RND is enforced properly.

A.PKI

OE.PKI is suitable as it directly corresponds to A.PKI.

A.Administrator

OE.Administrator indicates that administrators in charge of setting up, modifying or deleting of data or APs within TOE should be appointed on the condition that; they are able to correctly operate the specific IT devices and; will not attempt any malicious act on the assets of the TOE, and that necessary rights for the administration are granted to them. Furthermore, it also indicates that reliable external terminals should be provided for use of administrators. This objective is suitable to uphold A.Administrator.

A. Protect_VAD

OE. Protect_VAD is suitable as it directly corresponds to A. Protect_VAD.

5. Security requirements

This chapter gives the security functional requirements and the security assurance requirements for the TOE.

5.1. Security functional requirements

The TOE Security Objectives result in a set of Security Functional Requirements (SFRs).

About the notation used for Security Functional Requirements (SFRs):

- Refinements are denoted as **bold text**.
- Selections made by the PP author are denoted as underlined text. Selections to be filled in by the ST author are denoted with [selection:] and are *italicised*.
- Assignments made by the PP author are denoted as underlined text. Assignments to be filled in by the ST author are denoted with [assignment:] and are *italicised*. In some other cases the assignment made by the PP author defines an assignment to be performed by the ST author. In this case, the text is both underlined and *italicised*.
- Iterations are denoted by showing a slash "/".

FCS_CKM.1 **Cryptographic key generation**

FCS_CKM.1.1 The TSF shall generate SK/PK pair in accordance with a specified cryptographic key generation algorithm RSA and specified cryptographic key sizes [assignment: *2048 bit or more*] that meet the following: [assignment: *list of standards*].

FCS_CKM.6/SK **Timing and event of cryptographic key destruction**

FCS_CKM.6.1/SK The TSF shall destroy SK/PK pair when no longer needed.

FCS_CKM.6.2/SK The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

FCS_CKM.6/PK-EA **Timing and event of cryptographic key destruction**

FCS_CKM.6.1/PK-EA The TSF shall destroy PK-EA when no longer needed.

FCS_CKM.6.2/PK-EA The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

FCS_COP.1/SK **Cryptographic operation**

FCS_COP.1.1/SK The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes [assignment: *2048 bit or more*] that meet the following: [assignment: *list of standards*].

FCS_COP.1/PK-EA **Cryptographic operation**

FCS_COP.1.1/PK-EA The TSF shall perform digital signature verification in accordance with a specified cryptographic algorithm RSA and cryptographic key sizes [assignment: *2048 bit or more*] that meet the following: RSASSA-PKCS1-v1_5 in [PKCS #1].

FCS_COP.1/Hash **Cryptographic operation**

FCS_COP.1.1/Hash The TSF shall perform hash calculation in accordance with a specified cryptographic algorithm SHA-256 and cryptographic key sizes none that meet the following: [FIPS180-4].

FCS_RNG.1 **Random number generation**

FCS_RNG.1.1 The TSF shall provide a [selection: *physical, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*].

FCS_RNG.1.2 The TSF shall provide [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*] that meet [assignment: *a defined quality metric*].

FDP_ACC.1 **Subset access control**

FDP_ACC.1.1 The TSF shall enforce the JPKI access control SFP on

(1) subjects: subjects shown in Table 5-1,

(2) objects: objects shown in Table 5-1,

(3) operations: operations shown in Table 5-1.

FDP_ACF.1 **Security attribute based access control**

FDP_ACF.1.1 The TSF shall enforce the JPKI access control SFP to objects based on the following:

(1) Subjects: subjects shown in Table 5-1.

(2) Objects: objects shown in Table 5-1,

(3) SFP relevant security attribute for subject: authentication result of the user associated with the subject,

(4) SFP relevant security attribute for object: operations allowed to the subject shown in Table 5-1.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

If authentication result of the user associated with the subject is “authenticated successfully”, the subject will be able to perform operations allowed to the object.

