Common Security Evaluation &
Certification Consortium
of GBIC and UKF

Common
Security Evaluation & Certification
Consortium

Common.SECC

Rule Book 1.6

Annex 6

Modular Evaluation Guidance

Version 1.0

November 29, 2018

Version	Date	Author	Change
0.1	January 15. 2018	Hanns Groeschke / SRC	First creation considering the proposals from Brightsight and SRC.
0.9	November 27.2018	Hanns Groeschke / SRC	First draft and first complete version
1.0	November 29.2018	Common.SECC	Endorsement by Common.SECC Coordination Committee

Table of Contents

1 Introduction

According to [JTEMS PPV4], strict conformance has to be claimed by the ST author to be conformant to the PP.

This document shall serve as a guidance for POI terminal vendors and ST writers, who cannot strictly claim the underlying protection profile for payment terminals, e.g. by having a TOE which only has a subset of TSFs compared to the definition of TSFs in [JTEMS PPV4]. This guidance shall make sure that even though the PP cannot be claimed strictly, an appropriate level of assurance will be reached by the TOE. The ST shall then clearly clarify that only a subset of TSFs can be claimed by the TOE. Any additions of security functionalities which are not covered by a TSF of the PP have to be clearly marked and described in line with the CC standard by using the terminology and the general approach of the PP.

Chapter 2 of this document is an overview of how the ST, which does not strictly claim [JTEMS PPV4] shall be structured. Chapter 3 gives an example of a recommended approach for the vendor, evaluation lab, and certification bodies on how preparative steps for a certification and an evaluation process could be performed. In Chapter 4 the TSF parts in [JTEMS PPV4] are presented together with the related assets, SFR packages and SFRs as defined in [JTEMS PPV4] which shall give guidance for an appropriate choice of SFRs which have to be included into the ST.

2 Structure of the ST

The ST Author has to consider the following:

2.1 ST introduction:

- Clarify that even though the PP is not claimed strictly, the ST uses the **structure, terminology and general approach of the PP** (for example in terms of definition of different TSF components that require different levels of protection).
- Clarify that the ST covers a **subset of security functional requirements** compared to the original PP. The requirements of the PP that are included in the ST are included with ether no modification or clearly marked refinements.
- Specify whether the ST will include a modified set of requirements from the POI-COMPREHENSIVE+SRED configuration described in PP.
- Provide a description of the **TOE type**. Make sure to specify in what way the TOE is similar/different compared to the TOE type typically in scope of the PP.

2.2 Conformance claims:

- Specify that the ST claims conformance to the CC:
  - - Common Criteria version 3.1 revision 5, CC Part 1
  - - CC Part 2 extended. The extended components are defined in ST and are taken from the [PP] with/without modifications.
  - - CC Part 3 extended. The extended components are defined in ST and are taken from the [PP] with/without modifications.
- Specify that the ST does not claim conformance to PP.
- Specify that the ST does (not) claim conformance to the EAL-POI assurance package.
  - If conformance is claimed, all assurance classes of EAL-POI will be considered in the ST without any addition/deletion/modification.
  - If no conformance is claimed, the ST author must specify which assurance classes are in scope of the evaluation (for simplicity, use the EAL-POI assurance package as much as possible, additions shall be clearly marked).

2.3 Security Problem definition:

- On basis of the TOE type, select the relevant:
  - Assets,
  - subjects,
  - threats,
  - assumptions and
  - OSPs.
- If items are removed (compared to the [PP]), provide a clear rationale of why they are not applicable.
- If items are refined/modified, provide a clear rationale.

- If additional items are introduced, clearly define them.

2.4 Security Objectives for the TOE:

- Specify that the Security Objectives for the TOE are a subset of the security objectives listed in PP (definition of security objectives is critical as this is the basis for selecting the SFRs) In section 4 it is described how to choose the relevant SFRs.
- Provide a clear rationale of why some objectives have been excluded.
- Provide a clear mapping of security objectives to TSF components.

2.5 Security Objectives for the Operational Environment:

- Specify that the Security Objectives for the Operational Environment are taken from the PP with no addition/deletion/modification.

2.6 Rationale between SPD and Security Objectives:

- Specify that the rationale is modified from the one in PP. Make sure that all removed items have been clearly marked and that the rationale still is complete.
- Example:
    - - All O.xxx map to at least one threat
    - - All OE.xxx map to at least one Threat, OSP or Assumption
    - - All Threats map to at least one O.xxx or OE.xxx
    - - All OSPs map to at least one O.xxx or OE.xxx
    - - All Assumptions map to at least one OE.xxx

