JICSAP
Japan ID Connect with Secure Authentication Promotional association

Public Transportation IC Card Protection Profile

Version 1.12

Japan ID Connect with Secure Authentication Promotional association

01 August 2018

Contents

1 Introduction

This document is the PP for CC evaluation of transportation card in Japan as well as followers in other countries.

This PP is provided in accordance with "Common Criteria for Information Technology Security Evaluation".

For definitions of the terms, abbreviations, and literary references used in this document, see Chapter 7, "Glossary and references".

1.1 PP Reference

This section provides the information necessary to identify and control this PP.

Table 1: PP identification

PP attribute	Value
Name	Public Transportation IC Card Protection Profile
Version	1.12
Issue Date	1 August, 2018
Provided by	Dai Nippon Printing Co., Ltd. JR East Mechatronics Co., Ltd Kyodo Printing Co., Ltd. Panasonic Semiconductor Solutions Co., Ltd. Sony Imaging Products & Solutions Inc. Toppan Printing Co., Ltd. as a member of Japan ID Connect with Secure Authentication Promotional association Standardization Dept.
Supervised by	IC System Security Japan Consortium
Certified by	Japan Information Technology Security Evaluation and Certification Scheme (JISEC)

1.2 TOE Overview

The TOE is an integrated circuit with a contactless interface (with optional contact interface) and a smart card embedded software called "PT Software". The TOE is used as the public transportation IC card in Japan.

The assumed usage of the public transportation IC card is a stored fare card, a post-pay card, seasonal ticket card and one-day ticket card for public transportation. To take a train, a Passenger just taps the card to the ticket gate and the fare is automatically deducted from the card. The card can be used not only for trains but also subways and buses.

The card can be also used for other purposes such as e-money, e-ticket, ID card, and so on. The e-money services allow a person to buy something quickly at kiosk, shopping malls, vending machines, and Internet. A person can enter an event hall or his/her office by touching the e-ticket card or ID card to gates of facilities.

As these services have been widely deployed in Japan, the security of the public transportation IC card is crucial. The public transportation IC card is expected to adapt to the requirement from the Japanese transportation circumstances.

One of the important characteristics of the Japanese transportation system is that a huge number of Passengers go through the gate in rush hour. Therefore, fast processing speed is required to the public transportation IC card.

Other important aspect is a nationwide interoperation among several Public Transportation Operators. A public transportation IC card issued by one of the operators can be accepted by the other operators in the interoperation agreement. Despite the interoperation, each operator can implement its own services (e.g., discount for frequent Passengers) to its card. Therefore, the public transportation IC card shall provide flexible file system that realizes the multi-application for their services.

A Public Transportation Operator can offer Ticket Services by incorporating the public transportation IC card into a ticketing system. To set up the Ticket Services and the access rights and rules to the information in the

card, the Public Transportation Operator configures the card. This configuration work enables various Ticket Services, such as cash-purse and transport-payment solutions. Ticket Services information of multiple Public Transportation Operators can be put into a single card.

The following figure shows an example operation to provide a Ticket Service. Typical operation of the ticket gates (i.e., external entity) is as follows:

1. The ticket gate detects the card.
2. The ticket gate and the card perform mutual authentication.
3. If the mutual authentication is successfully performed, the ticket gate reads the ticket information from the card. If the ticket is valid, the ticket gate writes necessary information to the cards and then allows the Passenger to pass through the gate.

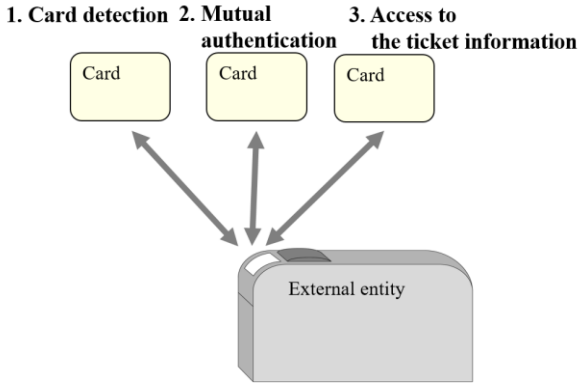


Figure 1: An example operation of the Ticket Service

The following figure illustrates the physical scope of the TOE, which is indicated in blue:

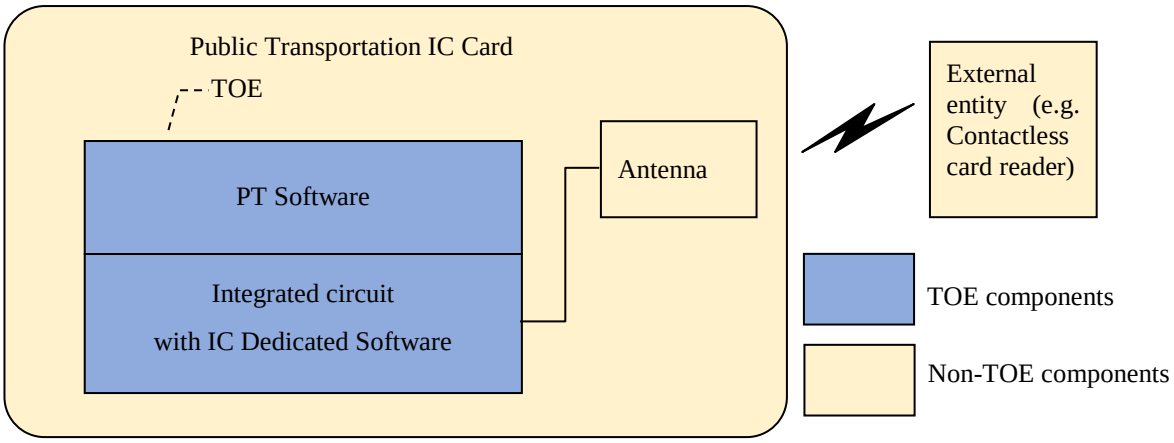


Figure 2: TOE physical scope

The components of the TOE are explained as follows:

- "PT Software" constitutes the part of the TOE that is an embedded software that provides the public transportation application and the operating system that is responsible for managing and providing access to a file system.
- "Integrated circuit with IC Dedicated Software" is a security integrated circuit which is composed of a processing unit, cryptographic co-processor, security components (e.g., security detectors, sensors and circuitry to protect the TOE), a contactless interface, an optional contact interface, and volatile and non-volatile memories. The TOE may also include IC developer/manufacturer proprietary IC Dedicated Software as long as it is delivered by the IC manufacturer. Such software is often used for testing purposes during production only but may also provide additional services to facilitate usage of the hardware and/or to provide additional services (e.g., a cryptographic library).

