Federal Office
for Information Security

Common Criteria Protection Profile Configurations

Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au)

Protection Profile-Module CSP Time Stamp Service and Audit (PPM-TS-Au)

BSI-CC-PP-0107-2019

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn

Internet: https://www.bsi.bund.de

Table of Contents

Figures

Tables

1 Introduction

This document consists of the following parts:

- chapter 2 defines the Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au)
- chapters 3 to 9 defines the Protection Profile Module Time Stamp Service and Audit for CSP

2 PP-Configuration CSP-TS-Au

2.1 Reference

This PP-Configuration is identified as

Title: Cryptographic Service Provider – Time Stamp Service and Audit (PPC-CSP-TS-Au)

Version: 0.9.5, as of April 8th 2019

Registration: BSI-CC-PP-0107-2019

2.2 Components Statement

This PP-Configuration PPC-CSP-TS-Au has one single Base-PP:

Title: Cryptographic Service Provider (PP CSP)

Version: 0.9.8

Registration: BSI-CC-PP-0104-2019

This PP-Configuration consists of the Base-PP together with the PP-Module

Title: Protection Profile-Module CSP Time Stamp Service and Audit

Version: 0.9.5

described in chapter 3 to 9 of this document.

2.3 Conformance Statement

This PP -Configuration requires strict conformance of any ST or PP claiming conformance to this PP.

2.4 Conformity to Security Assurance Requirements

This PP-Configuration inherits conformity to SAR requirements from its Base-PP CSP: Assurance package EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.

3 PP-Module Introduction

3.1 PP-Module Reference

Title:	Common Criteria Protection Profile Module Cryptographic Service Provider - Time Stamp Service and Audit
Sponsor:	BSI
CC Version:	3.1 Revision 5
General Status:	Final
Version Number:	0.9.5
Registration:	-
Keywords:	cryptographic service provider, time stamp service

3.2 Base-PP Identification

The PP-module requires

– the Protection Profile Cryptographic Service Provider (PP CSP), BSI-CC-PP-0104-2019 [PP CSP]

3.3 TOE overview

TOE type

The Target of Evaluation (TOE) is a cryptographic service provider (CSP) component.

TOE definition

The TOE is physically defined as a device consisting of hardware, firmware and software. The TOE provides additional TOE security functionality (TSF) with respect to the TSF of the Base-PP [PP-CSP] in order to enable time service, time stamp service and security audit.

The *time service* allows the user to query the internal time of the TSF.

The *time stamp service* provides evidence that user data were presented to the TSF and exported audit data were generated at certain point in time and in a verifiable sequence. The validity of these user data and audit records can be verified.

The *audit* functionality generates audit records on selected user activities controlled by the TSF and security events of the TOE defined by the Base-PP and the PP-Module. The *Administrator* role (cf. the Base-PP for definition of the roles) may be split in an additional role *Auditor and Timekeeper.*

- *The Auditor* is allowed to configure the audit functionality, review audit data and export audit trails.
- *The Timekeeper* is allowed to adjust the internal clock.

Neither of those roles is allowed to manage cryptographic keys, users and update code packages.

Method of use

The TOE provides time service and time stamp service as additional method of use compared with those of the TOE defined in the Base-PP. The time service provides users with reliable time as known to the TOE. The time stamp service provides evidence some user data are provided to the TOE at given point in time. The

security audit can be used to make the user responsible for their actions including those described in the Base-PP. The audit records can be exported in a signed and time stamped form.

Life cycle

The life cycle of the TOE is the same as of the TOE defined in the Base-PP.

Non-TOE hardware/software/firmware available to the TOE

The TOE does not need non-TOE hardware, firmware or software to run.

4 Consistency rationale

This section analyses the consistency of the TOE type, the security problem definition (SPD), security objectives and security functional requirements (SFR) of the Base-PP with those of this PP-Module.

4.1 Consistency rationale with Base-PP CSP

4.1.1 TOE type

The TOE type is exactly the same as the TOE type in the Base-PP CSP: cryptographic service provider (CSP) component. The TOE provides additionally to the TSF in the Base-PP CSP the cryptographic security service for time stamps, the non-cryptographic time service and the security audit.

