Federal Office
for Information Security

Common Criteria Protection Profile Configurations Cryptographic Service Provider - Time Stamp Service and Audit – Clustering (PPC-CSP-TS-Au-Cl)

Protection Profile-Module CSP Clustering (PPM-Cl)

BSI-CC-PP-0108-2019

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:

- the Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service, Audit and Clustering (PPC-CSP-TS-Au-Cl) in chapter 2,
- the Protection Profile Module Clustering (PPM-Cl) of CSP in chapters 3 to 9.

Please note, that this Protection Profile Configuration is built out of two modules (PPM-TS-Au and PPM-Cl, see also section 2.2). The module PPM-Cl is actually given and defined in detail in section 3, whereas the PP-Module Time Stamp Service and Audit (PPM-TS-Au) is incorporated only by reference to the Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit [PP CSP-TS-Au] from which the respective module PPM-TS-Au (cf. [PP CSP-TS-Au], section 3 to 9) is meant to be used identically in this PPC.

2 PP-Configuration CSP-TS-Au-Cl

2.1 Reference

This PP-Configuration is identified as

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

Version: 0.9.4, as of April 8th 2019

Registration: BSI-CC-PP-0108-2019

2.2 Components Statement

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

Title: Cryptographic Service Provider (PP CSP), Version:0.9.8, [PP CSP]

Registration: BSI-CC-PP-0104-2019

This PP-Configuration consists of the Base-PP together with two PP-Modules

- Title: Protection Profile-Module CSP Time Stamp Service and Audit (PPM-TS-Au), Version: 0.9.5 [PP CSP-TS-Au],
- Title: Protection Profile-Module CSP Clustering (PPM-Cl), Version:0.9.4, defined in chapter 3 to 9.

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

Please note, that this Protection Profile Configuration is built out of two modules (PPM-TS-Au and PPM-Cl, see also section 2.2). The module PPM-Cl is actually given below and defined in detail. The PP-Module PPM-TS-Au is incorporated only by reference to the PP-Module, whereas the PP-Module Time Stamp Service and Audit (PPM-TS-Au) is incorporated only by reference to the Protection Profile Configuration Cryptographic Service Provider – Time Stamp Service and Audit [PP CSP-TS-Au], from which the respective module PPM-TS-Au (cf. [PP CSP-TS-Au], section 3 to 9) is meant to be used identically in this PPC. Therefore, the actual contents and definitions of PPM-TS-Au are not reiterated below but input via reference to the PPC TS-Au [PP CSP-TS-Au].

3.1 PP-Module Reference

Title:	Common Criteria Protection Profile Module Cryptographic Service Provider - Clustering
Sponsor:	BSI
CC Version:	3.1 Revision 5
General Status:	Final
Version Number:	0.9.4
Registration:	-
Keywords:	cryptographic service provider, clustering

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 as the TOE of the Base-PP but with additional functionality supporting cluster.

TOE definition

The TOE is physically defined as a device consisting of software and may include hardware and firmware as defined in the Base-PP. The TOE provides additional TOE security functionality (TSF) with respect to the TOE of the Base-PP in order to enable the set-up of a CSP-cluster of TOE samples for scalability of performance and availability of security services.

The *Administrator* role (cf. the Base-PP for definition of the roles) is authorized to set up a CSP-cluster of TOE samples. For the initialization of a CSP-cluster the Administrator selects one TOE sample as Master-CSP and the other TOE samples as Slave-CSPs. The TOE samples of the CSP-cluster agree cluster keys for encrypted and integrity protected exchange of TSF data. The Master-CSP transfers TSF data *Authentication Data Records* of known users and cryptographic keys to Slave-CSP under control of the *Administrator* or the *Application Component* using the CSP-cluster.

The TOE provides clustering as additional method of use compared with those of the TOE defined in the Base-PP.

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

The PP-module is used in the PP-Configurations PPC-CSP-TS-Au-Cl with Base-PP CSP. 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 cryptographic service provider (CSP) component as the TOE type in the Base-PP CSP: cryptographic service provider (CSP) component. The TOE provides additional TSF for clustering.

4.1.2 Security problem definition (SPD)

Threats

The security problem definition of the PP-module PPM-Cl does not define any threats additional to the threats described in the Base-PP CSP.

Organizational Security Policies

Compared to the SPD of the Base-PP CSP the PP module PPM-Cl adds new organizational security policy OSP.Cluster addressing only the clustering of the TOE samples.