The TOE manages several data sets, each having a different purpose, on a single TOE. The TOE has a file system consisting of Areas and Services, which organise files in a tree structure (as shown in Figure 3).The security measures of the TOE aim at protecting the access to the Areas and Services (including associated user data), and maintaining the confidentiality and integrity of assets such as the user data and Access Key.

A Service has the Service Attribute that defines the type of access to the user data and the security condition to access the user data. If a Service requires authentication, the external entity and the TOE shall authenticate each other by using Access Key that corresponds to the Service. When the authentication is successfully completed, the TOE allows the external entity to access the user data according to the Service Attribute. This mechanism prevents unauthorised access to the user data. The summary of the access control to the user data is shown in Table 2.

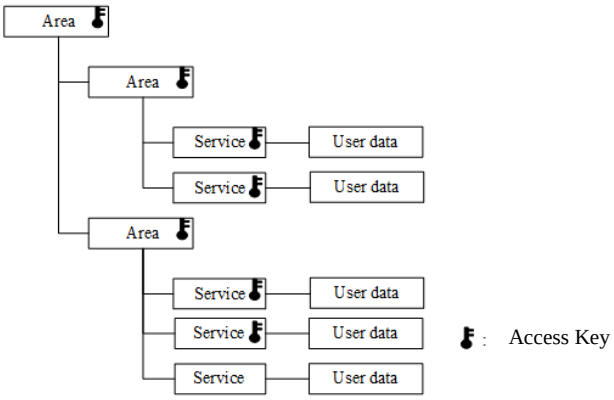


Figure 3: The file system (example)

Table 2: Level of access control to the user data

Authentication status of the external entity	Service Attribute	Operation permitted
Not authenticated	Read Only Access: authentication not required	Read user data
	Read/Write Access: authentication not required	Read/Write user data
Successfully authenticated with the Access Key corresponding to the Service	Read Only Access: authentication required	Read user data
	Read/Write Access: authentication required	Read/Write user data

An Area defines the management operation of the Area and the Service. The external entity and the TOE shall authenticate each other by using Access Key that corresponds to the Area. When the authentication is successfully completed, the TOE allows the external entity to perform the management operation (e.g., setting Service Attribute).

The TOE has several self-protection mechanisms sufficient to satisfy all requirements for self-protection, non-bypassability, and domain separation as described by the CC supporting documents for the smartcard security evaluations [AAPS].

The TOE offers the following features:

- it can receive commands from the card reader
- it can send responses to the card reader

The TOE offers the following security features:

- mutual authentication between the external entity and the TOE
- management of Services (e.g., setting Service Attribute)

- controlled access to the user data stored internally in the TOE
- trusted communication channel between the external entity and the TOE
- protection of confidentiality and/or integrity of assets stored internally in the TOE
- anti-tearing and rollback mechanism
- protection against excess environment conditions
- protection against information leakage
- protection against probing and alteration
- prevent abuse of function
- support of unique identification of the TOE

The security features are provided partly by the PT Software and partly by the underlying hardware.

The lifecycle of the TOE is explained in Section 1.3.

The assets that the TOE is expected to protect is described in Section 3.1.

The threats to be countered by the TOE, the assumptions about the TOE environment, the organisational security policies with which the TOE is designed to comply is described in Section 3.2, 3.3, and 3.4.

1.3 Lifecycle

The lifecycle of the TOE is explained using the smartcard lifecycle as defined in "Security IC Platform Protection Profile with Augmentation Packages" [BSI-PP-0084], which includes the phases listed in the following table:

Table 3: Phases of the TOE lifecycle

Phase	Description
Phase 1	IC embedded software development
Phase 2	IC development
Phase 3	IC manufacturing
Phase 4	IC packaging
Phase 5	Composite product integration
Phase 6	Personalisation
Phase 7	Operational usage

The PT Software is developed in Phase 1. The IC and IC Dedicated Software) is developed in Phase 2 and produced in Phase 3. Then the TOE can be delivered in form of wafers or sawn wafers (dice). The TOE can also be delivered in form of packaged products. In this case the corresponding assurance requirements of this Protection Profile for the development and production of the TOE not only pertain to Phase 1, 2 and 3 but to Phase 4 in addition.

In the following the term "TOE Delivery" is uniquely used to indicate

- after Phase 3 and before Phase 4 if the TOE is delivered in form of wafers or sawn wafers (dice) or

- after Phase 4 and before Phase 5 if the TOE is delivered in form of packaged products.

This Protection Profile defines assurance requirements for the TOE's development and production environment up to "TOE Delivery"

An explanation of each phase of the TOE lifecycle follows:

Phase 1: The TOE contains the PT Software, which is developed in Phase 1 by the PT Software developer.

After Phase 1, the PT Software developer delivers the PT Software and its Pre-personalisation data (if necessary) to the IC manufacturer or the IC packaging manufacturer.

Phase 2: IC development (IC design and IC Dedicated Software development) is performed by the IC developer.

After Phase 2, the IC design and the IC Dedicated Software are delivered to the IC manufacturer.

Phase 3: IC manufacturing (integration and photomask fabrication, IC production, IC testing, initialisation including injection of Initialisation Data, and Pre-personalisation if necessary) is performed by the IC manufacturer.