4.1.2 Security problem definition (SPD)

Threats

This PP-Module does not add threats compared to the SPD of the Base PP CSP.

Organizational Security Policies

Compared to the SPD of the Base-PP CSP this PP-Module adds new organizational security policies OSP.TimeService and OSP.Audit.

The OSP.TimeService “Time Service and Time stamp service” addresses the additional non-cryptographic time service and cryptographic time stamp service.

The OSP.Audit “Audit for key management and cryptographic operations” addresses the security auditing related to activities controlled by the TSF as defined in the Base-PP and the PP-Module and security critical events.

Assumptions

This PP-Module does not add assumptions compared to the SPD of the Base-PP CSP.

4.1.3 Security Objectives

The PP-Module adds new security objectives for the TOE O.TimeService and O.Audit. The security objective O.TimeService implements the OSP.TimeService by means of additional security services. The security objective O.Audit implements the OSP.Audit by means of security audit functionality that is outside of the scope of the Base-PP.

The PP-Module adds new security objectives for the operational environment OE.Audit and OE.TimeSource in order to provide security measures necessary to support new security services and the audit functionality. OE.Audit ensure the regular audit review and the availability of exported audit records. OE.TimeSource ensure the availability of reliable external time stamps for adjustment of TOE internal time source.

4.1.4 Security Functional Requirements

The Module-PP adds the following new SFRs compared to the Base-PP:

FAU_GEN.1, FAU_STG.1, FAU_STG.3, FDP_ACF.1/TS, FDP_DAU.2/TS, FDP_ETC.2/TS, FDP_ITC.2/TS, FMT_MTD.1/Audit, FMT_MOF.1/TSA, FMT_SMF.1/TSA, FMT_SMR.1/TSA, FPT_STM.1, FPT_TIT.1/Audit

These SFRs concern exclusively Time-Stamps and the Audit mechanism. These functionalities are not addressed in the Base-PP. Therefore the SFRs do not lead to any inconsistency.

4.1.5 Conclusion

In summary, the PP-Module adds TSF to the TSF required in the Base-PP CSP.

5 Conformance claims

5.1 CC conformance claims

The PP-Module claims conformance to CC version 3.1 Revision 5.

Conformance of this PP-Module with respect to CC Part 2 [CC2] (security functional components) is CC Part 2 extended.

Conformance of this PP-Module with respect to CC Part 3 [CC3] (security assurance components) is CC Part 3 conformant.

The PP-Configuration (PPC-CSP-TS-Au), consisting of the Base-PP “Cryptographic Service Provider (PP CSP)” and the PP-Module “CSP Time Stamp Service and Audit”, claims conformance to CC version 3.1 Revision 5.

Conformance of this PP-Configuration with respect to CC Part 2 [CC2] (security functional components) is CC Part 2 extended.

Conformance of this PP-Configuration with respect to CC Part 3 [CC3] (security assurance components) is CC Part 3 conformant.

The

- Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 5 [CC4]

has to be taken into account.

The PP-Module does not claim conformance to any security functional requirements package.

5.2 Conformance rationale

This chapter is not applicable because the PP-Module does not claim conformance to any PP or security functional requirements package.

5.3 Conformance statement

The PP-Module inherits the conformance statement of the Base-PP [PP-CSP] it is used with in the PP-Configuration, i.e. security targets and protection profiles claiming conformance to this PP-Module at hand must conform with **strict** conformance.

6 Security problem definitions

6.1 Introduction

Assets

The assets of the TOE are

– user data and time stamps shall be integrity protected,

– time services which time base shall be protected against manipulation.

The cryptographic keys are TSF data because they are used for cryptographic time stamp operations protecting user data and audit records, and the enforcement of the SFR relies on these data for the operation of the TOE. The audit records are TSF data generated by the TSF and exported to the user.

Subjects

The TOE knows subjects as defined in the Base-PP. They obtain their associated security attributes by the TSF defined in the Base-PP. The security attributes of subjects known to the TOE are defined in the Base-PP

– *User Identity* (User-ID),

– *Role*.

Objects

User data objects of the time stamp service are imported, used in time stamp operation, exported and destroyed after use. TSF data objects time and time stamps are created, temporarily or permanently stored, imported, exported and destroyed as objects of the security management. Cryptographic keys used by the time stamp service are TSF data objects of the key management as described in the Base-PP.