Assumptions

The PP module PPM-Cl defines additional assumption A.ClusterAppl addressing only the management of security attributes of the known users and cryptographic keys within the CSP cluster protected by the additional TSF for clustering. The additional assumption are necessary for clustering and do not interfere with the other TSF defined in the Base-PP CSP.

4.1.3 Security objectives

The PP-module PPM-Cl defines security objectives for the TOE O.Cluster in order to implement the OSP.Cluster by TSF. The security objectives for the TOE O.Audit defined in PPM-TS-Au applies also to TSF implementing the O.Cluster. The security objectives for the operational environment OE.ClusterCtrl and OE.TSFdataTrans enforces the OSP.Cluster by administrative security measures and ensures the assumption A.ClusterApp. The additional security objectives are necessary for clustering and do not interfere with the other TSF defined in the Base-PP CSP.

4.1.4 Security Functional Requirements

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

FAU_GEN.1/CL, FCS_CKM.5/CLDH, FDP_ACC.1/CL, FMT_MTD.1/CL, FPT_ESA.1/CL, FPT_ISA.1/CL, FPT_TCT.1/CL, FPT_TDC.1/CL, FPT_TIT.1/CL.

These SFRs concern exclusively the cluster functionality which is not addressed in the Base-PP. The SFR FAU_GEN.1/CL extends the SFR FAU_GEN.1 for audit data generation and uses the reliable time stamps according to FPT_STM.1 in the PP-Module PPM-TS-Au. The SFR FCS_CKM.5/CLDH requires derivation of cryptographic keys used for encryption and MAC protection as required by FCS_COP.1/ED and FCS_COP.1/MAC required 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 CC conformance claims

5.1 CC conformance claim

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-Cl), consisting of the Base-PP “Cryptographic Service Provider (PP CSP)”,the PP-Modules “CSP Time Stamp Service and Audit” and “CSP Clustering”, 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 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 TOE protects the TSF data the security attributes of the known users and the cryptographic keys with their security attributes transferred from Master-CSP to Slave-CSPs.

Users and subjects

The TOE knows external entities (users) as

– *human user* communicating with the TOE for security management of the TOE,

– *application component* using the cryptographic and other security services of the TOE and supporting the communication with remote entities (e. g. by providing certificates),

– *cluster-CSP* being another TOE sample in a cluster with the TOE.

The TOE communicates with cluster-CSP in encrypted and integrity protected form. The communication with human users and application component is described in the Base-PP. The subjects as active entities in the TOE perform operations on objects. They obtain their associated security attributes from the authenticated users on behalf they are acting, or by default.

Objects

The TSF operates TSF data objects (i. e. passive entities, that contain or receive information, and upon which subjects perform operations). The TSF data objects contain the security attributes of the known users and the cryptographic keys with their security attributes transferred from Master-CSP to Slave-CSPs.

Security attributes

The security attributes of user known to the TOE are stored in *Authentication Data Records* containing

– *User Identity* (User-ID),

– *Authentication reference data*,

– *Role* with detailed access rights.

The TOE knows at least the following roles taken by a user or a subject acting on behalf of a user:

– *Administrator*: successful authenticated user allowed to access the TOE in order to perform management functions. It is taken by a human user or a subject acting on behalf of a human user after successful authentication as Administrator.

  The *Administrator* role may be split in more detailed roles:

  - *Crypto-Officer*: role that is allowed to access the TOE in order to perform management of a cryptographic TSF.
  - *User Administrator*: role that is allowed to access the TOE in order to perform user management.

  The SFR uses the general term Administrator or a selection between Administrator role and these detailed roles in case they are supported by the TOE and separation of duties is appropriate.

– *Application Component*: subjects in this role are allowed to use assigned security services of the TOE without authenticated human user session (e. g. export and import of wrapped keys). This role may be assigned to an entity communicating through a physically separated secure channel or through a trusted channel (which requires assured identification of its end points).
– *Cluster-CSP*: another TOE sample in a cluster with the TOE with security attribute *Master-CSP* or *Slave-CSP*. This role is bound to the communication through the trusted channel between cluster CSPs established by the administrator.