After Phase 3, the TOE can be delivered in form of wafers or sawn wafers (dice).

Phase 4: IC packaging (security IC packaging, IC testing and Pre-personalisation if necessary) is performed by the IC packaging manufacturer.

After Phase 4, the TOE can be delivered in form of packaged products.

Phase 5: The smartcard manufacturer integrates the TOE into its public transportation IC card product and then delivers that product to the Administrator (e.g., Public Transportation Operator).

Phase 6: The Administrator (e.g., Public Transportation Operator) performs the personalisation (issuing the TOE) where the user data, the Service Attribute and the Access Keys are loaded into the TOE memory.

Phase 7: The public transportation IC card product is delivered to Passenger for operational use.

1.4 Available non-TOE hardware/software/firmware

The TOE is used as the IC card. Operation of the TOE does not rely on other IT environment, except for power supply from an external entity.

Public Transportation Operators are required to prepare card readers depending on their purposes.

1.5 Composite Evaluation

Composite evaluation is applicable. When the hardware part of the public transportation IC card has been evaluated, the redundant evaluation may be omitted in the composite evaluation. Meanwhile, additional evaluation for the security functionality implemented by software or combination of software and hardware shall be performed. When composite evaluation is not applied, the entire public transportation IC card shall be evaluated.

2 Conformance Claims

This chapter describes the conformance claims.

2.1 CC Conformance Claim

The evaluation is based on the following:

- "Common Criteria for Information Technology Security Evaluation", Version 3.1 Release 5 (composed of Parts1-3, [CC Part 1], [CC Part 2], and [CC Part 3])
- "Common Methodology for Information Technology Security Evaluation: Evaluation Methodology", Version 3.1 [CC CEM]

This PP claims the following conformances:

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

The extended Security Functional Requirements are defined in chapter 5.

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

The minimum level of assurance is:

- Evaluation Assurance Level 5 (EAL5) augmented with ALC_DVS.2 and AVA_VAN.5

3 Security Problem Definition

The statement of the security problem describes the assets that the TOE is expected to protect and the security measures that are to be enforced by the TOE or its operational environment.

To this end, the security problem definition (this chapter) identifies and lists the following:

- primary and secondary assets
- the threats to be countered by the TOE
- the assumptions about the TOE environment
- the organisational security policies with which the TOE is designed to comply.

3.1 Assets

The assets that the TOE is expected to protect are as follows:

- the primary asset of the TOE is the user data stored in the TOE
- all the assets employed to protect confidentiality and/or integrity of the primary assets are secondary assets (such as Access Key, the PT Software, Initialisation Data and Pre-personalisation Data).

The user data that shall be protected is defined by the Administrator (e.g., Public Transportation Operator) in the personalisation phase. The TOE allows a flexible, configurable access control system, and therefore, a user data can be public or kept confidential according to access control policy.

Not all the secondary assets have to be identified and included in PPs/STs because they depend on the protection mechanism for the primary assets. The secondary assets should be identified during the TOE evaluation.

3.2 Threats

This section describes threats. The threats shall be countered by the TOE or/and its operational environment.

T.Hardware_Attack

An attacker may perform physical attacks, perturbation attacks and side channel attacks against IC chips in order to (i) disclose or manipulate the assets of the TOE or (ii) manipulate (explore, bypass, deactivate or change) security services of the TOE.

T.Logical_Attack

In the operational environment after issuing the TOE, an attacker may try to (i) disclose the assets of the TOE or (ii) alter the assets of the TOE without authentication.

T.Comm_Attack

An attacker may try to (i) disclose the assets that is sent or received through the communication channel or (ii) alter the messages on the communication channel.

T.Abuse_Func

An attacker may use functions of the TOE which may not be used after TOE delivery in order to (i) disclose or manipulate the assets of the TOE, (ii) manipulate (explore, bypass, deactivate or change) security services of the TOE, (iii) manipulate (explore, bypass, deactivate or change) functions of the TOE or (iv) enable an attack disclosing or manipulating the assets of the TOE.

3.3 Organisational Security Policies

This section describes organisational security policies that apply to TOEs and operational environment.

P.Configure

The TOE is a tool to be used by the Administrator in a system that shall implement specific business rules. The TOE shall provide the means for the level of the access control to be specified explicitly by the Administrator for each asset.

P.Identification

An accurate identification shall be established for the TOE. This requires that each instantiation of the TOE carries this unique identification.

P. TOE_Auth

TOE shall be able to authenticate the external entities and authenticate itself to the external entities.

3.4 Assumptions

This section describes assumptions to be addressed in the operational environment of the TOE. These assumptions need to be true for the effective security functionality of the TOE.

A.Process

It is assumed that security procedures are used after delivery of the TOE by the TOE manufacturer up to delivery to the Passenger to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use).

A.Keys

Access Keys for TOE use are generated outside the TOE, by the supporting system in a controlled environment. This system shall check that all such keys are suitably secure by, for example, weeding out weak keys. Access Keys are then handled correctly without misoperation. The process of key generation and management shall be suitably protected and shall be performed in a controlled environment.

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 TOE Security Objectives

The following TOE Security Objectives have been identified for the TOE, as a result of the discussion of the Security Problem Definition. Each objective is stated in bold type font. It is followed by an application note, in regular font, which provides additional information and interpretation.

O.Hardware_Attack

The TOE shall provide protection against in place to handle the physical interaction, physical manipulation and physical probing to the hardware and disclosure/reconstruction of assets while stored and/or processed in the IC chips. In addition, the TOE shall ensure its correct operation by preventing its operation outside the normal operating conditions where reliability and secure operation has not been proven or tested.

O.AC

The TOE shall be able to authenticate the external entities. And the TOE shall provide the means of controllable limited access to the objects and resources they own or are responsible for in a configurable and deterministic manner. This objective combines all aspects of authentication and access control.

O.Auth

The TOE shall be able to authenticate the external entities and authenticate itself to external entities.