Security attributes

The role *Administrator* defined in the Base-PP may be split in more detailed roles. One of these roles may be

- *Auditor*: role that is allowed to configure the audit functionality, review audit data and export audit trails.
- *The Timekeeper* is allowed to adjust the internal time.

Cryptographic keys used for the time stamp service and the export of audit records have at least the security attributes

– *Key identity* that uniquely identifies the key,

– *Key entity*, i. e. the identity of the entity this key is assigned to,

– *Key type*, i. e. as secret key, private key, public key,

– *Key usage type*, identifying the cryptographic mechanism or service the key can be used for, where the keys for time stamp service (cf. FDP_DAU.2/TS) have the key usage type "*TimeStamp*",

and may have the security attribute

– *Key usage counter,* i. e. the number of operations performed with this key, where the key usage counter of the private key used for time stamp service counts the number of created signature

– *Key validity time period*, i. e. the time period for operational use of the key; the key must not be used before or after this time slot.

6.2 Threats

The PP-Module does not define threats additional to those defined in the Base-PP.

6.3 Organisational security policies

The PP-Module defines the following organisational security policies additional to those defined in the Base-PP.

OSP.Audit Audit for key management and cryptographic operations
The TOE provides security auditing related to activities controlled by the TSF and security critical events. The security auditing provides evidence to make users responsible for actions they are authorized for and to protect users against unwarranted accusation. The Administrator is allowed to select auditable events.

OSP.TimeService Time Service and Time stamp service
The TOE provides non-cryptographic time service and cryptographic time stamp service for user data and TSF data. The time stamp service provides evidence that user data were presented to the TSF and exported audit data were generated at certain point in time and in a verifiable sequence.

6.4 Assumptions

The PP-Module does not define assumptions additional to those defined in the Base-PP.

7 Security objectives

7.1 Security objectives for the TOE

O.Audit Audit
The TSF provides security auditing of selected user activities controlled by the TSF and security critical events. The Administrator is allowed to select auditable events, to manage the audit functionality and the export of audit records.

O.TimeService Time services
The TOE provide an internal time service and time stamp service for the user.

7.2 Security objectives for the operational environment

OE.Audit Review and availability of audit records
The Administrator shall ensure the regular audit review and the availability of exported audit records.

OE.TimeSource External time source
The operational environment provides reliable external time source for the adjustment of the TOE internal time source.

7.3 Security objective rationale

The following table traces the security objectives for the TOE back to threats countered by that security objective and OSPs enforced by that security objective, and the security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

	OSP.Audit	OSP.TimeService
O.Audit	x	
O.TimeService		x
OE.Audit	x	
OE.TimeSource		x

Table 1: Security objective rationale

The following part of the chapter demonstrates that the security objectives counter all threats and enforce all OSPs, and the security objectives for the operational environment uphold all assumptions.

The organizational security policy OSP.Audit “Audit for key management and cryptographic operations” is directly implemented by

– the security objective for the TOE O.Audit requiring security auditing and

– the security objective for the operational environment OE.Audit requiring the regular audit review and the availability of exported audit records.

The organizational security policy OSP.TimeService “Time Service and Time stamp service” is directly implemented by

– the security objective for the TOE O.TimeService “Time services ” requiring the TOE to provide an internal time service and time stamp service for the user, and
– the security objective for the operational environment OE.TimeSource “External time source” requiring the operational environment to provide reliable external time stamps for adjustment of TOE internal time source.

8 Extended component definition

The PP-Module uses the extended SFR component FPT_TIT.1 of the extended family FPT_TIT as defined in the Base-PP PP CSP.

9 Security requirements

The CC allows several operations to be performed on functional requirements: *refinement*, *selection*, *assignment*, and *iteration.* Each of these operations is used in this PP.
The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is (i) denoted by the word "refinement" in **bold** text and the added/changed words are in bold text, or (ii) directly included in the requirement text as **bold** text. In cases where words from a CC requirement component were deleted, these words are ~~crossed out~~.
The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections that have been made by the PP authors are denoted as *italic* text and the original text of the component is given by a footnote. 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 *italicized*.
The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments that have been made by the PP authors are denoted by showing as *italic* text and the original text of the component is given by a footnote. 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 *italicized*.
The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/" and the iteration indicator after the component identifier.