The cryptographic keys and their security attributes are defined in the Base-PP and the PP-Module PPM-CSP-TS-Au. The PP-Module PPM-CSP-CL uses 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; the PP-Module use the clustering encryption key for cryptographic operation according to FCS_COP.1/ED and clustering MAC keys for cryptographic operation according to FCS_COP.1/MAC as defined in the Base-PP.
– *Key access control attributes*, i. e. list of combinations of the identity of the user, the role for which the user is authenticated and the allowed key management function or cryptographic operation, including
  • *Clustering*: transfer of the key in a cluster of TOE samples (i. e. export by TOE as Master-CSP and import by TOE as Slave-CSP) is allowed or forbidden.

6.2 Threats

The security problem definition of the PP-module does not define any threats additional to the threats described in the Base-PP.

6.3 Organisational security policies

OSP.Cluster Cluster of TOE samples
The administrator establishes and manages a cluster of multiple TOE samples for secure transfer of the security attributes of the known users and the cryptographic keys as necessary for scalability of performance and availability of security services.

6.4 Assumptions

A.ClusterAppl Cluster management by application
The application using the security services of the TOE transfers security attributes of the known users and cryptographic keys with their security attributes from Master-CSP to Slave-CSPs as necessary for scalability of performance and availability of security services.

7 Security objectives

7.1 Security objectives for the TOE

O.Cluster Cluster
The TSF supports cluster of TOE samples by secure transfer of the security attributes of the known users and the cryptographic keys with their security attributes from Master-CSP to Slave-CSPs in encrypted and integrity protected form.

7.2 Security objectives for the operational environment

OE.ClusterCtrl Control of the cluster
The administrator establishes and manages a cluster only of trustworthy samples of the TOE as necessary for scalability of performance and availability of security services.

OE.TSFdataTrans Transfer of TSF data within the CSP cluster
The administrator and the application using the security services of the TOE transfer the security attributes of the known users and the cryptographic keys with their security attributes from Master-CSP to Slave-CSPs as necessary for scalability of performance and availability of security services.

7.3 Security objective rationale

The following table traces the security objectives for the TOE back the OSPs enforced by that security objective, and the security objective for the operational environment back OSPs enforced by that security objective, and assumptions upheld by that security objective. Note the OSP.SecCryM “Secure cryptographic mechanisms” defined in the Base-PP.

	OSP.SecCryM	OSP.Cluster	A.ClusterAppl
O.Cluster	x	x	
OE.ClusterCtrl		x	
OE.TSFdataTrans		x	x

Table 1: Security objective rationale

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

The organizational security policy OSP.SecCryM “Secure cryptographic mechanisms” defined in the Base-PP is implemented by means of secure cryptographic mechanisms required in

– O.Cluster “Cluster” requiring secure transfer in encrypted and integrity protected form of the security attributes of the known users and the cryptographic keys with their security attributes from Master-CSP to Slave-CSPs.

The organizational security policy OSP.Cluster “Cluster of TOE samples” is implemented by security objectives for the TOE and the operational environment:

– O.Cluster requiring support for cluster of TOE samples as CSPs with distribution of Authentication Data Records and cryptographic keys from Master-CSP to Slave-CSPs through a trusted channel keeping the confidentiality and integrity of the security attributes of the known users and of the cryptographic keys with their security attributes.

– OE.ClusterCtrl requiring administrator to build a cluster only of trustworthy samples of the TOE as needed for scalability of performance and availability of security services.
– OE.TSFdataTrans requires the administrator and the application using the security services of the TOE transfer security attributes of the known users and cryptographic keys with their security attributes from Master-CSP to Slave-CSPs as necessary for scalability of performance and availability of security services.

The assumption A.ClusterAppl is directly ensured by OE.TSFdataTrans.

8 Extended component definition

The PP-Module uses the extended SFR components FCS_CKM.5, FPT_ESA.1, FPT_ISA.1, FPT_TCT.1 and FPT_TIT.1 defined in the Base-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 *Clustering SFP* for protection of the security attributes of the known users and the cryptographic keys with their security attributes.

The SFR FCS_CKM.5/CLDH based on elliptic curves refer for selection of curves, key sizes and standards to the Tables 2 and 3 defined in the Base-PP [PP CSP].

9.1.1 Clustering

The cluster of TOE samples is set up by the Administrator as Cluster-CSPs by

– selecting one TOE sample of the cluster as Master-CSP, all other TOE samples of the cluster are Slave-CSPs,

– initialization of secure channels between the Master-CSP and the Slave-CSPs,

– transfer of TSF data as security attributes of known users and cryptographic keys with security attributes from Master-CSP to Slave-CSPs using the application.