Objectives	T.MerchUsurp	T.CardholderUsurpCiphPPIN	~~T.CardholderUsurpClearPPIN~~	T.CardholderUsurpEPIN	T.Transaction	T.FundsAmount	~~T.PromptControl~~	T.BadDebt	T. SecureCommunicationLines	~~T.Magstripe~~	T.IllegalCodeInstall	OSP.ApplicationSeparation	OSP.POISurvey	OSP.MercahntSurvey	OSP.KeyManagement	OSP.WellFormedPayApp	A.UserEducation	A.SecureDevices	A.PinAndCardManagement
O.PINEntry			~~x~~	x															
O.EncPIN				x															
O.CipherPPIN		x																	
~~O.ClearPPIN~~			~~x~~																
O.CoreSWHW		x	~~x~~	x															
O.PEDMiddleSWHW		x	~~x~~				~~x~~												
O.PaymentTransaction	x				x	x		x	x										
O.POISW	x				x	x		x	x		x								
O.PaymentApplicationDownload											x								
O.POIApplicationSeparation					x	x		x	x			x							
~~O.PromptControl~~							~~x~~												
~~O.ICCardReader~~		~~x~~	~~x~~																
~~O.MSR~~										~~x~~									
OE.WellFormedPayApp	x	x	~~x~~	x	x	x		x	x							x			
OE.POISurvey	x	x	~~x~~	x	x	x		x	x				x						
OE.MerchantSurvey	x				x	x								x					
OE.UserEducation		x	~~x~~	x															
OE.SecureDevices	x	x	~~x~~	x	x	x		x	x									x	
OE.KeyManagement	x	x		x	x	x		x	x						x				
OE.PinAndCardManagement		x	~~x~~	x															x
OE.LocalDevices	x	x	~~x~~		x	x		x	x										

Table 2 SPD coverage by objectives.

Figure 1 Example of a Rationale between SPD and Security Objectives

2.7 Extended component definition:

- If possible, use the same extended components defined in PP.
- If not possible, make sure to specify in what way, different extended components are applied to the ST → this has particular impact on the AVA_POI component.

2.8 Security Functional Requirements:

- At the beginning of the chapter, specify which packages of requirements from the PP have been taken/deleted/modified and provide a rationale. See chapter 4 on how to choose the TSF parts and all related SFRs.
- Specify that no additional requirements are introduced by the ST with respect to PP.
- Perform all necessary operations (assignments, selections, iterations).
- Provide the Dependencies rationale for all Security Functional Requirements → Note: it has to be taken in accounting for all dependencies. Removal of assets and security objectives may result in unfulfilled dependencies.

2.9 Security Assurance Requirements:

- At the beginning of the chapter, specify which security assurance requirements from the PP have been taken/deleted/modified and provide a rationale.
- Specify that no additional security assurance requirements are introduced by the ST with respect to PP. If additional security assurance requirements are introduced then a clear rational must be provided.
- Provide the Dependencies rationale for all Security Assurance Requirements.

2.10 Rationale between Security Objectives and SFRs:

- Make sure that even considering the removed security objectives and the removed SFRs, the mapping is correct, in the sense that each SFR maps to at least one security objective.

2.11 TOE Summary Specification:

- Make sure to maintain consistency. All chosen SFRs must be discussed.

3 Recommended approach for modular evaluation and certification process

The evaluator ***shall*** examine the ST to determine that all TSF parts which are usually expected to be included for the device under evaluation are presented in the ST. The ST Author has to provide a reasonable justification on the chosen TSF parts. Ideally, the coverage of chosen TSF parts has been coordinated by the vendor with the evaluation lab and the certification body before start of the evaluation and certification process.

For example: A device which has an IC Card Reader cannot be evaluated on basis of a ST which does not claim adequately the ICCR TSF.

4 TSF Parts

This section will show an overview of the TSF structure as defined in [JTEMS PPV4] for each base PP configuration. All TSFs will be presented with its assets and will be mapped to the related SFR packages as described in the PP. Although the SFR package-mappings are already provided in [JTEMS PPV4], the mappings below will help the ST author to choose all relevant TSF parts for the TOE. Each TSF part can be understood as an individual module by the ST Author. The ST Author ***shall*** ensure that all fitting SFRs are included adequately into the ST for each selected TSF part.

Note: The ST Author includes the relevant SFR package only ones into the ST for all TSFs which have the related SFR package. For example: If the CoreTSF and the CoreTSFKeys are relevant, then the ENC_PIN Package will be included into the ST only ones.

4.1 TSF structure as defined in [JTEMS PPV4].

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
PED-ONLY configuration		
CoreTSF PIN, ENC_PIN, PLAIN_PINCleartext, PLAIN_PINCiphertext, PLAIN_PIN, CORE_SW, CORE_HW, ENC_PIN_PK, E2E_PAN_PK, TOE_PAN_SK, E2E_PAN_SK	PIN Entry Package	**PIN Entry Package** FDP_IFC.1.1/PIN_Entry FDP_ITC.1.1/PIN_ENTRY FDP_ITC.1.2/PIN_ENTRY FDP_ITC.1.3/PIN_ENTRY FPT_EMSEC.1.1/PIN_ENTRY FPT_EMSEC.1.2/PIN_ENTRY FIA_UAU.2.1/PIN_ENTRY FIA_UID.1.1/PIN_ENTRY FIA_UID.1.2/PIN_ENTRY FTA_SSL.3.1/PIN_ENTRY