9.1 Security functional requirements

The TOE provides cryptographic security services for encryption and decryption of user data, entity authentication of external entities and to external entities, authentication prove and verification of user data, trusted channel and random number generation.

The TOE enforces the *Cryptographic Operation SFP* for protection of these cryptographic services which subjects, objects, and operations are defined in the SFRs FDP_ACC.1/Oper and FDP_ACF/Oper in the Base-PP, and FDP_ACF.1/TS in this PP-Module.

The TOE enforces the *Key Management SFP* and *Update SFP* defined in the Base-PP.

9.1.1 Time Stamp

FDP_DAU.2/TS Data Authentication with Identity of Guarantor – Signature with time stamp and optional key usage counter

Hierarchical to:	FDP_DAU.1 Basic Data Authentication
Dependencies:	FIA_UID.1 Timing of identification
FDP_DAU.2.1/TS	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the **existence at certain point in time, sequence and** validity of (a) *user data imported according to FDP_ITC.2/UD,* (b) *exported audit records according to FMT_MTD.1/Audit clause (1) and FAU_STG.3 clause (1)*[1] **with** **(1) time stamp of the evidence generation according to FPT_STM.1,** **(2) and optionally the key usage counter of the signature key**

1 [assignment: *list of objects or information types*]

by means of digital signature generated according to [**selection:** ***FCS_COP.1/CDS-ECDSA, FCS_COP.1/CDS-RSA***] **and keys holding the dedicated values of the security attributes Key identity that indicate key ownership of the TOE sample and Key usage type "Time stamp service".**

FDP_DAU.2.2/TS The TSF shall provide [assignment: *list of subjects*] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

Application note 1: The TSF according to FDP_DAU.2/TS is intended for time stamp service of the TOE for any provided user data and exported audit records. The user data source shall select the security attribute *Key usage type* "*TimeStamp*" of the signature key of the time stamp service. The signature key of exported audit records shall be defined according to FMT_MOF.1.1/TSA clause (5). The Key usage counter allows to verify the sequence of signed data e. g. in an audit trail. The verification of the evidence requires a certificate showing the identity of the TOE sample and the key usage type of time stamp service. The format of input data and output data shall meet the BSI TR-03151 [TR-03151] .

9.1.2 Access control on time stamp service

FDP_ITC.2/TS Import of user data with security attributes – User data for time stamping

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path]
FPT_TDC.1 Inter-TSF basic TSF data consistency

FDP_ITC.2.1/TS The TSF shall enforce the *Cryptographic Operation SFP*[2] when importing user data, controlled under the SFP, from outside of the TOE.

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

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

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

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

(1) *user data imported for time stamp generation to FDP_DAU.2/TS shall be imported with security attributes Key identity of the signature key and Key usage type TimeStamp, and the identification of the requested cryptographic operation*[3].

Application note 2: Keys to be used for the cryptographic operation of the imported user data are identified by security attribute *Key identity*.

FDP_ETC.2/TS Export of user data with security attributes - User data with time stamp

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_ETC.2.1/TS The TSF shall enforce the *Cryptographic Operation SFP*[4] when exporting user data, controlled under the SFP(s), outside of the TOE.

2 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

3 [assignment: *additional importation control rules*]

4 [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

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

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

FDP_ETC.2.4/TS The TSF shall enforce the following rules when user data is exported from the TOE:

(1) *user data exported as time stamped data according to FDP_DAU.2/TS shall be exported with digital signature and Key identity of the used signature-creation key*[5].

Application note 3: In case of internally generated data (e.g. audit records) the exported signed data shall be attributed with the *Key identity* of the used signature-creation key. Note that the TOE may implement more than one signature-creation key for signing internally generated data.

FDP_ACF.1/TS Security attribute based access control – Cryptographic operations

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/TS The TSF shall enforce the *Cryptographic Operation SFP*[6] to objects based on the following:

(1) *subjects: subjects with security attribute Role Application Component, [assignment: other roles]*;

(2) *objects: user data*[7].