FDP_ACC.1/CL Subset access control – Clustering

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/CL The TSF shall enforce the *Clustering SFP*[1] on

(1) *subjects: Administrator;*

1 [assignment: *access control SFP*]

(2) *objects: cluster keys, Authentication Data Records, cryptographic keys*;

(3) *operations: generation, export, import*[2].

FMT_MTD.1/CL Management of TSF data – Authentication Data Records and cryptographic keys

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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

(1) *generate according to FCS_CKM.5/CLDH*[3] the *cluster keys*[4] to *Administrator*[5],

(2) *export from the Master-CSP according to FPT_ESA.1/CL, FPT_TCT.1/CL and FPT_TIT.1/CL*[6] the *Authentication Data Records* [7] to *[selection: Application Component, Administrator, User Administrator]*[8],

(3) *import into Slave-CSPs according to FPT_ISA.1/CL, FPT_TCT.1/CL and FPT_TIT.1/CL*[9] the *Authentication Data Records* [10] to *[selection: Application Component, Administrator, User Administrator]*[11]

(4) *export from the Master-CSP according to FPT_ESA.1/CL, FPT_TCT.1/CL and FPT_TIT.1/CL*[12] the *cryptographic keys*[13] to *[selection: Application Component, Administrator, Crypto-Officer]*[14],

(5) *import into Slave-CSPs according to FPT_ISA.1/CL, FPT_TCT.1/CL and FPT_TIT.1/CL*[15] the *cryptographic keys* [16] to *[selection: Application Component, Administrator, Crypto-Officer]*[17].

Application note 1: Authentication Data Records and cryptographic keys are TSF data. The selection in FMT_MTD.1/CL allows for a more detailed separation of duties between the roles if supported by the TOE. The bullets (2) to (5) are refinements to avoid further iterations of the component FMT_MTD.1.1/CL and therefore printed in bold.

2 [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

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

4 [assignment: *list of TSF data*]

5 [assignment: *the authorised identified roles*]

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

7 [assignment: *list of TSF data*]

8 [assignment: *the authorised identified roles*]

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

10 [assignment: *list of TSF data*]

11 [assignment: *the authorised identified roles*]

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

13 [assignment: *list of TSF data*]

14 [assignment: *the authorised identified roles*]

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

16 [assignment: *list of TSF data*]

17 [assignment: *the authorised identified roles*]

FCS_CKM.5/CLDH Cryptographic key derivation – Cluster keys

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.5.1/CLDH The TSF shall derive cryptographic *cluster* keys[18] from *an agreed shared secret*[19] in accordance with a specified cryptographic key derivation algorithm *anonymous Diffie-Hellman Key Agreement for ECC key pair generation with [selection: elliptic curves in the ta*ble 2 *[PP CSP]]* [20] and specified cryptographic key sizes *[selection: key size in the table 2 [PP CSP]]* [21] that meet the following: [selection: *standards in the tables 2 and 3 [[PP CSP], [TR-03111]]*[22].

Application note 2: The cryptographic cluster keys shall be used for encryption according to FCS_COP.1/ED (cf. Base-PP) and FPT_TCT.1/CL and MAC protection according to FCS_COP.1/MAC (cf. Base-PP) and FPT_TIT.1/CL during transfer of Authentication Data Records and the cryptographic keys from Master-CSP to Slave-CSP. The tables 2 and 3 are defined in the Base-PP [PP CSP].

FPT_TCT.1/CL TSF data confidentiality transfer protection – Cluster

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset informationflow control]
[FMT_MTD.1 Management of TSF data or
FMT_MTD.3 Secure TSF data]

FPT_TCT.1.1/CL The TSF shall enforce the *Clustering SFP*[23] by providing the ability to *transmit and receive*[24] **Authentication Data Records and cryptographic keys** ~~TSF data~~ in a manner protected from unauthorised disclosure **according to FCS_COP.1/ED**.

Application note 3: FCS_COP.1/ED is defined in the Base-PP.

FPT_TIT.1/CL TSF data integrity transfer protection – Cluster

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset informationflow control]
[FMT_MTD.1 Management of TSF data or
FMT_MTD.3 Secure TSF data]

FPT_TIT.1.1/CL The TSF shall enforce the *Clustering SFP*[25] to *transmit and receive*[26] **Authentication Data Records and cryptographic keys** ~~TSF data~~ in a manner protected from *modification*[27] errors **according to FCS_COP.1/MAC**.

