Joint Interpretation Library

PP0084: Changes and Compliance to PP0035 and Transition Phase

JIL application note on the transition from BSI-PP-0035-2007 to BSI-CC-PP-0084-2014

Version 1.1
August 2014

This page is intentionally left blank

Table of contents

1 Objective

1 The protection profile “Security IC Platform Protection Profile with Augmentation Packages” [PP0084] has been developed to replace the protection profile “Security IC Platform Protection Profile” [PP0035] for the Common Criteria certification of the Security IC platforms.

2 The purpose of this application note is to facilitate a smart transition for the usage of the PP0035 and PP0084, while clarifying the relationship between PP0035 and PP0084.

3 This application note:

a) summarizes the changes made in the PP0084 Protection Profile,

b) defines the compliance of PP0084 to PP0035, for Common Criteria certification processes which are referencing to PP0035 and

c) defines the transition phase for the usage of the PP0035 and PP0084.

2 Changes from PP0035 to PP0084

4 Protection Profile PP0084 has been developed as an evolution of PP0035 with the purpose of bringing it up to date with the security requirements for new Security IC platforms. The changes involve the addition of some new security features and the removal of some security features which are no longer applicable.

5 The new security features formalize the security functional requirements “Stored data confidentiality”(FDP_SDC.1) and“Stored data integrity monitoring and action” (FDP_SDI.2).

6 Further, the security functional requirement “Random Number Generation” (FCS RNG.1) allows the possibility of defining in addition to the physical random number generator defined in PP0035, a hybrid physical or hybrid deterministic random number generator.

7 In addition, the optional packages “Authentication of the Security IC”, “Packages for Loader” and “Packages for Cryptographic Services” are added to standardize the security requirements for flash loading of software, and for cryptographic support.

8 The features which have been removed are the assumption A.Plat-Appl in the security problem definition, and the corresponding security objective OE.Plat-Appl which are no longer considered applicable.

9 Some editorial changes have also been made which improve the intelligibility of the text in PP0084 and which bring the literature references up to date. These improvements do not concern the security functional requirements and security statements.

10 Compared to PP0035, PP0084 offers extended possibilities, therefore it is recommended that PP0084 is referenced instead of PP0035 in any new composite Protection Profile. Please refer to Annex A (informative) for a more detailed description of the differences.

3 Compliance of PP0084 to PP0035

11 The new protection profile PP0084 can be generally considered to be a superset of the protection profile PP0035 on which it is based and therefore includes all security requirements of the PP0035.Therefore, for composite evaluations, the protection profile PP0084 is mostly compliant to the protection profile PP0035 so that products evaluated according to PP0084 may be used alternatively to PP0035 where PP0035 is referenced.

12 Specific care has to be taken for a certain choice of the optional packages and SFR operations offered in PP0084 only. In addition, the application of Loader mechanisms may affect Life-Cycle aspects of the TOE and shall not contradict to the Life-Cycle as defined within the PP.

13 This application note does not describe how to use PP0084 to achieve maximum conformity with PP0035. Therefore, the composite product evaluator is in charge to assess the correct re-use of a platform ST in those differing areas of the two PPs as it is needed for the composite TOE security policy.

14 For the case that an ST for a composite TOE

- claims conformance to a composite PP containing itself a conformance claim to the PP0035 and
- covers a TOE whose underlying IC claims conformance to PP 0084

or for the case that an ST for a composite TOE

- claims conformance to a composite PP containing itself a conformance claim to the PP0084 and
- covers a TOE whose underlying IC claims conformance to the PP 0035

15 it has to be ensured that the ST respective its composite TOE with the underlying IC do not contradict the original intention of the claimed composite PP. This includes the security problem definition, definition of security objectives and choice of security functional requirements, specifically those items to be provided by the platform.

16 The composite product evaluator has to check the ST of the composite TOE for this requirement within his composite related evaluation tasks (ASE_COMP.1.x). In particular, this is related to the contents of the PP0084 that deviates from the contents of PP0035 and are explicitly chosen for the composite TOE (in the first case) or composite PP (in the second case).

4 Transition phase

17 New applications for certification claiming compliance to either PP0035 or PP0084 can be filed until December 31, 2014.

18 From January 1st, 2015 onwards, new applications claiming conformance according to PP0035 won't be accepted.

19 Current products which have been certified using PP0035 may continue to be maintained using this protection profile (i.e. re-assessment, maintenance, re-certification). This means that a change to be compliant to PP0084 is not required but can be done on a voluntary basis.

20 Remark: It may be the case that some tenders for new projects will require compliance to PP0084 (instead of PP0035). The 'owner' of the tender is kindly requested to consider to also accept PP0035 compliant products in order to allow providers to offer products from their product portfolio that are still only compliant to PP0035 (just for historical reasons). This might be valid for a period until only PP0084 compliant products are on the market..

5 Reference

[PP0084] Eurosmart Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, BSI-CC-PP-0084-2014

[PP0035] Eurosmart Security IC Platform Protection Profile, Version 1.0, July 2007, BSI-PP-0035-2007

Annex A (informative)

DIFFERENCES BETWEEN SECURITY TARGETS CLAIMING CONFORMANCE TO BSI-CC-PP-0084-2014 AND BSI-PP-0035-2007

The Security IC Platform Protection Profile, Version 1.0, 15.06.2007, BSI-CC-PP-0035, was updated by the Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, BSI-CC-PP-0084. This annex provides a detailed description of the differences between security targets claiming conformance to these protection profiles.