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
	ENC_PIN Package	**ENC_PIN Package** FDP_IFC.1.1/ENC_PIN FDP_IFF.1.1/ENC_PIN FDP_IFF.1.2/ENC_PIN FDP_IFF.1.3/ENC_PIN FDP_IFF.1.4/ENC_PIN FDP_IFF.1.5/ENC_PIN FMT_MSA.1.1/ENC_PIN FMT_SMR.1.1/ENC_PIN FMT_SMR.1.2/ENC_PIN FIA_UID.1.1/ENC_PIN FIA_UID.1.2/ENC_PIN FDP_RIP.1.1/ENC_PIN FDP_RIP.1.1/ENC_PIN FDP_ITT.1.1/ENC_PIN FDP_ITT.1.1/ENC_PIN FTP_TRP.1.1/ENC_PIN FTP_TRP.1.2/ENC_PIN FTP_TRP.1.3/ENC_PIN
	PLAIN_PIN Package	**PLAIN_PIN Package** FDP_IFC.1.1/PLAIN_PIN FDP_IFF.1.1/PLAIN_PIN FDP_IFF.1.2/PLAIN_PIN FDP_IFF.1.3/PLAIN_PIN

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FDP_IFF.1.4/PLAIN_PIN FDP_IFF.1.5/PLAIN_PIN FDP_RIP.1.1/PLAIN_PIN FDP_ITT.1.1/PLAIN_PIN FMT_MSA.1.1/PLAIN_PIN FIA_UID.1.1/PLAIN_PIN FIA_UID.1.2/PLAIN_PIN
	IC Card Reader Package	**IC Card Reader Package** FDP_IFC.1.1/ICCardReader FDP_IFF.1.1/ICCardReader FDP_IFF.1.2/ICCardReader FDP_IFF.1.3/ICCardReader FDP_IFF.1.4/ICCardReader FDP_IFF.1.5/ICCardReader FDP_RIP.1.1/ICCardReader FDP_ITT.1.1/ICCardReader FDP_ACC.1.1/ICCRLoader FDP_ITC.1.1/ICCRLoader FDP_ITC.1.2/ICCRLoader FDP_ITC.1.3/ICCRLoader
	CoreTSF Package	**CoreTSF Package** FPT_TST.1.1/CoreTSF FPT_TST.1.2/CoreTSF FPT_TST.1.3/CoreTSF FPT_FLS.1.1/CoreTSF FDP_ACC.1.1/CoreTSFLoader

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FDP_ITC.1.1/CoreTSFLoader FDP_ITC.1.2/CoreTSFLoader FDP_ITC.1.3/CoreTSFLoader
	Cryptography Package The SFRs of the Cryptography Package shall be iterated as needed by the ST author. The dependencies shall be adapted consequently.	**Cryptography Package** FCS_RND.1.1 FCS_COP.1.1 FDP_ITC.2.1 FDP_ITC.2.2 FDP_ITC.2.3 FDP_ITC.2.4 FDP_ITC.2.5 FTP_ITC.1.1/Crypto FTP_ITC.1.2/Crypto FTP_ITC.1.3/Crypto FPT_TDC.1.1 FPT_TDC.1.2 FPT_PHP.3.1/CoreTSF FPT_EMSEC.1.1/CoreTSF FPT_EMSEC.1.2/CoreTSF FPT_PHP.3.1/ICCardReader FPT_PHP.3.1/MSR (If MSR TSF is used)
	Physical Protection Package related to the TSF part	**Physical Protection Package related to the TSF part** FPT_PHP.3.1/CoreTSF FPT_EMSEC.1.1/CoreTSF FPT_EMSEC.1.2/CoreTSF

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FPT_PHP.3.1/ICCardReader FPT_PHP.3.1/MSR (If MSR TSF is used)
CoreTSFKeys ENC_PIN, Ciphertext PLAIN_PIN, ENC_PIN_SK, PLAIN_PIN_SK	ENC_PIN Package PLAIN_PIN Package	**ENC_PIN Package** FDP_IFC.1.1/ENC_PIN FDP_IFF.1.1/ENC_PIN FDP_IFF.1.2/ENC_PIN FDP_IFF.1.3/ENC_PIN FDP_IFF.1.4/ENC_PIN FDP_IFF.1.5/ENC_PIN FMT_MSA.1.1/ENC_PIN FMT_SMR.1.1/ENC_PIN FMT_SMR.1.2/ENC_PIN FIA_UID.1.1/ENC_PIN FIA_UID.1.2/ENC_PIN FDP_RIP.1.1/ENC_PIN FDP_RIP.1.1/ENC_PIN FDP_ITT.1.1/ENC_PIN FDP_ITT.1.1/ENC_PIN FTP_TRP.1.1/ENC_PIN FTP_TRP.1.2/ENC_PIN FTP_TRP.1.3/ENC_PIN **PLAIN_PIN Package**

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FDP_IFC.1.1/PLAIN_PIN FDP_IFF.1.1/PLAIN_PIN FDP_IFF.1.2/PLAIN_PIN FDP_IFF.1.3/PLAIN_PIN FDP_IFF.1.4/PLAIN_PIN FDP_IFF.1.5/PLAIN_PIN FDP_RIP.1.1/PLAIN_PIN FDP_ITT.1.1/PLAIN_PIN FMT_MSA.1.1/PLAIN_PIN FIA_UID.1.1/PLAIN_PIN FIA_UID.1.2/PLAIN_PIN
	IC Card Reader Package	**IC Card Reader Package** FDP_IFC.1.1/ICCardReader FDP_IFF.1.1/ICCardReader FDP_IFF.1.2/ICCardReader FDP_IFF.1.3/ICCardReader FDP_IFF.1.4/ICCardReader FDP_IFF.1.5/ICCardReader FDP_RIP.1.1/ICCardReader FDP_ITT.1.1/ICCardReader FDP_ACC.1.1/ICCRLoader FDP_ITC.1.1/ICCRLoader FDP_ITC.1.2/ICCRLoader FDP_ITC.1.3/ICCRLoader
	Physical Protection Package related to the TSF part	**Physical Protection Package related to the TSF part**