18 [assignment: *key type]*
19 [assignment: *input parameters*]
20 [assignment: c*ryptographic key derivation algorithm*]
21 [assignment: *cryptographic key sizes*]
22 [assignment: *list of standards*]
23 [assignment: *access control SFP, information flow control SFP*]
24 [selection: *transmit, receive, transmit and receive*]
25 [assignment: *access control SFP, information flow control SFP*]
26 [selection: *transmit, receive, transmit and receive*]
27 [selection: *modification, deletion, insertion, replay*]

FPT_TIT.1.2/CL The TSF **in role Slave-CSP** shall be able to determine on receipt of **Authentication Data Records and cryptographic keys** ~~TSF data~~, whether *modification*[28] has occurred **according to FCS_COP.1/MAC**.

Application note 4: FCS_COP.1/MAC is defined in the Base-PP.

FPT_ISA.1/CL Import of TSF data with security attributes – Cluster

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset informationflow control]
[FMT_MTD.1 Management of TSF data, or
FMT_MTD.3 Secure TSF data]
[FMT_MSA.1 Management of security attributes, or
FMT_MSA.4 Security attribute value inheritance]
FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_ISA.1.1/CL The TSF **in role Slave-CSP** shall enforce the *Clustering SFP*[29] when importing **Authentication Data Records and cryptographic keys** ~~TSF data~~, controlled under the SFP, from ~~outside of the TOE~~ **Master-CSP**.

FPT_ISA.1.2/CL The TSF **in role Slave-CSP** shall use the security attributes associated with the imported **Authentication Data Records and cryptographic keys** ~~TSF data~~.

FPT_ISA.1.3/CL The TSF **in role Slave-CSP** shall ensure that the protocol used provides for the unambiguous association between the security attributes and the **Authentication Data Records and cryptographic keys** ~~TSF data~~ received.

FPT_ISA.1.4/CL The TSF **in role Slave-CSP** shall ensure that interpretation of the security attributes of the imported **Authentication Data Records and cryptographic keys** ~~TSF data~~ is as intended by the source of the **Authentication Data Records and cryptographic keys** ~~TSF data~~.

FPT_ISA.1.5/CL The TSF **in role Slave-CSP** shall enforce the following rules when importing **Authentication Data Records and cryptographic keys** ~~TSF data~~ controlled under the SFP from ~~outside of the TOE~~ **Master-CSP**:

(1) *TSF in role Slave-CSP always imports Authentication Data Records with security attributes from Master-CSP.*

(2) *TSF in role Slave-CSP imports cryptographic keys with security attributes from Master-CSP only if the security attribute Clustering of the key allows transfer*[30].

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

29 [assignment: *access control SFP, information flow control SFP*]

30 [assignment: *additional importation control rules*]

FPT_ESA.1/CL Export of TSF data with security attributes – Cluster

Hierarchical to: No other components.

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

[FMT_MTD.1 Management of TSF data or
FMT_MTD.3 Secure TSF data]
[FMT_MSA.1 Management of security attributes, or
FMT_MSA.4 Security attribute value inheritance]
FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_ESA.1.1/CL The TSF **in role Master-CSP** shall enforce the *Clustering SFP*[31] when exporting **Authentication Data Records and cryptographic keys** ~~TSF data~~, controlled under the SFP(s), ~~outside of the TOE~~ **to Slave-CSP**.

FPT_ESA.1.2/CL The TSF **in role Master-CSP** shall export the **Authentication Data Records and cryptographic keys** ~~TSF data~~ with the TSF data's associated security attributes.

FPT_ESA.1.3/CL The TSF **in role Master-CSP** shall ensure that the security attributes, when exported ~~outside the TOE~~ **to Slave-CSP**, are unambiguously associated with the exported **Authentication Data Records and cryptographic keys** ~~TSF data~~.

FPT_ESA.1.4/CL The TSF **in role Master-CSP** shall enforce the following rules when **Authentication Data Records and cryptographic keys** ~~TSF data~~ is exported ~~from the TOE~~ **to Slave-CSP**:

(1) *TSF in role Master-CSP exports Authentication Data Records with security attributes to any Slave-CSP.*

(2) *TSF in role Master-CSP exports cryptographic key with security attributes to Slave-CSP only if the security attribute Clustering of the key allows transfer*[32].