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

(1) *Application Component, [assignment: other roles] is allowed to perform cryptographic operation according to FDP_DAU.2/TS on user data with cryptographic keys with Key usage type TimeStamp.*

(2) *[assignment: other rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]*[8].

FDP_ACF.1.3/TS 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*].

FDP_ACF.1.4/TS The TSF shall explicitly deny access of subjects to objects based on the

(1) *No subject is allowed to use cryptographic keys by cryptographic operation other than those identified in the security attributes Key usage type and the Key access control attributes*;

(2) *[assignment: additional rules, based on security attributes, that explicitly deny access of subjects to objects]*.[9]

5 [assignment: *additional exportation control rules*]

6 [assignment: *access control SFP*]

7 [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*]

8 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

9 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

9.1.3 Security Management

FMT_SMF.1/TSA Specification of Management Functions

Hierarchical to: No other components.

Dependencies: No dependencies.

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

(1) *management of security functions behaviour FMT_MOF.1/TSA*[10].

FMT_SMR.1/TSA Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1/TSA The TSF shall maintain the roles **additional to those required by FMT_SMR.1 in the Base-PP**: *[selection: Auditor,Timekeeper, no other roles]*[11].

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

Application note 4: The ST may select the general role *Administrator* or more detailed Administrator roles as supported by the TOE. The ST may select

– *Auditor* role in FMT_SMR.1/TSA separated from Administrator roles selected in the SFR FMT_SMR.1 according to the Base-PP and, or

– *Timekeeper* role in FMT_SMR.1/TSA separated from Administrator roles selected in the SFR FMT_SMR.1 according to the Base-PP and, or

– *no other roles* in FMT_SMR.1/TSA and assign the management of audit TSF in FMT_MTD.1/Audit to a selected Administrator role in the SFR FMT_SMR.1 according to the Base-PP.

The assignment of security management of audit and other functions must not result in a conflict of duties

FMT_MOF.1/TSA Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MOF.1.1/TSA The TSF shall restrict the ability to

(1) *modify the behaviour of*[12] the function~~s~~ *adjustment of the internal clock according to FPT_STM.1 clause (1)*[13] to *[selection: Administrator, Timekeeper]*[14],

(2) *modify the behaviour of*[15] the function~~s~~ *adjustment of the internal clock according to FPT_STM.1 clause (2)*[16] to *[selection: Administrator, Timekeeper]* [17],

10 [assignment: *list of management functions to be provided by the TSF*]

11 [assignment: *authorised identified roles*]

12 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

13 [assignment: *list of functions*]

14 [assignment: *the authorised identified roles*]

15 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

16 [assignment: *list of functions*]

17 [assignment: *the authorised identified roles*]

(3) *determine the behaviour of and modify the behaviour of*[18] the functions *select the auditable events according to FAU_GEN.1*[19] to *[selection: Administrator, Auditor]*[20],

(4) *determine the behaviour of and modify the behaviour of*[21] the functions *automatic export of audit trails according to FAU_STG.3.1 clause (1)*[22] to *[selection: Administrator, Auditor]*[23]

(5) *determine the behaviour of and modify the behaviour of*[24] the functions *FDP_DAU.2/TS by selection of signature key used to sign exported audit trails*[25] to *[selection: Administrator, Auditor]*[26].

Application note 5: The SFR defines additional management of security functions behaviour for new SFR with respect to the Base-PP. The refinements of FMT_MOF.1.1/TSA in bullets (2) to (5) are made in order to avoid further iterations of the component.

9.1.4 Security audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

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

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

b) All auditable events for the *not specified*[27] level of audit; and

c) *Discrete* a*djustment of the real time clock*

(1) by automatic adjustment of the clock according to FPT_STM.1.1 clause (2) if selected as auditable event,

(2) by Administrator according to FPT_STM.1.1 clause (1) or(2),

(3) failure of adjustment according to FPT_STM.1.1,

d) *other auditable events*

(1) *Start-up after power-up,*

(2) *Import of UCP (FDP_ITC.2/UCP),*

(3) *Authentication failure handling (FIA_AFL.1): the reaching of the threshold for the unsuccessful authentication attempts with claimed Identity of the user,*

[selection:

18 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

19 [assignment: *list of functions*]

20 [assignment: *the authorised identified roles*]

21 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

22 [assignment: *list of functions*]