O.Configure

The TOE shall provide the means of the access control to be specified explicitly set by the Administrator.

O.Comm_Attack

The TOE receives and sends the assets over a contactless interface and an optional contact interface, which is considered easy to eavesdrop or tap and alter. Therefore, the TOE shall provide secure channel that allow the TOE and an external entity to communicate with each other in a secure manner. The secure channel shall protect the confidentiality and integrity of the transferred assets.

O.Abuse_Func

The TOE shall prevent that functions of the TOE which may not be used after TOE Delivery can be abused in order to (i) disclose critical assets of the TOE, (ii) manipulate critical assets of the TOE, (iii) manipulate PT Software or (iv) bypass, deactivate, change or explore security features or security services of the TOE. Details depend, for instance, on the capabilities of the Test Features provided by the IC Dedicated Test Software which are not specified here.

O.Identification

The TOE shall provide the means to store Initialisation Data in its non-volatile memory. Initialisation Data (or parts of them) are used for TOE identification.

4.2 TOE Operational Environment Security Objectives

This section identifies the IT security objectives that are to be satisfied by the imposing of technical or procedural requirements on the TOE operational environment. Each objective is stated in bold type font; it is followed by an application note, in regular font, which supplies additional information and interpretation.

OE.TOE_Auth

The operational environment shall support the authentication verification mechanism and know authentication reference data of the TOE.

OE.Keys

Access Keys for use by the TOE are generated externally (that is, beyond control of the TOE). The generation and handling of the keys shall be performed in a secure manner.

Application note: An appropriate user guidance for key generation and handling should be defined and verified in the TOE evaluation.

OE.Process

In the TOE operational environment, confidentiality and integrity of the TOE and its manufacturing and test data shall be maintained by means of procedural measures between delivery of the TOE by the TOE manufacturer and delivery of the TOE to the Passenger.

4.3 Security Objectives Rationale

This section demonstrates the suitability of the choice of security objectives and that the stated security objectives counter all identified threats, policies, or assumptions.

The following table maps the security objectives to the security problem, which is defined by the relevant threats, policies, and assumptions. This illustrates that each threat, policy, or assumption is covered by at least one security objective.

Table 4: Assumptions, Threats or Policies versus Security Objectives defined in the PP

Threat, policy or assumption	Objective
T.Hardware_Attack	O.Hardware_Attack
T.Logical_Attack	O.AC
T.Comm_Attack	O.Comm_Attack
T.Abuse_Func	O.Abuse_Func
P. TOE_Auth	O.Auth
	OE.TOE_Auth
P.Identification	O.Identification
P.Configure	O.Configure
A.Keys	OE.Keys
A.Process	OE.Process

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

O.Hardware_Attack and O.Abuse_Func objectives (refer to Table 4) directly correspond to the description of the threats. It is clear from the description of each objective, that the corresponding threat is removed if the objective is valid.

The O.AC objective makes sure that the TOE can authenticate the external entities and implements an access control system that protects the stored assets from unauthorised access. Thus, T.Logical_Attack threat is mitigated if the objective is valid.

The O.Configure objective provides the capability to configure the access rules and operations for the authorised User and Administrator. Thus, the P.Configure policy is covered by the objective.

The P.TOE_Auth policy is covered by the O.Auth objective describing the proving part of the authentication and the OE.TOE_Auth operational environment the verifying part of the authentication. Thus, the P.TOE_Auth policy is covered by the objectives.

The O.Comm_Attack objective provides a secure channel that shall be established between the TOE and an external entity; this secure channel shall protect all the transferred assets from disclosure and from integrity errors, whether as a result of an attack or environmental conditions (such as loss of power). Thus, the T.Comm_Attack threat is mitigated if the objective is valid.

The O.Identification objective requires that the TOE has to support the possibility of a unique identification. The unique identification can be stored on the TOE. Since the unique identification is generated by the production environment the production environment shall support the integrity of the generated unique identification. The technical and organisational security measures that ensure the security of the development environment and production environment are evaluated based on the assurance measures that are part of the evaluation. Therefore, the P.Identification policy is covered by this objective, as far as organisational measures are concerned.

The OE.Keys and the OE.Process operational environments directly correspond to the description of the A.Keys and A.Process assumptions, thus these assumptions are met.

5 Extended Components Definitions

The PP defines the following extended components.

- FDP_SDC.1 Stored data confidentiality
- FMT_LIM.1 Limited capabilities
- FMT_LIM.2 Limited availability
- FAU_SAS.1 Audit storage

5.1 Definition of the Family FDP_SDC

To define the security functional requirements of the TOE an additional family (FDP_SDC.1) of the Class FDP (user data protection) is defined here.

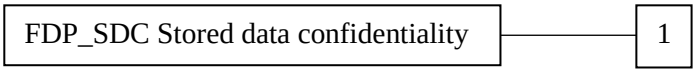
The family “Stored data confidentiality (FDP_SDC)” is specified as follows.

FDP_SDC Stored data confidentiality

Family behaviour

This family provides requirements that address protection of user data confidentiality while these data are stored within memory areas protected by the TSF. The TSF provides access to the data in the memory through the specified interfaces only and prevents compromise of their information bypassing these interfaces. It complements the family stored data integrity (FDP_SDI) which protects the user data from integrity errors while being stored in the memory.

Component levelling



FDP_SDC.1 Requires the TOE to protect the confidentiality of information of the user data in specified memory areas.

Management: FDP_SDC.1

There are no management activities foreseen.

Audit: FDP_SDC.1

There are no actions defined to be auditable.

FDP_SDC.1 Stored data confidentiality

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SDC.1.1 **The TSF shall ensure the confidentiality of the information of the user data while it is stored in the [assignment: memory area].**

5.2 Definition of the Family FMT_LIM

To define the IT security functional requirements of the TOE an additional family (FMT_LIM) of the Class FMT (Security Management) is defined here. This family describes the functional requirements for the Test Features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE (refer to Section 6.1) appropriate to address the specific issues of preventing the abuse of functions by limiting the capabilities of the functions and by limiting their availability.