FPT_TDC.1/CL Inter-TSF basic TSF data consistency – Clustering

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TDC.1.1/CL The TSF shall provide the capability to consistently interpret *Authentication Data Records and cryptographic keys with their security attributes*[33] when shared between the TSF and **TOE sample in the cluster** ~~another trusted IT product~~.

FPT_TDC.1.2/CL The TSF shall use *the following rules:*

(1) *the TSF in Slave-CSP role shall interpret the imported Authentication Data Records with their security attributes in the same way as it interprets the Authentication Data Records when it exports them in Master-CSP role,*

(2) *the TSF in Slave-CSP role shall interpret the imported cryptographic keys with their security attributes in the same way as it interprets the Authentication Data Records when it exports them in Master-CSP role,*[34]

when interpreting the **Authentication Data Records and cryptographic keys** ~~TSF data~~ from **Master-CSP** ~~another trusted IT product~~.

31 [assignment: *access control SFP, information flow control SFP*]

32 [assignment: *additional exportation control rules*]

33 [assignment: *list of TSF data types*]

34 [assignment: *list of interpretation rules to be applied by the TSF*]

9.1.2 Security audit

FAU_GEN.1/CL Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1/CL 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*[35] level of audit; and

c) *other auditable events*

(1) *Generation of cluster keys for the secure channel according to FMT_MTD.1/CL and FCS_CKM.5/CLDH,*

(2) *Export of Authentication Data Records and cryptographic keys from the Master-CSP according to FPT_ESA.1.3/CL,Management of Authentication Data Records (FMT_MTD.1/RAD): creation and deletion of Authentication Data Record,*

(3) *Import according to FPT_ISA.1/CL of Authentication Data Records and cryptographic keys into Slave-CSPs.*[36].

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

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

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

Application note 5: The SFR FAU_GEN.1/CL adds auditable events to FAU_GEN.1 required by PPM-TS-Au. The SFR FPT_STM.1 is required by PPM-TS-Au.

Application note 6: *FMT_MTD.1/RAD* is defined in the Base-PP.

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.

SFR	Dependencies of the SFR	SFR components
FAU_GEN.1/CL	FPT_STM.1 Reliable time stamps	FPT_STM.1 required by PPM-TS-Au
FCS_CKM.5/CLDH	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/ED, FCS_COP.1/MAC and FCS_CKM.4 required in the Base-PP

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

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

SFR	Dependencies of the SFR	SFR components
FDP_ACC.1/CL	FDP_ACF.1 Security attribute based access control	Dependency on FDP_ACF.1 is not fulfilled. Access control to key management functions are specified by FMT_MTD.1/CL because cryptographic keys are TSF data.
FMT_MTD.1/CL	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1, FMT_SMR.1 required in the Base-PP
FPT_ESA.1/CL	[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] [FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data consistency	FDP_ACC.1/CL FMT_MTD.1/CL, FMT_MTD.1/RAD and FMT_MTD.1/KM required in the Base-PP, FMT_MSA.1/KM applies for exported and imported keys and required in the Base-PP, FPT_TDC.1/CL
FPT_ISA.1/CL	[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] [FMT_MSA.1 Management of security attributes, or FMT_MSA.4 Security attribute value inheritance] FPT_TDC.1 Inter-TSF basic TSF data	FDP_ACC.1/CL FMT_MTD.1/CL, FMT_MTD.1/RAD and FMT_MTD.1/KM required in the Base-PP, FMT_MSA.1/KM applies for exported and imported keys and required in the Base-PP, FPT_TDC.1/CL
FPT_TCT.1/CL	[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/CL FMT_MTD.1/CL
FPT_TDC.1/CL	No dependencies	
FPT_TIT.1/CL	[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/CL, FMT_MTD.1/CL

Table 2: Dependency rationale

9.2.2 Security functional requirements rationale

The table 3 traces each SFR back to the security objectives for the TOE. Note the security objective O.Audit is defined in the PP-Module PPM-TS-Au.

	O.Audit	O.Cluster
FAU_GEN.1/CL	x	
FCS_CKM.5/CLDH		x
FDP_ACC.1/CL		x
FMT_MTD.1/CL		x
FPT_ESA.1/CL		x
FPT_ISA.1/CL		x
FPT_TCT.1/CL		x
FPT_TDC.1/CL		x
FPT_TIT.1/CL		x

Table 3: Security functional requirement rationale

The security objective for the TOE O.Audit “Audit” is met by the SFR FAU_GEN.1 in PPM-TS-AU and additionally by SFR FAU_GEN.1/CL to generate the audit records of auditable events for clustering.