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

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

Table 5-1 : JPKI access control SFP

Subject	Security Attribute	Object	Operation
S.Sigy	Successful authentication result as Signatory	SK	Digital signature creation
		Certificate	Read
		PK-EA	Write
S.Admin	Successful authentication result as Administrator	SK/PK pair	Generate key pair
		PK	Read
		Certificate	Write
		User data	Write
S.User	Not authenticated	PK-EA	Digital signature verification
		User data	Read

FDP_ITC.1 **Import of user data without security attributes**

FDP_ITC.1.1 The TSF shall enforce the JPKI access control SFP when importing user data, controlled under the SFP, from outside of the TOE.

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

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: none.

FIA_UID.1 **Timing of identification**

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions*]

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

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

FIA_UAU.1 **Timing of authentication**

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions*]

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

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

FIA_UAU.4 **Single-use authentication mechanism**

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to External authentication using PK-EA.

FIA_UAU.5 **Multiple authentication mechanisms**

FIA_UAU.5.1 The TSF shall provide

the multiple authentication mechanisms shown in Table 5-2

to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the rules describing how the multiple authentication mechanisms provide authentication shown in Table 5-2.

Table 5-2 : Multiple authentication mechanisms

Authentication mechanism	Rules
Mutual authentication specified in [GP_D]	Mutual authentication specified in [GP_D] is used for authenticating user as Administrator.
Password authentication	Password authentication is used as default authentication mechanism for authentication of Signatory.
External authentication using PK-EA	External authentication is used as alternative authentication mechanism for authenticating user as Signatory. To activate the method, the PK-EA corresponding to the individual Signatory needs to be registered.

FIA_AFL.1 **Authentication failure handling**

FIA_AFL.1.1 The TSF shall detect when [assignment: *positive integer number*] unsuccessful authentication attempts occur related to consecutive failed authentication attempts.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall block PW and PK-EA.

FMT_SMR.1 **Security roles**

FMT_SMR.1.1 The TSF shall maintain the roles R.Admin and R.Sigy.

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

FMT_SMF.1 **Security management functions**

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

(1) changing default and unblocking of PW,

(2) modification of PW.

FMT_MSA.3 **Static attribute initialisation**

FMT_MSA.3.1 The TSF shall enforce the JPKI 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 R.Admin to specify alternative initial values to override the default values when an object or information is created.

Application Note: The security attributes of JPKI access control SFP will not be changed after creation. Therefore, FMT_MSA.1 is not applied.

FMT_MTD.1/Admin Management of TSF data

FMT_MTD.1.1/Admin The TSF shall restrict the ability to change_default, unblock the PW to R.Admin.

FMT_MTD.1/Signatory Management of TSF data

FMT_MTD.1.1/Signatory The TSF shall restrict the ability to modify the PW to R.Sigy.

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist attacks with physical means and included in the IC evaluation method provided by the [JIWG] supporting documents to the TSF by responding automatically such that the SFRs are always enforced.

FTP_ITC.1 Inter-TSF trusted channel

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

FTP_ITC.1.2 The TSF shall permit another trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for

(1) generation of SK/PK pair, export of PK and import of Certificate

(2) changing default and unblocking of PW

(3) update of user data

(4) [assignment: other list of functions for which a trusted channel is required]

5.2. Security assurance requirements

The Security Assurance Requirements for the TOE are those taken from the Evaluation Assurance Level 4 (EAL4) and augmented with the component ALC_DVS.2, AVA_VAN.5, and the component of composite product package ADV_COMP.1, ALC_COMP.1, ATE_COMP.1, ASE_COMP.1 and AVA_COMP.1. The assurance requirements are shown in the following table.