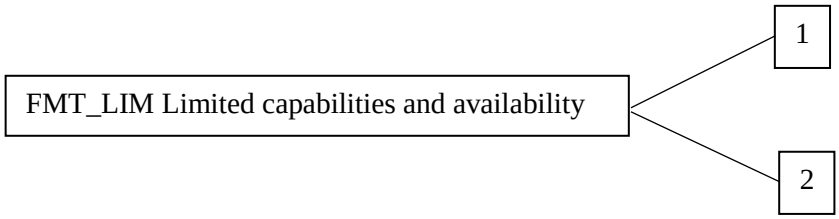
The family "Limited capabilities and availability (FMT_LIM)" is specified as follows.

FMT_LIM Limited capabilities and availability

Family behaviour

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note that FDP_ACF restricts the access to functions whereas the component Limited Capability of this family requires the functions themselves to be designed in a specific manner.

Component levelling



FMT_LIM.1 Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.

FMT_LIM.2 Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.

Management: FMT_LIM.1, FMT_LIM.2

There are no management activities foreseen.

Audit: FMT_LIM.1, FMT_LIM.2

There are no actions defined to be auditable.

The TOE Functional Requirement "Limited capabilities (FMT_LIM.1)" is specified as follows.

FMT_LIM.1 Limited capabilities

Hierarchical to: No other components.

Dependencies: FMT_LIM.2 Limited availability.

FMT_LIM.1.1 **The TSF shall be designed and implemented in a manner that limits its capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced [assignment: Limited capability policy].**

The TOE Functional Requirement "Limited availability (FMT_LIM.2)" is specified as follows.

FMT_LIM.2 Limited availability

Hierarchical to: No other components.

Dependencies: FMT_LIM.1 Limited availability.

FMT_LIM.2.1 **The TSF shall be designed in a manner that limits its availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced [assignment: Limited availability policy].**

Application note: The functional requirements FMT_LIM.1 and FMT_LIM.2 assume that there are two types of mechanisms (limitation of capabilities and limitation of availability) which together shall provide protection in order to enforce the same policy or two mutual supportive policies related to the same functionality. This allows e.g. that

(i) the TSF is provided without restrictions in the product in its user environment but its capabilities are so limited that the policy is enforced or conversely

(ii) the TSF is designed with high functionality but is removed or disabled in the product in its user environment.

5.3 Definition of the Family FAU_SAS

To define the security functional requirements of the TOE an additional family (FAU_SAS) of the Class FAU (Security Audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

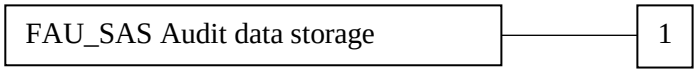
The family "Audit data storage (FAU_SAS)" is specified as follows.

FAU_SAS Audit data storage

Family behaviour

This family defines functional requirements for the storage of audit data.

Component levelling



FAU_SAS.1 Requires the TOE to provide the possibility to store audit data.

Management: FAU_SAS.1

There are no management activities foreseen.

Audit: FAU_SAS.1

There are no actions defined to be auditable.

FAU_SAS.1 Audit storage

Hierarchical to: No other components.

Dependencies: No dependencies.

FAU_SAS.1.1 **The TSF shall provide [assignment: list of subjects] with the capability to store [assignment: list of audit information] in the [assignment: type of persistent memory].**

6 IT Security Requirements

IT security requirements include the following:

- Security functional requirements (SFRs)
  That is, requirements for security functions such as information flow control, identification and authentication.
- Security assurance requirements (SARs)
  Provide grounds for confidence that the TOE meets its security objectives (such as configuration management, testing, vulnerability assessment.)
- This chapter discusses these requirements in detail. It also explains the rationales behind them, as follows:
  - Security functional requirements rationale
  - Security assurance requirements rationale

6.1 Security Functional Requirements for the TOE

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

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

- The refinement operation is used in many cases, to make the requirements easier to read and understand.
- Selections having been made by the PP author are denoted as underlined text. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made [selection:] and are *italicised*.
- Assignments having been made by the PP author are denoted by showing as **underlined text and bold**. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:] and are *italicised*. In some cases the assignment made by the PP authors defines a selection to be performed by the ST author. Thus this text is *underlined and italicised* like this.

FDP_SDC.1 Stored data confidentiality

FDP_SDC.1.1 The TSF shall ensure the confidentiality of the information of the user data while it is stored in the [assignment: *memory area*][1].

Application note: The ST author should assign a secure memory to the memory area, in general ROM is not considered as the secure memory.

FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [assignment: *integrity errors*][2] on all objects, based on the following attributes: [assignment: *user data attributes*][3].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [assignment: *action to be taken*][4].

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist **physical manipulation and physical probing**[5] to the **hardware of the TOE and software composing the TSF**[6] by responding automatically such that the SFRs are always enforced.

[1] [assignment: memory area]
[2] [assignment: integrity errors]
[3] [assignment: user data attributes]
[4] [assignment: action to be taken]
[5] [assignment: physical tampering scenarios]
[6] [assignment: list of TSF devices/elements]

Refinement: The TSF will implement appropriate mechanisms to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TSF can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that security functional requirements are enforced. Hence, "automatic response" means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

FDP_ITT.1 Basic internal transfer protection

FDP_ITT.1.1 The TSF shall enforce the **Data Processing Policy**[7] to prevent the disclosure[8] of user data when it is transmitted between physically-separated parts of the TOE.

Refinement: The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as physically-separated parts of the TOE.

FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure[9] when it is transmitted between separate parts of the TOE.

Refinement: The different memories, the CPU and other functional units of the TOE (e.g. a cryptographic co-processor) are seen as separated parts of the TOE.

FDP_IFC.1 Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the **Data Processing Policy**[10] on **all confidential data when they are processed or transferred by the TOE**[11].