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FPT_PHP.3.1/CoreTSF FPT_EMSEC.1.1/CoreTSF FPT_EMSEC.1.2/CoreTSF FPT_PHP.3.1/ICCardReader FPT_PHP.3.1/MSR (If MSR TSF is used)
ICCR TSF PLAIN_PIN, ICCR_SW, ICCR_HW, PLAIN_PIN_SK	IC Card Reader Package Physical Protection Package related to the TSF part	**IC Card Reader Package** FDP_IFC.1.1/ICCardReader FDP_IFF.1.1/ICCardReader FDP_IFF.1.2/ICCardReader FDP_IFF.1.3/ICCardReader FDP_IFF.1.4/ICCardReader FDP_IFF.1.5/ICCardReader FDP_RIP.1.1/ICCardReader FDP_ITT.1.1/ICCardReader FDP_ACC.1.1/ICCRLoader FDP_ITC.1.1/ICCRLoader FDP_ITC.1.2/ICCRLoader FDP_ITC.1.3/ICCRLoader **Physical Protection Package related to the TSF part** FPT_PHP.3.1/CoreTSF FPT_EMSEC.1.1/CoreTSF FPT_EMSEC.1.2/CoreTSF FPT_PHP.3.1/ICCardReader FPT_PHP.3.1/MSR (If MSR TSF is used)

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
PEDMiddleTSF Ciphertext PLAIN_PIN, PED_MIDDLE_SW, PED_MIDDLE_HW, PED_MIDDLE_PK, PED_MIDDLE_SK, PLAIN_PIN_SK	PEDMiddleTSF Package	**PEDMiddleTSF Package** FPT_TST.1.1/PEDMiddleTSF FPT_TST.1.2/PEDMiddleTSF FPT_TST.1.3/PEDMiddleTSF FPT_FLS.1.1/PEDMiddleTSF FDP_ACC.1.1/PEDMiddleTSFLoader FDP_ITC.1.1/PEDMiddleTSFLoader FDP_ITC.1.2/PEDMiddleTSFLoader FDP_ITC.1.3/PEDMiddleTSFLoader
	PED Prompt Control Package	**PED Prompt Control Package** FDP_ACC.1.1/PEDPromptControl FDP_ACF.1.1/PEDPromptControl FDP_ACF.1.2/PEDPromptControl FDP_ACF.1.3/PEDPromptControl FDP_ACF.1.4/PEDPromptControl
	Cryptography Package The SFRs of the Cryptography Package shall be iterated as needed by the ST author. The dependencies shall be adapted consequently.	**Cryptography Package** FCS_RND.1.1 FCS_COP.1.1 FDP_ITC.2.1 FDP_ITC.2.2 FDP_ITC.2.3 FDP_ITC.2.4 FDP_ITC.2.5 FTP_ITC.1.1/Crypto FTP_ITC.1.2/Crypto FTP_ITC.1.3/Crypto

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FPT_TDC.1.1 FPT_TDC.1.2 FPT_PHP.3.1/CoreTSF FPT_EMSEC.1.1/CoreTSF FPT_EMSEC.1.2/CoreTSF FPT_PHP.3.1/ICCardReader FPT_PHP.3.1/MSR (If MSR TSF is used)
MSR TSF Magnetic Stripe Track Data	Physical Protection Package related to the TSF part	FPT_PHP.3.1/MSR
POI COMPREHENSIVE configuration		
CoreTSF PIN, ENC_PIN, PLAIN_PINCleartext, PLAIN_PINCiphertext, PLAIN_PIN, CORE_SW, CORE_HW, ENC_PIN_PK	PIN Entry Package ENC_PIN Package	**PIN Entry Package** FDP_IFC.1.1/PIN_Entry FDP_ITC.1.1/PIN_ENTRY FDP_ITC.1.2/PIN_ENTRY FDP_ITC.1.3/PIN_ENTRY FPT_EMSEC.1.1/PIN_ENTRY FPT_EMSEC.1.2/PIN_ENTRY FIA_UAU.2.1/PIN_ENTRY FIA_UID.1.1/PIN_ENTRY FIA_UID.1.2/PIN_ENTRY FTA_SSL.3.1/PIN_ENTRY **ENC_PIN Package** FDP_IFC.1.1/ENC_PIN FDP_IFF.1.1/ENC_PIN FDP_IFF.1.2/ENC_PIN

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FDP_IFF.1.3/ENC_PIN FDP_IFF.1.4/ENC_PIN FDP_IFF.1.5/ENC_PIN FMT_MSA.1.1/ENC_PIN FMT_SMR.1.1/ENC_PIN FMT_SMR.1.2/ENC_PIN FIA_UID.1.1/ENC_PIN FIA_UID.1.2/ENC_PIN FDP_RIP.1.1/ENC_PIN FDP_RIP.1.1/ENC_PIN FDP_ITT.1.1/ENC_PIN FDP_ITT.1.1/ENC_PIN FTP_TRP.1.1/ENC_PIN FTP_TRP.1.2/ENC_PIN FTP_TRP.1.3/ENC_PIN
	PLAIN_PIN Package	**PLAIN_PIN Package** FDP_IFC.1.1/PLAIN_PIN FDP_IFF.1.1/PLAIN_PIN FDP_IFF.1.2/PLAIN_PIN FDP_IFF.1.3/PLAIN_PIN FDP_IFF.1.4/PLAIN_PIN FDP_IFF.1.5/PLAIN_PIN FDP_RIP.1.1/PLAIN_PIN FDP_ITT.1.1/PLAIN_PIN FMT_MSA.1.1/PLAIN_PIN FIA_UID.1.1/PLAIN_PIN