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

– The SFR FDP_ACC.1/CL defines subjects, objects and operations of the Clustering SFP.

– The SFR FMT_MTD.1/CL restricts the management of TSF data Authentication Data Records and cryptographic key by initiating the cluster to an administrator, and export and import of TSF data to an authorised identified role.

– The SFRs FPT_ESA.1/CL and FPT_ISA.1/CL require that export and import of TSF data is performed with security attributes.

– The SFR FPT_TCT.1/CL requires protection of confidentiality and the SFR FPT_TIT.1/CL the protection of integrity of the TSF data when transferred from Master-CSP to Slave-CSP.

– The SFR FCS_CKM.5/CLDH requires the TSF to agree on cryptographic keys. Note, the Base-PP defines the SFRs FCS_COP.1/ED and FCS_COP.1/MAC for encryption and MAC of the transferred TSF data.

– The SFR FPT_TDC.1/CL requires the TSF interpret consistently the TSF exchanged between TOE samples of the cluster.

10 Reference Documentation

CC1	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
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-TS-Au	BSI, Protection Profile Configuration Cryptographic Service Provider - Time Stamp Service and Audit, BSI-CC-PP-0107-2019, 2019
TR-03111	BSI: Elliptic Curve Cryptography, BSI Technical Guideline TR-03111

Keywords and Abbreviations

Term	Description
authentication reference data	data used by the TOE to verify the authentication attempt of a user
authentication verification data	data used by the user to authenticate themselves to the TOE
authenticity	the property that ensures that the identity of a subject or resource is the one claimed (cf. ISO/IEC 7498-2:1989)
cluster	a system of TOE samples initialized by an administrator and communication through trusted channels in order to manage known users and to share the cryptographic keys
cryptographic key	a variable parameter which is used in a cryptographic algorithm or protocol
data integrity	the property that data has not been altered or destroyed in an unauthorized manner (cf. ISO/IEC 7498-2:1989)
firmware	executable code that is stored in hardware and cannot be dynamically written or modified during execution while operating on a non-modifiable or limited execution platform, cf. ISO/IEC 19790
hardware	physical equipment or comprises the physical components used to process programs and data or to protect physically the processing components, cf. ISO/IEC 19790
Issuer of update code package	Trusted authority issuing an update code package (UCP) and holding the signature private key for signing the UCP and corresponding to the public key implemented in the TOE for verification of the UCP. The issuer is typically the TOE manufacturer. The issuer of an UCP is identified by the security attribute Issuer of the UCP.
private key	confidential key used for asymmetric cryptographic mechanisms like decryption of cipher text, signature-creation or authentication proof, where it is difficult for the adversary to derive the confidential private key from the known public key
public key	public known used for asymmetric cryptographic mechanisms like encryption of cipher text, signature-verification or authentication verification, where it is difficult for the adversary to derive the confidential private key from the known public key
secret key	key of symmetric cryptographic mechanisms, using two identical keys with the same secret value or two different values, where one may be easy calculated from the other one, for complementary operations like encryption / decryption, signature-creation / signature-verification, or authentication proof / authentication verification.

secure channel	a trusted channel which is physically protected and logical separated communication channel between the TOE and the user, or is protected by means of cryptographic mechanisms
software	executable code that is stored on erasable media which can be dynamically written and modified during execution while operating on a modifiable execution platform, cf. ISO/IEC 19790
trusted channel	a means by which a TSF and another trusted IT product can communicate with necessary confidence (cf. CC part 1 [CC1], paragraph 97)
update code package	code if implemented changing the TOE implementation at the end of the TOE life time

Table 4: Glossary

Acronym	Term
A.xxx	Assumption
CC	Common Criteria
CSP	cryptographic service provider
ECC	Elliptic curve cryptography
HMAC	Keyed-Hash Message Authentication Code
KDF	Key derivation function
MAC	Message Authentication Code
n. a.	Not applicable
O.xxx	Security objective for the TOE
OE.xxx	Security objective for the TOE environment
OSP.xxx	Organisational security policy
PACE	Password Authenticated Connection Establishment
PKI	Public key infrastructure
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 5: Abbreviations