Application Note: The ST author should define Data Processing Policy in the ST as follows:

The following Security Function Policy (SFP) Data Processing Policy is defined for the requirement "Subset information flow control (FDP_IFC.1)":

"User data of the TOE and TSF data shall not be accessible from the TOE except when PT Software decides to communicate the user data of the TOE via an external interface. The protection shall be applied to confidential data only but without the distinction of attributes controlled by PT Software."

FRU_FLT.2 Limited fault tolerance

FRU_FLT.2.1 The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: **exposure to operating conditions which are not detected according to the requirement Failure with preservation of secure state (FPT_FLS.1)**[12].

Refinement: The term "failure" above means "circumstances". The TOE prevents failures for the "circumstances" defined above.

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: **exposure to operating conditions which may not be tolerated according to the requirement Limited fault tolerance (FRU_FLT.2) and where therefore a malfunction could occur**[13].

Refinement: The term "failure" above also covers "circumstances". The TOE prevents failures for the "circumstances" defined above.

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 assured identification of its end points and protection of the channel data from modification or disclosure.

---

[7] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[8] [selection: disclosure, modification, loss of use]
[9] [selection: disclosure, modification]
[10] [assignment: information flow control SFP]]
[11] [assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP]
[12] [assignment: list of type of failures]
[13] [assignment: list of types of failures in the TSF]

FTP_ITC.1.2 The TSF shall permit another trusted IT product[14] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: *list of functions for which a trusted channel is required*][15].

Application note: The trusted channel can be realised by a communication using cryptography. When the cryptographic key is generated by the TOE, a random number generator according to the strength of the cryptographic algorithm may be required.

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **User and Administrator**[16].

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

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow **Polling, Public_read, Public_write and** [selection: *[assignment: other list of TSF mediated actions], none*][17] 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.

Application note: The ST author should not assign the TSF mediated actions that requires identification and authentication.

Application note: Polling is an action to detect a card. Public_read is a read operation to the user data files that do not require authentication. Public_write is a write operation to the user data files that do not require authentication.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow **Polling, Public_read, Public_write and** [selection: *[assignment: other list of TSF mediated actions], none*][18] 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.

Application note: The ST author should not assign the TSF mediated actions that requires authentication.

Application note: Polling is an action to detect a card. Public_read is a read operation to the user data files that do not require authentication. Public_write is a write operation to the user data files that do not require authentication.

FIA_UAU.4 Single-use authentication mechanisms

FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [assignment: *identified authentication mechanism(s)*]][19].

Application note: The ST author should not assign the authentication mechanism that is not recognised as a strong authentication in general. The authentication mechanism can use a cryptographic algorithm. A random number generator may be required for the authentication data.

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **Service Access Policy**[20] on:[21]

- **Subjects: subjects shown in Table 5**

[14] [selection: the TSF, another trusted IT product]
[15] [assignment: list of functions for which a trusted channel is required]
[16] [assignment: the authorised identified roles]
[17] [assignment: list of TSF-mediated actions]
[18] [assignment: list of TSF mediated actions]
[19] [assignment: identified authentication mechanism(s)]
[20] [assignment: access control SFP]
[21] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

- **Objects: objects shown in Table 5**
- **Operations: operations shown in Table 5**

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **Service Access Policy**[22] to objects based on:[23]

- **Subjects: subjects shown in Table 5**
- **Objects: objects shown in Table 5**
- **SFP relevant security attributes for each subject and object: security attribute authentication status and security attribute ACL shown in Table 5**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:[24]

- **A Subject can do this operation on an Object when: the Subject is successfully authenticated, and the operation is listed in Table 5.**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*][25].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*][26].

Application note: To specify more than one access control policy, FDP_ACC.1 and FDP_ACF.1 can be iterated multiple times in a ST to different subsets of subjects, operations and objects.

Table 5: Service Access Policy

Subject	Security attribute Authentication status	Object	Security attribute ACL	Operation
Process representing User	Not authenticated	User data file	Read only, Authentication not required	Read
			Read/Write, Authentication not required	Read or Write
	Successfully authenticated with the Access Key corresponding to the Service	User data file	Read only, Authentication with the Access Key corresponding to the Service required	Read
			Read/Write, Authentication with the Access Key corresponding to the Service required	Read or Write

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **Service Access Policy**[27] to restrict the ability to **set and** [selection: *[assignment: other operations], none*][28] the security attributes **ACL**[29] to **Administrator**[30].

[22] [assignment: access control SFP]
[23] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]
[24] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[25] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[26] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[27] [assignment: access control SFP(s), information flow control SFP(s)]
[28] [selection: change_default, query, modify, delete, [assignment: other operations]]

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **management of security attributes**[31].

FMT_LIM.1 Limited capabilities

FMT_LIM.1.1 The TSF shall be designed and implemented in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: **Deploying Test Features after TOE Delivery does not allow user data of the TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks**[32].

FMT_LIM.2 Limited availability

FMT_LIM.2.1 The TSF shall be designed and implemented in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: **Deploying Test Features after TOE Delivery does not allow user data of the TOE to be disclosed or manipulated, TSF data to be disclosed or manipulated, software to be reconstructed and no substantial information about construction of TSF to be gathered which may enable other attacks**[33].

FAU_SAS.1 Audit storage

FAU_SAS.1.1 The TSF shall provide the **test process before TOE Delivery**[34] with the capability to store **Initialisation Data and** [selection: *[assignment: other data], none*][35] in the [assignment: *type of persistent memory*][36].

[29] [assignment: list of security attributes]
[30] [assignment: the authorised identified roles]
[31] [assignment: list of management functions to be provided by the TSF]
[32] [assignment: Limited capability policy]
[33] [assignment: Limited availability policy]
[34] [assignment: list of subjects]
[35] [assignment: list of audit information]
[36] [assignment: type of persistent memory]

6.2 Security Assurance Requirements for the TOE

The Security Assurance Requirements for the TOE are those taken from the Evaluation Assurance Level 5 (EAL5) and augmented by taking the components ALC_DVS.2 and AVA_VAN.5. The assurance requirements are shown in the following table.