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FIA_UID.1.2/PLAIN_PIN
	CoreTSF Package	**CoreTSF Package** FPT_TST.1.1/CoreTSF FPT_TST.1.2/CoreTSF FPT_TST.1.3/CoreTSF FPT_FLS.1.1/CoreTSF FDP_ACC.1.1/CoreTSFLoader FDP_ITC.1.1/CoreTSFLoader FDP_ITC.1.2/CoreTSFLoader FDP_ITC.1.3/CoreTSFLoader
	Cryptography Package The SFRs of the Cryptography Package shall be iterated as needed by the ST author. The dependencies shall be adapted consequently.	**Cryptography Package** FCS_RND.1.1 FCS_COP.1.1 FDP_ITC.2.1 FDP_ITC.2.2 FDP_ITC.2.3 FDP_ITC.2.4 FDP_ITC.2.5 FTP_ITC.1.1/Crypto FTP_ITC.1.2/Crypto FTP_ITC.1.3/Crypto FPT_TDC.1.1 FPT_TDC.1.2 FPT_PHP.3.1/CoreTSF FPT_EMSEC.1.1/CoreTSF FPT_EMSEC.1.2/CoreTSF

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
	Physical Protection Package related to the TSF part	FPT_PHP.3.1/ICCardReader FPT_PHP.3.1/MSR (If MSR TSF is used) **Physical Protection Package related to the TSF part** FPT_PHP.3.1/CoreTSF FPT_EMSEC.1.1/CoreTSF FPT_EMSEC.1.2/CoreTSF FPT_PHP.3.1/ICCardReader FPT_PHP.3.1/MSR (If MSR TSF is used)
CoreTSFKeys ENC_PIN, Ciphertext PLAIN_PIN, ENC_PIN_SK, PLAIN_PIN_SK	ENC_PIN Package	**ENC_PIN Package** FDP_IFC.1.1/ENC_PIN FDP_IFF.1.1/ENC_PIN FDP_IFF.1.2/ENC_PIN FDP_IFF.1.3/ENC_PIN FDP_IFF.1.4/ENC_PIN FDP_IFF.1.5/ENC_PIN FMT_MSA.1.1/ENC_PIN FMT_SMR.1.1/ENC_PIN FMT_SMR.1.2/ENC_PIN FIA_UID.1.1/ENC_PIN FIA_UID.1.2/ENC_PIN FDP_RIP.1.1/ENC_PIN FDP_RIP.1.1/ENC_PIN FDP_ITT.1.1/ENC_PIN FDP_ITT.1.1/ENC_PIN FTP_TRP.1.1/ENC_PIN FTP_TRP.1.2/ENC_PIN

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FTP_TRP.1.3/ENC_PIN
	PLAIN_PIN Package	**PLAIN_PIN Package** FDP_IFC.1.1/PLAIN_PIN FDP_IFF.1.1/PLAIN_PIN FDP_IFF.1.2/PLAIN_PIN FDP_IFF.1.3/PLAIN_PIN FDP_IFF.1.4/PLAIN_PIN FDP_IFF.1.5/PLAIN_PIN FDP_RIP.1.1/PLAIN_PIN FDP_ITT.1.1/PLAIN_PIN FMT_MSA.1.1/PLAIN_PIN FIA_UID.1.1/PLAIN_PIN FIA_UID.1.2/PLAIN_PIN
	IC Card Reader Package	**IC Card Reader Package** FDP_IFC.1.1/ICCardReader FDP_IFF.1.1/ICCardReader FDP_IFF.1.2/ICCardReader FDP_IFF.1.3/ICCardReader FDP_IFF.1.4/ICCardReader FDP_IFF.1.5/ICCardReader FDP_RIP.1.1/ICCardReader FDP_ITT.1.1/ICCardReader FDP_ACC.1.1/ICCRLoader FDP_ITC.1.1/ICCRLoader FDP_ITC.1.2/ICCRLoader FDP_ITC.1.3/ICCRLoader

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
	Physical Protection Package related to the TSF part	**Physical Protection Package related to the TSF part** FPT_PHP.3.1/CoreTSF FPT_EMSEC.1.1/CoreTSF FPT_EMSEC.1.2/CoreTSF FPT_PHP.3.1/ICCardReader FPT_PHP.3.1/MSR (If MSR TSF is used)
ICCR TSF PLAIN_PIN, ICCR_SW, ICCR_HW, PLAIN_PIN_SK	IC Card Reader Package	**IC Card Reader Package** FDP_IFC.1.1/ICCardReader FDP_IFF.1.1/ICCardReader FDP_IFF.1.2/ICCardReader FDP_IFF.1.3/ICCardReader FDP_IFF.1.4/ICCardReader FDP_IFF.1.5/ICCardReader FDP_RIP.1.1/ICCardReader FDP_ITT.1.1/ICCardReader FDP_ACC.1.1/ICCRLoader FDP_ITC.1.1/ICCRLoader FDP_ITC.1.2/ICCRLoader FDP_ITC.1.3/ICCRLoader
	Physical Protection Package related to the TSF part	**Physical Protection Package related to the TSF part** FPT_PHP.3.1/CoreTSF FPT_EMSEC.1.1/CoreTSF FPT_EMSEC.1.2/CoreTSF