23 [assignment: *the authorised identified roles*]

24 [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]

25 [assignment: *list of functions*]

26 [assignment: *the authorised identified roles*]

27 [selection: *choose one of: minimum, basic, detailed, not specified*]

(4) *Generation of (selected types of) signature key pairs (all FCS_CKM.1 instantiations for generation of permanent stored keys)*

(5) *Execution of (selected types of) cryptographic operation (all FCS_COP.1 instantiations),*

(6) *Cryptographic key destruction (FCS_CKM.4) of permanent stored keys,*

(7) *Failure with preservation of secure state (FPT_FLS.1): entering and exiting secure state*,

(8) *Management of security functions (FMT_MOF.1, FMT_MOF.1/TSA)*,

(9) *[assignment: additional specifically defined auditable events],*

(10) *No other event*

(11) *Management of TSF data (FMT_MTD.1/AUDIT): Export, clear and selection of events causing audit data*[28]].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*].

Application note 6: The SFR FDP_ITC.2/UCP, FIA_AFL.1, FCS_CKM.1, FCS_COP.1, FCS_CKM.4, FPT_FLS.1 and FMT_MOF.1 are defined in the Base-PP. The SFR FPT_STM.1, FMT_MOF.1/TSA and FMT_MTD.1/Audit are defined in this PP-Module.

FMT_MTD.1/Audit Management of TSF data

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1/Audit The TSF shall restrict the ability to

(1) *manual export,*

(2) *clear after manual export,*

(3) *select audited events in FAU_GEN.1,*

(4) *define the number of audit records causing automatic export and clearing of exported audit records according to FAU_STG.3.1 clause (1),*

(5) *define the percentage of storage capacity of audit records if actions are assigned in FAU_STG.3.1 clause (2)*[29]

the *audit records*[30] to *[selection: Auditor, Administrator]*[31].

Application note 7: The selection of auditable events according to FMT_MTD.1.1/Audit, clause (3) enables or disables or specifies the generation of audit records as defined in FAU_GEN.1. The role *Administrator* may be

28 [assignment: *other specifically defined auditable events*]

29 [selection: *change_default, query, modify, delete, clear,[assignment: other operations]*]

30 [assignment: *list of TSF data*]

31 [assignment: *the authorised identified roles*]

selected only if it is selected in FMT_SMR.1 in the Base-PP and any conflict of duties is prevented (cf. application note to FMT_SMR.1/TSA).

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

FAU_STG.1.2 The TSF shall be able to *prevent*[32] unauthorised modifications to the stored audit records in the audit trail.

FAU_STG.3 Action in Case of Possible Audit Data Loss

Hierarchical to: No other components.

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.3.1 The TSF shall

(1) *automatically export audit trails and clear automatically exported audit records*[33] if the audit trail exceeds *an [selection: Administrator, Auditor] defined number of audit records within [assignment: pre-defined range]*[34]

(2) ***[assignment: actions to be taken in case of possible audit storage failure]* if the audit trail exceeds an *[selection: Administrator, Auditor] settable percentage of storage capacity*[35]**.

Application note 8: The ST writer shall perform the open operations in FAU_STG.3.1 element. If the number of audit records in clause (1) is set to 1 then the TSF export each audit record automatically. If the number of number of audit records in clause (1) is set higher than maximum number of audit records in the audit trail then the TSF does not export audit records automatically. The assignment of clause (2) may be "no actions" if an appropriate number of audit records is assigned in clause (1).

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps **by means of [selection:**

(1) *internal clock with accuracy [assignment: approximate deviation] with the ability of adjustment of the clock by the [selection: Administrator, Timekeeper],*

(2) *internal clock with accuracy [assignment: approximate deviation] with automatic adjustment of the clock by an externally trustable source in a cryptographically verifiable manner (e.g. by signed Network Time Protocol) and the ability of adjustment of the clock by the [selection: Administrator, Timekeeper].*

Application note 9: The external trustable source (e.g. signed Network Time Protocol) provides a reliable time source for adjustment of the internal clock. The time intervals of adjustments in clause (2) may be configured by the Administrator. Any adjustment or failure of adjustment of the internal clock is an

32 [selection, choose one of: *prevent, detect*]

33 [assignment: *actions to be taken in case of possible audit storage failure*]

34 [assignment: *pre-defined limit*]

35 [assignment: *pre-defined limit*]

auditable event according to FAU_GEN.1.1.The refinement with selection defines different cases for internal clocks and are therefore printed in bold.