Table 5-3 Assurance requirements: EAL4 augmented with ALC_DVS.2, AVA_VAN.5, and COMP package

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Architectural Design with domain separation and non-bypassability
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF

	ADV_TDS.3 Basic modular design
	ADV_COMP.1 Design compliance with the base component-related user guidance, ETR for composite evaluation and report of the base component evaluation authority
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.2 Sufficiency of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_COMP.1 Integration of the dependent component into the related base component and consistency check for delivery and acceptance procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
	ASE_COMP.1 Consistency of Security Target (ST)
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
	ATE_COMP.1 Composite product functional testing
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis
	AVA_COMP.1 Composite product vulnerability assessment

5.2.1. Security requirement coverage

Table 5-4 Functional requirement to TOE security objective mapping

	O.I&A	O.Access_Control	O.Secure_messaging	O.Cryptography	O.Phys_Attack	O.RND
FCS_CKM.1				X		
FCS_CKM.6/SK				X		
FCS_CKM.6/PK-EA				X		
FCS_COP.1/SK				X		
FCS_COP.1/PK-EA				X		
FCS_COP.1/Hash				X		
FCS_RNG.1						X
FDP_ACC.1		X				
FDP_ACF.1		X				
FDP_ITC.1		X		X		
FIA_UID.1	X					
FIA_UAU.1	X					
FIA_UAU.4	X					
FIA_UAU.5	X					
FIA_AFL.1	X					
FMT_MSA.3		X		X		
FMT_MTD.1/Admin	X					
FMT_MTD.1/Signatory	X					
FMT_SMF.1	X			X		
FMT_SMR.1	X	X		X		
FPT_PHP.3					X	
FTP_ITC.1		X	X			

O.I&A

FIA_UID.1 and FIA_UAU.1 describe the requirements of identification and authentication for users. Multiple authentication mechanisms for Administrator and Signatory can be provided by FIA_UIA.5. FIA_UAU.4 is applied to restrict reuse of authentication data to prevent illegal authentication of Signatory using PK-EA. FIA_AFL.1 describes the TSF action for authentication failures for each authentication mechanism. The administrative requirements for authentication data of the TOE users are provided by FMT_MTD.1/Admin, FMT_MTD.1/Signatory, FMT_SMF.1 and FMT_SMR.1. These SFRs achieve O.I&A sufficiently.

O.Access_Control

O.Access_Control requires that only the legitimate users are allowed to access user data within their own privileges. This requirement is provided by FDP_ACC.1, FDP_ACF.1. FDP_ITC.1, FMT_MSA.3, and FMT_SMR.1 are applied to manage the security attributes. These SFRs achieve O.Access_Control sufficiently.

O.Secure_messaging

O.Secure_messaging is directly realised through the requirement for the secure channel FTP_ITC.1 between the TOE and the external device.

O.Cryptography

FCS_COP.1/SK, FCS_COP.1/PK-EA and FCS_COP.1/Hash provide cryptographic functions for digital signature creation, external authentication and data hashing respectively. The lifecycle of the cryptographic key used for digital signature creation is managed by FCS_CKM.1 and FCS_CKM.6/SK. The public key used for external authentication is imported from outside of TOE. This requirement is addressed by FDP_ITC.1, FMT_MSA.3, FMT_SMR.1 and FMT_SMF.1. FCS_CKM.6/PK-EA ensures that public key for external authentication is destroyed securely. These SFRs achieve O.Cryptography sufficiently.

O.Phys_Attack

O.Phys_Attack requires countermeasures against security violation of data and functions of the TOE with physical attacks. FPT_PHP.3 requires resistance to physical attacks to the TSF. If the TSF is not violated with physical attacks, the TSF will prevent security violation of data and functions of the TOE, with the logical security functionality of the TSF. Therefore, if this SFR is met, O.Phys_Attack will be achieved sufficiently.

O.RND

The security objective O.RND requires countermeasures that a random number to be generated has sufficient quality and makes it difficult to be guessed by an attacker. FCS_RNG.1 requires generation of random numbers satisfying a quality metric needed.