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FPT_PHP.3.1/ICCardReader FPT_PHP.3.1/MSR (If MSR TSF is used)
PEDMiddleTSF POI_SW, MAN_DAT, PAY_DAT, PED_MIDDLE_PK, PED_MIDDLE_SK, PLAIN_PIN_SK	PEDMiddleTSF Package	**PEDMiddleTSF Package** FPT_TST.1.1/PEDMiddleTSF FPT_TST.1.2/PEDMiddleTSF FPT_TST.1.3/PEDMiddleTSF FPT_FLS.1.1/PEDMiddleTSF FDP_ACC.1.1/PEDMiddleTSFLoader FDP_ITC.1.1/PEDMiddleTSFLoader FDP_ITC.1.2/PEDMiddleTSFLoader FDP_ITC.1.3/PEDMiddleTSFLoader
	PED Prompt Control Package	**PED Prompt Control Package** FDP_ACC.1.1/PEDPromptControl FDP_ACF.1.1/PEDPromptControl FDP_ACF.1.2/PEDPromptControl FDP_ACF.1.3/PEDPromptControl FDP_ACF.1.4/PEDPromptControl
	Cryptography Package The SFRs of the Cryptography Package shall be iterated as needed by the ST author. The dependencies shall be adapted consequently.	**Cryptography Package** FCS_RND.1.1 FCS_COP.1.1 FDP_ITC.2.1 FDP_ITC.2.2 FDP_ITC.2.3 FDP_ITC.2.4 FDP_ITC.2.5

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FTP_ITC.1.1/Crypto FTP_ITC.1.2/Crypto FTP_ITC.1.3/Crypto FPT_TDC.1.1 FPT_TDC.1.2 FPT_PHP.3.1/CoreTSF FPT_EMSEC.1.1/CoreTSF FPT_EMSEC.1.2/CoreTSF FPT_PHP.3.1/ICCardReader FPT_PHP.3.1/MSR (If MSR TSF is used)
MiddleTSF POI_SW, MAN_DAT, MAN_DAT, SRED Account Data (If SRED module is added), POI_PK, POI_SK, PAY-MENT_APP	POI_DATA Package	**POI_DATA Package** FDP_ACC.1.1/POI_DATA FDP_ACF.1.1/POI_DATA FDP_ACF.1.2/POI_DATA FDP_ACF.1.3/POI_DATA FDP_ACF.1.4/POI_DATA FDP_ITT.1.1/POI_DATA FDP_UIT.1.1/POI_DATA FDP_UIT.1.2/POI_DATA FDP_UCT.1.1/POI_DATA FDP_RIP.1.1/POI_DATA FTP_ITC.1.1/POI_DATA FTP_ITC.1.2/POI_DATA FTP_ITC.1.3/POI_DATA
	MiddleTSF Package	**MiddleTSF Package** FDP_ACC.1.1/ApplicationLoader FDP_ITC.1.1/ApplicationLoader

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FDP_ITC.1.2/ApplicationLoader FDP_ITC.1.3/ApplicationLoader FDP_ACC.1.1/MiddleTSFLoader FDP_ITC.1.1/MiddleTSFLoader FDP_ITC.1.2/MiddleTSFLoader FDP_ITC.1.3/MiddleTSFLoader FPT_FLS.1.1/MiddleTSF
	Cryptography Package The SFRs of the Cryptography Package shall be iterated as needed by the ST author. The dependencies shall be adapted consequently.	**Cryptography Package** FCS_RND.1.1 FCS_COP.1.1 FDP_ITC.2.1 FDP_ITC.2.2 FDP_ITC.2.3 FDP_ITC.2.4 FDP_ITC.2.5 FTP_ITC.1.1/Crypto FTP_ITC.1.2/Crypto FTP_ITC.1.3/Crypto FPT_TDC.1.1 FPT_TDC.1.2 FPT_PHP.3.1/CoreTSF FPT_EMSEC.1.1/CoreTSF FPT_EMSEC.1.2/CoreTSF FPT_PHP.3.1/ICCardReader FPT_PHP.3.1/MSR (If MSR TSF is used)
MSR TSF	Physical Protection Package related to the TSF part	FPT_PHP.3.1/MSR