Table 6: Assurance components

Assurance class	Assurance components
Development	ADV_ARC.1
	ADV_FSP.5
	ADV_IMP.1
	ADV_INT.2
	ADV_TDS.4
Guidance documents	AGD_OPE.1
	AGD_PRE.1
Life-cycle support	ALC_CMC.4
	ALC_CMS.5
	ALC_DEL.1
	ALC_DVS.2
	ALC_LCD.1
	ALC_TAT.2
Security Target evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Tests	ATE_COV.2
	ATE_DPT.3
	ATE_FUN.1
	ATE_IND.2
Vulnerability assessment	AVA_VAN.5

6.3 Security Functional Requirements Rationale

The following table presents both the rationale for choosing specific Security Functional Requirements (SFRs) and how those requirements correspond to the specific Security Objectives:

Table 7: TOE Security Functional Requirements versus Security Objectives

Objective	TOE Security Functional Requirements
O.Hardware_Attack	- FDP_SDC.1 “Stored data confidentiality”
	- FDP_SDI.2 “Stored data integrity monitoring and action”
	- FPT_PHP.3 “Resistance to physical attack”
	- FDP_ITT.1 “Basic internal transfer protection”
	- FPT_ITT.1 “Basic internal TSF data transfer protection”
	- FDP_IFC.1 “Subset information flow control”
	- FRU_FLT.2 “Limited fault tolerance
	- FPT_FLS.1 “Failure with preservation of secure state”
O.AC	- FIA_UID.1 “Timing of identification”
	- FIA_UAU.1 “Timing of authentication”
	- FIA_UAU.4 “Single-use authentication mechanisms”
	- FDP_ACC.1 “Subset access control
	- FDP_ACF.1 “Security attribute based access control”
O.Auth	- FIA_UID.1 “Timing of identification”
	- FIA_UAU.1 “Timing of authentication”
	- FIA_UAU.4 “Single-use authentication mechanisms”
	- FTP_ITC.1 “Inter-TSF trusted channel”
O.Configure	- FMT_SMR.1 “Security roles”
	- FMT_MSA.1 “Management of security attributes”
	- FMT_SMF.1 “Specification of Management Functions”
O.Comm_Attack	- FTP_ITC.1 “Inter-TSF trusted channel”
O.Abuse_Func	- FMT_LIM.1 “Limited capabilities”
	- FMT_LIM.2 “Limited availability”
O.Identification	- FAU_SAS.1 “Audit storage”

The objective O.Hardware_Attack states that the TOE shall provide protection against measuring the physical interaction which is achieved by the SFRs FDP_ITT.1, FPT_ITT.1 and FDP_IFC.1 by protecting user data and TSF data in processing and internal transfer even if the information leakage is not inherent but caused by the attacker. The protection against physical manipulation and physical probing to the hardware is achieved by the SFR FPT_PHP.3. The protection against disclosure/reconstruction of user data while stored in the memory is achieved by the SFRs FDP_SDC.1 and FDP_SDI.2 supported by the SFR FPT_PHP.3. Finally, to prevent malfunction is covered by the SFR FRU_FLT.2 that requires fault tolerance in failures, and by the SFR FPT_FLS.1 that preserves a secure state in failures.

The objective O.AC is achieved through the SFRs FDP_ACC.1 and FDP_ACF.1, which together specify the access control policy. The operation of the access control system is supported by the SFR FIA_UAU.4 to make sure that unique authentication sessions shall be used every time. The SFRs FIA_UID.1 and FIA_UAU.1 complement the access control system operation by allowing very specific functions to be used without authentication.

The objective O.Auth is achieved by the SFRs FTP_ITC.1, FIA_UAU.4, FIA_UID.1 and FIA_UAU.1 which provide mutual authentication on the secure channel between the TOE and the external entity

The objective O.Configure is achieved by the SFRs FMT_SMR.1 and FMT_MSA.1 in conjunction with the SFR FMT_SMF.1 allow for the implementation of a flexible, configurable access control system and specify the roles that shall be allowed to utilise the access control system configuration capabilities.

The objective O.Comm_Attack is directly realised through the requirement for the secure channel the SFR FTP_ITC.1 between the TOE and the external device.

The objective O.Abuse_Func is achieved by the SFRs FMT_LIM.1 and FMT_LIM.2 because the limitation of availability and capability of functions after the TOE delivery prevents an attacker from abusing functions.

The objective O.Identification is achieved by the SFR FAU_SAS.1. Initialisation Data (or parts of them) are used for TOE identification. The technical capability of the TOE to store Initialisation Data is provided according to the SFR FAU_SAS.1.

The following table presents the list of the SFRs with the associated dependencies.

Table 8: Security Functional Requirements dependencies

ID	SFR	Dependencies	Notes
FDP_SDC.1	Stored data confidentiality	None	
FDP_SDI.2	Stored data integrity monitoring and action	None	
FPT_PHP.3	Resistance to physical attack	None	
FDP_ITT.1	Basic internal transfer protection	FDP_ACC.1 or FDP_IFC.1	Included (FDP_IFC.1)
FPT_ITT.1	Basic internal TSF data transfer protection	None	
FDP_IFC.1	Subset information flow control	FDP_IFF.1	Not satisfied (See discussion below)
FRU_FLT.2	Limited fault tolerance	FPT_FLS.1	Included
FPT_FLS.1	Failure with preservation of secure state	None	
FMT_SMR.1	Security roles	FIA_UID.1	Included
FIA_UID.1	Timing of identification	None	
FIA_UAU.1	Timing of authentication	FIA_UID.1	Included
FIA_UAU.4	Single-use authentication mechanisms	None	
FDP_ACC.1	Subset access control	FDP_ACF.1	Included
FDP_ACF.1	Security attribute based access control	FDP_ACC.1 FMT_MSA.3	Included Not satisfied (See discussion below)
FMT_MSA.1	Management of security attributes	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1 FMT_SMF.1	Included (FDP_ACC.1) Included Included
FMT_SMF.1	Specification of Management Functions	None	
FTP_ITC.1	Inter-TSF trusted channel	None	
FMT_LIM.1	Limited capabilities	FMT_LIM.2	Included
FMT_LIM.2	Limited availability	FMT_LIM.1	Included
FAU_SAS.1	Audit storage	None	