Table 5-5 Satisfaction of dependencies of security functional requirements

SFRs	Dependencies	Satisfied by
FCS_CKM.1	[FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1], [FCS_RBG.1 or FCS_RNG.1], FCS_CKM.6	FCS_COP.1/SK, FCS_RNG.1, FCS_CKM.6/SK
FCS_CKM.6/SK	[FDP_ITC.1, or FDP_ITC.2,	FCS_CKM.1

	or FCS_CKM.1, or FCS_CKM.5]	
FCS_CKM.6/PK-EA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5]	FDP_ITC.1
FCS_COP.1/SK	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5], FCS_CKM.6	FCS_CKM.1 FCS_CKM.6/SK
FCS_COP.1/PK-EA	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5], FCS_CKM.6	FDP_ITC.1 FCS_CKM.6/PK-EA
FCS_COP.1/Hash	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1, or FCS_CKM.5], FCS_CKM.6	Non-satisfied dependency because no key generation/import and destruction for hash function is necessary.
FCS_RNG.1	No dependencies	n/a
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3
FDP_ITC.1	[FDP_ACC.1, or FDP_IFC.1], FMT_MSA.3	FDP_ACC.1, FMT_MSA.3
FIA_UID.1	No dependencies	n/a
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.4	No dependencies	n/a
FIA_UAU.5	No dependencies	n/a
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_SMR.1 is applied. FMT_MSA.1 is not applied because the security attributes of JPKI access control SFP will not be changed after creation.
FMT_MTD.1/Admin	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Signatory	FMT_SMR.1, FMT_SMF.1	FMT_SMR.1, FMT_SMF.1
FMT_SMF.1	No dependencies	n/a
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_PHP.3	No dependencies	n/a
FTP_ITC.1	No dependencies	n/a

5.3. Security assurance requirements rationale

To meet the assurance expectations of customers, the assurance level EAL4 and the augmentation with the requirements ALC_DVS.2, AVA_VAN.5, and the COMP package are chosen. The assurance level of EAL4 is selected because it provides a sufficient level of assurance for this type of TOE, which is expected to protect high value assets. Explanation of the security assurance component ALC_DVS.2 and AVA_VAN.5 follows:

- ALC_DVS.2 Sufficiency of security measures: This Protection Profile selects ALC_DVS.2 instead of ALC_DVS.1 because it verifies the security measures that provide the necessary level of protection to maintain the confidentiality and integrity of the TOE and its user data.
- AVA_VAN.5 Highly resistant: The TOE might be in danger of high-level attacks such as those it might encounter in a university laboratory. Therefore, AVA_VAN.5 is augmented to confirm that TOE has a high level of resistance against such attacks.

The COMP package is selected because the TOE requires composite evaluation with the certified underlying platform.

6. References

[CC CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CEM:2022, Revision 1, CCMB-2022-11-006, November 2022.

[CC Part 1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CC:2022, Revision 1, CCMB-2022-11-001, November 2022

[CC Part 2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, CC:2022, Revision 1, CCMB-2022-11-002, November 2022

[CC Part 3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CC:2022, Revision 1, CCMB-2022-11-003, November 2022.

[CC Part 4] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, CC:2022, Revision 1, CCMB-2022-11-004, November 2022.

[CC Part 5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, CC:2022, Revision 1, CCMB-2022-11-005, November 2022.

[CC Errata] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, July 2024.

[FIPS 180-4] FIPS PUB 180-4: Secure Hash Standard (SHS), Federal Information Processing Standards Publication, 2015, August, National Institute of Standards and Technology

[GP][1] GlobalPlatform Card Specification

[GP_D][1] GlobalPlatform Card Specification – Amendment D Secure Channel Protocol ‘03’

[JC-SPEC][1] Java Card Platform Virtual Machine Specification, Classic Edition

[JIWG][1] Joint Interpretation Library – Application of Attack Potential to Smartcards and Similar Devices

[PKCS #1] PKCS #1: RSA Cryptography Standard, Version 2.2, October 27, 2012, RSA Laboratories

[1] Note : Regarding [GP], [GP_D], [JC_SPEC] and [JIWG], ST author needs to identify which version to use.