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
Magnetic Stripe Track Data		
POI-CHIP.ONLY configuration		
CoreTSF PIN, ENC_PIN, CORE_SW, CORE_HW, ENC_PIN_PK, ENC_PIN_SK, POI_PayDatSK	PIN Entry Package	**PIN Entry Package** FDP_IFC.1.1/PIN_Entry FDP_ITC.1.1/PIN_ENTRY FDP_ITC.1.2/PIN_ENTRY FDP_ITC.1.3/PIN_ENTRY FPT_EMSEC.1.1/PIN_ENTRY FPT_EMSEC.1.2/PIN_ENTRY FIA_UAU.2.1/PIN_ENTRY FIA_UID.1.1/PIN_ENTRY FIA_UID.1.2/PIN_ENTRY FTA_SSL.3.1/PIN_ENTRY
	ENC_PIN Package	**ENC_PIN Package** FDP_IFC.1.1/ENC_PIN FDP_IFF.1.1/ENC_PIN FDP_IFF.1.2/ENC_PIN FDP_IFF.1.3/ENC_PIN FDP_IFF.1.4/ENC_PIN FDP_IFF.1.5/ENC_PIN FMT_MSA.1.1/ENC_PIN FMT_SMR.1.1/ENC_PIN FMT_SMR.1.2/ENC_PIN FIA_UID.1.1/ENC_PIN FIA_UID.1.2/ENC_PIN FDP_RIP.1.1/ENC_PIN

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FDP_RIP.1.1/ENC_PIN FDP_ITT.1.1/ENC_PIN FDP_ITT.1.1/ENC_PIN FTP_TRP.1.1/ENC_PIN FTP_TRP.1.2/ENC_PIN FTP_TRP.1.3/ENC_PIN
	CoreTSF Package	**CoreTSF Package** FPT_TST.1.1/CoreTSF FPT_TST.1.2/CoreTSF FPT_TST.1.3/CoreTSF FPT_FLS.1.1/CoreTSF FDP_ACC.1.1/CoreTSFLoader FDP_ITC.1.1/CoreTSFLoader FDP_ITC.1.2/CoreTSFLoader FDP_ITC.1.3/CoreTSFLoader
	Cryptography Package The SFRs of the Cryptography Package shall be iterated as needed by the ST author. The dependencies shall be adapted consequently.	**Cryptography Package** FCS_RND.1.1 FCS_COP.1.1 FDP_ITC.2.1 FDP_ITC.2.2 FDP_ITC.2.3 FDP_ITC.2.4 FDP_ITC.2.5 FTP_ITC.1.1/Crypto FTP_ITC.1.2/Crypto FTP_ITC.1.3/Crypto

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FPT_TDC.1.1 FPT_TDC.1.2 FPT_PHP.3.1/CoreTSF FPT_EMSEC.1.1/CoreTSF FPT_EMSEC.1.2/CoreTSF FPT_PHP.3.1/ICCardReader
	Physical Protection Package related to the TSF part	**Physical Protection Package related to the TSF part** FPT_PHP.3.1/CHIP-ONLY FPT_EMSEC.1.1/CHIP-ONLY FPT_EMSEC.1.2/CHIP-ONLY
PEDMiddleTSF PED_MIDDLE_SW, PED_MIDDLE_HW, PED_MIDDLE_PK, PED_MIDDLE_SK	PEDMiddleTSF Package	**PEDMiddleTSF Package** FPT_TST.1.1/PEDMiddleTSF FPT_TST.1.2/PEDMiddleTSF FPT_TST.1.3/PEDMiddleTSF FPT_FLS.1.1/PEDMiddleTSF FDP_ACC.1.1/PEDMiddleTSFLoader FDP_ITC.1.1/PEDMiddleTSFLoader FDP_ITC.1.2/PEDMiddleTSFLoader FDP_ITC.1.3/PEDMiddleTSFLoader
	PED Prompt Control Package	**PED Prompt Control Package** FDP_ACC.1.1/PEDPromptControl FDP_ACF.1.1/PEDPromptControl FDP_ACF.1.2/PEDPromptControl FDP_ACF.1.3/PEDPromptControl

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
	Cryptography Package The SFRs of the Cryptography Package shall be iterated as needed by the ST author. The dependencies shall be adapted consequently.	FDP_ACF.1.4/PEDPromptControl **Cryptography Package** FCS_RND.1.1 FCS_COP.1.1 FDP_ITC.2.1 FDP_ITC.2.2 FDP_ITC.2.3 FDP_ITC.2.4 FDP_ITC.2.5 FTP_ITC.1.1/Crypto FTP_ITC.1.2/Crypto FTP_ITC.1.3/Crypto FPT_TDC.1.1 FPT_TDC.1.2 FPT_PHP.3.1/CoreTSF FPT_EMSEC.1.1/CoreTSF FPT_EMSEC.1.2/CoreTSF FPT_PHP.3.1/ICCardReader
MiddleTSF POI_SW, MAN_DAT, PAY_DAT, POI_PK, POI_SK, PAYMENT_APP	POI_DATA Package	**POI_DATA Package** FDP_ACC.1.1/POI_DATA FDP_ACF.1.1/POI_DATA FDP_ACF.1.2/POI_DATA FDP_ACF.1.3/POI_DATA FDP_ACF.1.4/POI_DATA FDP_ITT.1.1/POI_DATA FDP_UIT.1.1/POI_DATA FDP_UIT.1.2/POI_DATA