Note that it is not expected that the internal clock continues to operate when the TOE is switched off. An implementation that e.g. counts CPU ticks with sufficient accuracy while switched on would suffice to fulfil the requirements, provided that all auditable events are logged properly.

FPT_TIT.1/Audit TSF data integrity transfer protection – Audit functionality

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]
FPT_TIT.1.1/Audit	The TSF shall enforce the *Update SFP, [selection: Key Management SFP, Cryptographic Operation SFP]*[36] to *transmit*[37] TSF data **audit records** in a manner protected from *modification, deletion, insertion and replay*[38] errors.
FPT_TIT.1.2/Audit	The TSF shall be able to determine on receipt of TSF data **time**, whether *modification*[39] has occurred.

Application note 10: The Update SFP is enforced by the export of audit records about import of UCP, cf. FAU_GEN.1.1 clause d) (2). The selection of the Key Management SFP or Cryptographic Operation SFP depends on the selection of auditable events of key management, cryptographic operations and adjustment of the internal clock (e. g. used for verification of validity time period) in FAU_GEN.1.1 clause c). The TSF transmits audit records and receives time as TSF data for security audit. The TSF protects the audit records by means of digital signature against modification and by means of time stamps and key usage counter of the signature key as part of the signature against deletion, insertion and replay as required in FPT_TIT.1.1.

9.2 Security requirements rationale

9.2.1 Dependency rationale

This chapter demonstrates that each dependency of the security requirements is either satisfied, or justifies the dependency not being satisfied.

Note, the column SFR components showing the concrete SFR satisfying the dependencies are typical use cases. It does not exclude that the SFR in the first column may solve dependencies of other SFR as well. E. g. the SFR FCS_CKM.1/ECC defines requirements for ECC key generation and the ECC key pair may be directly used for ECDSA digital signatures according to FCS_COP.1/CDS-ECDSA and FCS_COP.1/VDS-ECDSA but also for encryption and decryption of the AES key in FCS_COP.1/HEM and FCS_COP.1/HDM.

36 [assignment: *access control SFP*]

37 [selection: *transmit, receive, transmit and receive*]

38 [selection: *modification, deletion, insertion, replay*]

39 [selection: *modification, deletion, insertion, replay*]

SFR	Dependencies of the SFR	SFR components
FAU_GEN.1	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_STG.1	FAU_GEN.1 Audit data generation	FAU_GEN.1
FAU_STG.3	FAU_STG.1 Protected audit trail storage	FAU_STG.1
FDP_ACF.1/TS	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1/Oper in Base-PP, FMT_MSA.3 in Base-PP
FDP_DAU.2/TS	FIA_UID.1 Timing of identification	FIA_UID.1 in Base-PP
FDP_ETC.2/TS	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1/Oper in Base-PP
FDP_ITC.2/TS	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/Oper, trusted communication is provided by FCS_COP.1/HDM and FCS_COP.1/VDS-*, FTP_ITC.1, FPT_TDC.1/CK because import of user data is intended for cryptographic operation with key with appropriate security attribute “TimeStamp”, all these SFR in Base-PP
FMT_MOF.1/TSA	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1/TSA and FMT_SMR.1 in Base-PP, FMT_SMF.1/TSA
FMT_MTD.1/Audit	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1/TSA and FMT_SMR.1 in Base-PP, FMT_SMF.1/TSA
FMT_SMF.1/TSA	No dependencies	
FMT_SMR.1/TSA	FIA_UID.1 Timing of identification	FIA_UID.1 in Base-PP
FPT_STM.1	No dependencies	
FPT_TIT.1/Audit	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FMT_MTD.1 Management of TSF data or FMT_MTD.3 Secure TSF data]	FDP_ACC.1/UCP in Base-PP and FDP_ACC.1/KM and FDP_ACC.1/Oper if selected, FMT_MTD.1/Audit

Table 2: Dependency rationale

9.2.2 Security functional requirements rationale

The table 3 trace each SFR back to the security objectives for the TOE.