Part 2 of the Common Criteria defines the dependency of FDP_IFC.1 (information flow control policy statement) on FDP_IFF.1 (Simple security attributes). The specification of FDP_IFF.1 would not capture the nature of the security functional requirement nor add any detail. As stated in the Data Processing Policy referred to in FDP_IFC.1 there are no attributes necessary. The information flow is not controlled by security attributes and not used as the covert channel. Therefore, there is no need to include the SFR FDP_IFF.1 in the PP. The security functional requirement for the TOE is sufficiently described using FDP_ITT.1 and its Data Processing Policy (FDP_IFC.1).

The SFR “FMT_MSA.3 Static attribute initialisation” is a dependency for the SFR FDP_ACF.1. In the TOE, however, the security attributes are always explicitly set and the notion of “default value” for a security attribute simply does not exist. The security attributes are always set explicitly by the Administrator to a value appropriate for each asset without exception, so it is our opinion that the system is no less secure in the absence of the SFR FMT_MSA.3. Therefore, there is no need to include the SFR FMT_MSA.3 in the PP.

6.4 Security Assurance Requirements Rationale

To meet the assurance expectations of Public Transportation Operators, the assurance level EAL5 and the augmentation with the requirements ALC_DVS.2 and AVA_VAN.5 are chosen. The assurance level of EAL5 and the augmentation with the requirements ALC_DVS.2 and AVA_VAN.5 is selected because it provides a sufficient level of assurance for this type of TOE, which is expected to be not only highly resistant for protecting

high value assets but also highly reliable as a part of public transportation system, which is an important infrastructure. 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 assets.

- AVA_VAN.5 Advanced methodical vulnerability analysis:

  The TOE might be in danger of high-level attacks such as those it might encounter in malicious laboratories. Therefore, AVA_VAN.5 is augmented to confirm that TOE has a high level of resistance against such attacks.

The dependencies of SARs added to EAL5 are described in [CC Part 3]. The following table gives their dependencies and how they are satisfied.

Table 9: Security Assurance Requirements dependencies added to EAL5

ID	SFR	Dependencies	Notes
ALC_DVS.2	Sufficiency of security measures	None	
AVA_VAN.5	Advanced methodical vulnerability analysis	ADV_ARC.1	Dependencies are covered by the assurance components of EAL5 (ADV_ARC.1, ADV_FSP.5, ADV_TDS.4, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1 and ATE_DPT.3).
		ADV_FSP.4	
		ADV_TDS.3	
		ADV_IMP.1	
		AGD_OPE.1	
		AGD_PRE.1	
		ATE_DPT.1	

7 Glossary and References

This chapter explains the terms, definitions and literary references (bibliography) used in this document. The list entries in this chapter are ordered alphabetically.

7.1 Terms and Definitions

The following list defines the product-specific terms used in this document:

Administrator

An entity responsible for personalisation of the TOE. In most cases, a Public Transportation Operator is a representative example of Administrator.

Access Key

A key that corresponds to an Area and a Service.

Area

A part of the file system. An Area is similar to a directory in a general file system.

Card reader

A contactless and an optional contact smartcard Reader/Writer that interacts with the TOE.

IC Dedicated Software

IC proprietary software embedded in a security integrated circuit and developed by the IC developer (if necessary). Such software is required for testing purpose but may provide additional services to facilitate usage of the hardware and/or to provide additional services.

Initialisation Data

Initialisation Data defined by the IC manufacturer to identify the TOE and to keep track of the IC's production and further life-cycle phases are considered as belonging to the TSF data.

Passenger

A person who uses Ticket Service.

Pre-personalisation Data

Any data supplied by the PT Software developer that is injected into the non-volatile memory by the IC manufacturer or the IC packaging manufacturer.

PT Software

An embedded software that provides the public transportation application and the operating system.

Public Transportation Operator

An entity that provides a specific service to a Passenger.

Service

The part of the file system that contains information that stipulates the method of access to data. In this context, a Service is similar to a file in a general file system.

Service Attribute

An attribute that defines the type of access to the user data via Service.

Ticket Service

A specific service to a Passenger that is made technically possible by the TOE. Each Ticket Service is provided by a Public Transportation Operator to a Passenger.

User

An entity using any Service and Area that a personalised TOE offers. A ticket gate is a representative example of User. See also Administrator.

7.2 Acronyms

The following table lists and defines the product-specific abbreviated terms (acronyms) that appear in this document:

Table 10: Abbreviated terms and definitions

Term	Definition
ACL	Access Control List
CC	Common Criteria
OS	Operating System
PP	Protection Profile
RF	Radio Frequency
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

7.3 Bibliography

The following list defines the literature referenced in this document:

[AAPS] “Joint Interpretation Library Application of Attack Potential to Smartcards”, Version 2.9, January 2013

[BSI-PP-0084] "Security IC Platform Protection Profile with Augmentation Packages", Version 1.0, January 2014

[CC Part 1] "Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model", Version 3.1, Revision 5, April 2017

[CC Part 2] "Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components", Version 3.1, Revision 5, April 2017

[CC Part 3] "Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components", Version 3.1, Revision 5, April 2017

[CC CEM] "Common Methodology for Information Technology Security Evaluation: Evaluation Methodology", Version 3.1, Revision 5, April 2017

Public Transportation IC Card Protection Profile

Version 1.12

Japan ID Connect with Secure Authentication Promotional association

 Printed in Japan