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FDP_UCT.1.1/POI_DATA FDP_RIP.1.1/POI_DATA FTP_ITC.1.1/POI_DATA FTP_ITC.1.2/POI_DATA FTP_ITC.1.3/POI_DATA
	MiddleTSF Package	**MiddleTSF Package** FDP_ACC.1.1/ApplicationLoader FDP_ITC.1.1/ApplicationLoader FDP_ITC.1.2/ApplicationLoader FDP_ITC.1.3/ApplicationLoader FDP_ACC.1.1/MiddleTSFLoader FDP_ITC.1.1/MiddleTSFLoader FDP_ITC.1.2/MiddleTSFLoader FDP_ITC.1.3/MiddleTSFLoader FPT_FLS.1.1/MiddleTSF
	Cryptography Package The SFRs of the Cryptography Package shall be iterated as needed by the ST author. The dependencies shall be adapted consequently.	**Cryptography Package** FCS_RND.1.1 FCS_COP.1.1 FDP_ITC.2.1 FDP_ITC.2.2 FDP_ITC.2.3 FDP_ITC.2.4 FDP_ITC.2.5 FTP_ITC.1.1/Crypto FTP_ITC.1.2/Crypto FTP_ITC.1.3/Crypto

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FPT_TDC.1.1 FPT_TDC.1.2 FPT_PHP.3.1/CoreTSF FPT_EMSEC.1.1/CoreTSF FPT_EMSEC.1.2/CoreTSF FPT_PHP.3.1/ICCardReader
SRED		
SRED PP-Module PAY_DAT, PAN, TOE_CLEAR_PAN, TOE_CIPHER_PAN, TOE_PAN_SK, E2E_CIPHER_PAN, E2E_PAN_PK, E2E_PAN_SK, SURROGATE_PAN, SURROGATE_PAN_SALT	SRED Basis Package	**SRED Basis Package** FMT_SMR.1.1/SRED FMT_SMR.1.2/SRED FIA_UID.1.1/SRED FIA_UID.1.2/SRED FDP_ITC.1.1/SRED FDP_ITC.1.2/SRED FDP_ITC.1.3/SRED FPT_FLS.1.1/SRED FIA_UAU.2.1/SRED FDP_ACC.1.1/SRED FDP_ACF.1.1/SRED FDP_ACF.1.2/SRED FDP_ACF.1.3/SRED FDP_ACF.1.4/SRED FTA_SSL.3.1/SRED FPT_PHP.3.1/SRED

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FPT_EMSEC.1.1/SRED FPT_EMSEC.1.2/SRED FMT_MSA.1.1/SRED FPT_TST.1.1/SRED FPT_TST.1.2/SRED FPT_TST.1.3/SRED FTP_ITC.1.1/SRED FTP_ITC.1.2/SRED FTP_ITC.1.3/SRED
	SRED Cryptography Package	**SRED Cryptography Package** FTP_ITC.1.1/SRED_CRYPTO FTP_ITC.1.2/SRED_CRYPTO FTP_ITC.1.3/SRED_CRYPTO FPT_TDC.1.1/SRED_CRYPTO FPT_TDC.1.2/SRED_CRYPTO FDP_ITC.2.1/SRED_CRYPTO FDP_ITC.2.2/SRED_CRYPTO FDP_ITC.2.3/SRED_CRYPTO FDP_ITC.2.4/SRED_CRYPTO FDP_ITC.2.5/SRED_CRYPTO FCS_COP.1.1/SRED_CRYPTO
	SRED Distributed Architecture Package (if TOE has a distributed architecture)	**SRED Distributed Architecture Package (if TOE has a distributed architecture)** FDP_IFC.1.1/SRED_INT

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FDP_IFF.1.1/SRED_INT FDP_IFF.1.2/SRED_INT FDP_IFF.1.3/SRED_INT FDP_IFF.1.4/SRED_INT FDP_IFF.1.5/SRED_INT FDP_ITT.1.1/SRED_INT FMT_MSA.1.1/SRED_INT FDP_RIP.1.1/SRED_INT
	SRED End-to-end protection Package This package has to be added in any configuration	**SRED End-to-end protection Package** FDP_IFC.1.1/SRED_E2E FDP_IFF.1.1/SRED_E2E FDP_IFF.1.2/SRED_E2E FDP_IFF.1.4/SRED_E2E FDP_IFF.1.5/SRED_E2E FMT_MSA.1.1/SRED_E2E FIA_UID.1.1/SRED_E2E FIA_UID.1.2/SRED_E2E FDP_RIP.1.1/SRED_E2E FDP_ITT.1.1/SRED_E2E FTP_TRP.1.1/SRED_E2E FTP_TRP.1.2/SRED_E2E FTP_TRP.1.3/SRED_E2E
	SRED Surrogate PAN Package This package has to be added if the TOE enables the creation of surrogate values for the PAN	**SRED Surrogate PAN Package** FCS_COP.1.1/SRED_SURROGATE_PAN FDP_IFC.1.1/SRED_SURROGATE_PAN FDP_IFF.1.1/SRED_SURROGATE_PAN

TSF Part / **Assets in [JTEMS PPV4] of corresponding TSF part / Module**	**Related SFR packages from [JTEMS PPV4] to be added into the ST**	**SFRs from [JTEMS PPV4] to be added into the ST**
		FDP_IFF.1.2/SRED_SURROGATE_PAN FDP_IFF.1.3/SRED_SURROGATE_PAN FDP_IFF.1.4/SRED_SURROGATE_PAN FDP_IFF.1.5/SRED_SURROGATE_PAN

5 References

[JTEMS PPV4] OSeC Point of Interaction Protection Profile, 06.03.2015, Version 4.0 www.commoncriteriaportal.org/pps/