	O.Audit	O.TimeService
FAU_GEN.1	x	
FAU_STG.1	x	
FAU_STG.3	x	
FDP_ACF.1/TS		x
FDP_DAU.2/TS	x	x
FDP_ETC.2/TS		x
FDP_ITC.2/TS		x
FMT_MOF.1/TSA		x
FMT_MTD.1/Audit	x	
FMT_SMF.1/TSA	x	x
FMT_SMR.1/TSA	x	x
FPT_STM.1	x	x
FPT_TIT.1/Audit	x	

Table 3: Security functional requirement rationale

Notation in table 3: x denotes the SFR is traced back to the security objectives for the TOE, (x) denotes the SFR is traced back to the security objectives for the TOE if auditable event is selected in SFR FAU_GEN.1.

The security objective for the TOE O.TimeService “Time services” is met by the following SFR:

– The SFR FPT_STM.1 requires the TSF to provide time stamps for the real time service.

– The SFR FDP_DAU.2/TS requires the TSF to provide cryptographic protected time stamps for time stamp service supported by FCS_COP.1/CDS-ECDSA resp. FCS_COP.1/CDS-RSA for signature creation defined in the Base-PP.

– The SFR FDP_ACF.1/TS defines access control on time stamp service to enforce the *Cryptographic Operation SFP* defined in the Base-PP.

– The SFR FDP_ITC.2/TS for user data import with security attributes indicating the signature key for time stamps.

– The SFR FDP_ETC.2/TS requires the TSF to export user data with time stamps.

– The SFR FMT_SMF.1/TSA defines the management functions and FMT_SMR.1/TSA the roles for the time service and the time stamp service additional to those defined in the Base-PP.

– The SFR FMT_MOF.1/TSA defines the management of the time service and the time service TSF.

The security objective for the TOE O.Audit “Audit” is met by the following SFR:

– The SFR FAU_GEN.1 requires the TSF to generate the audit records of auditable events.

– The SFR FAU_STG.1 and FAU_STG.3 requires the TSF to protect and to prevent loss of audit records.

– The SFR FMT_MTD.1/Audit restricts the ability to export and to delete exported audit records to an Administrator. It prevents undetected deletion of audit records by generation of an audit record about deletion. The export, clear and selection of events causing audit data as management TSF data is an auditable event, cf. FAU_GEN.1, clause (11).

– The SFR FPT_TIT.1/Audit requires the TSF to protect audit records when transmitted and time when imported.

- The SFR FMT_SMF.1/TSA defines the management functions and FMT_SMR.1/TSA the roles for the audit TSF additional to those defined in the Base-PP.
- The SFR FMT_MOF.1/TSA requires the TSF to provide the capability to define the auditable events in clause (3) and the behaviour of automatic export of audit records in clause (4).
- The SFR FDP_DAU.2/TS requires the TSF to provide the capability to export audit trails signed and time stamped.
- The SFR FPT_TIT.1/Audit defines the TSF data integrity transfer protection for the audit functionality.
- The SFR FPT_STM.1 requires the TSF to provide time stamps being part of the audit records.

10 Reference Documentation

CC2	Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
CC3	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017
CC4	Common Methodology for Information Technology Security Evaluation, Evaluation methodology; CCMB-2017-04-004, Version 3.1 Revision 5, April 2017
PP CSP	BSI, Common Criteria Protection Profile Cryptographic Service Provider, BSI-CC-PP-0104-2019, , 2019
PP-CSP	BSI, Common Criteria Protection Profile - Cryptographic Service Provider, BSI-CC-PP-0104-2019, , Feburar 2019
TR-03151	BSI, Technical Guideline TR-03151 Secure Element API (SE API), Version 1.0, 5. Juni 2018

Keywords and Abbreviations

Acronym	Term
A.xxx	Assumption
CC	Common Criteria
O.xxx	Security objective for the TOE
OE.xxx	Security objective for the TOE environment
OSP.xxx	Organisational security policy
PP	Protection profile
SAR	Security assurance requirements
SFR	Security functional requirement
T.xxx	Threat
TOE	Target of Evaluation
TSF	TOE security functionality
UCP	update code package

Table 4: Abbreviations