Both PPs require strict conformance for a PP or ST claiming conformance to it. Strict conformance requires in essence, the ST specifies that the TOE does at least the same as in the PP, while the operational environment does at most the same as in the PP (cf. CC part 1, paragraph 480). The assurance family ASE_CCL in CC part 3 defines the requirements for conformance of a PP or ST to a PP like this: The conformance claim rationale shall demonstrate that the statement of the security problem definition (ASE_CCL.1.8C), security objectives (ASE_CCL.1.9C) and security requirements (ASE_CCL.1.10C) are consistent with the statement of the respective statements in the PPs for which conformance is being claimed. The CEM work units ASE_CCL.1-10, ASE_CCL.1-11 and ASE_CCL.1-12 define the concrete rules for the consistency.

The BSI-CC-PP-0084 update of BSI-CC-PP-0035 can be summarised in respect of the conformance claim like this:

- Clarification of user data and TSF data of the TOE and a composite TOE including the TOE of the PP implying editorial changes of security problem definition and security objectives,
- Keeping the security problem definition and security objectives for the TOE except editorial adaption but removing the assumption A.Plat-Appl and the security objective OE.Plat-Appl,
- Keeping all SFR but extending the SFR FCS_RNG.1 and adding two SFR FDP_SDC.1 and FDP_SDI.2. traced back to existing security objectives for the TOE.

In more details, a ST implementing the security problem definition, the security objective and the SFR as defined in BSI-PP-CC-0084 and being conformant to BSI-CC-PP-0084 shall perform appropriate operation for the FCS_RNG.1 to be conformant BSI-CC-PP-0035. A conformance claim rationale of such ST may demonstrate the conformance to BSI-CC-PP-0035 as follow.

The threats T.Leak-Inherent, T.Leak-Forced, the organizational security policy P.Process-TOE, the assumption A.Process-Sec-IC, the security objectives for the TOE O.Leak-Inherent O.Malfunction, O.Leak-Forced, O.Identification are stated identically in BSI-CC-PP-0084 and BSI-CC-PP-0035.

The threats T.Phys-Probing, T.Malfunction, and T.Phys-Manipulation, the security objective for the TOE O.Abuse-Func and the security objective for the operational environment OE.Resp-Appl are expressing the same content by editorial updated text. Note the IC Embedded Software is user data of the Security IC Platform as TOE of the PP but part of the TSF implementation of a composite TOE like smartcards including the Security IC Platform. The user data of such composite TOE include the user data of the Security IC Platform except the IC Embedded Software and the user data of the IC Dedicated Software.

The O.Phys-Manipulation in BSI-CC-PP-0084 describes more precisely protection as BSI-CC-PP-0035:

- of “the Security IC Embedded Software and the user data of the Composite TOE “ instead of “the Security IC Embedded Software and the User Data“ and
- against “undetected manipulation of memory contents “ instead of “controlled manipulation of memory contents”.

The O.Phys-Probing in BSI-CC-PP-0035 states: “The TOE must provide protection against disclosure of User Data, against the disclosure/reconstruction of the Security IC Embedded Software or against the disclosure of other critical information about the operation of the TOE”. It is met by the SFR “Basic internal transfer protection (FDP_ITT.1)” for user data, “Basic internal TSF data transfer protection (FPT_ITT.1)” and Subset information flow control (FDP_IFC.1) with the Data Processing Policy on all confidential data when they are processed or transferred by the TOE or by the Security IC Embedded Software. The security objectives O.Phys-Probing in BSI-CC-PP-0084 is updated in order to address the protection of confidentiality of data stored in protected memory areas as well. It states: “The TOE must provide protection against disclosure/reconstruction of user data while stored in protected memory areas and processed or against the disclosure of other critical information about the operation of the TOE”. This specific aspect of protection is met by the additional SFR “Stored data confidentiality (FDP_SDC.1)”.

SFR FDP_SDC.1 and FDP_SDI.2. traced back to security objectives O.Phys-Manipulation and O.Phys-Probing discussed above.

The BSI-CC-PP-0084 includes all SFR of BSI-CC-PP-0035 but

- changing the definition of the family FCS_RNG and the SFR FCS_RNG.1,
- adding two SFR FDP_SDC.1 and FDP_SDI.2.

The BSI-CC-PP-0084 updated the extended component definition of FCS_RNG.1 by

- splitting the random number generator(RNG) class “hybrid” defined in the element FCS_RNG.1.1 in BSI-CC-PP-0035 into two classes “hybrid physical” and “hybrid deterministic” explained in the application note to FCS_RNG.1,
- providing an addition selection [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*] in the element FCS_RNG.1.2 for clarification of the output format.

The ST shall perform specific operations of the SFR RNG.1 as defined in BSI-CC-PP-0084 for conformance with BSI-CC-PP-0035. Here are three examples for appropriate operations highlighted by underlined printing.

Example 1:

FCS_RNG.1	**Random number generation**
FCS_RNG.1.1	The TSF shall provide a physical random number generator that implements: total failure test of the random source.
FCS_RNG.1.2	The TSF shall provide octets of bits that meet independent bits with Shannon entropy of 7.976 bits per octet.

Example 2:

FCS_RNG.1	**Random number generation**
FCS_RNG.1.1	The TSF shall provide a physical random number generator that implements: total failure test of the random source.
FCS_RNG.1.2	The TSF shall provide octets of bits that meet Min-entropy of 7.95 bit per octet.

Example 3:

FCS_RNG.1	**Random number generation**
FCS_RNG.1.1	The TSF shall provide a hybrid physical random number generator that implements: total failure test of the random source.
FCS_RNG.1.2	The TSF shall provide octets of bits that meet Min-entropy of 7.95 bit per octet.

The RNG class “hybrid physical RNG” includes the RNG class “physical RNG”. Note that the ST writer may assign additional security capabilities in the element FCS_COP.1.1 and other comparable quality metric of the RNG output in the element FCS_COP.1.2. The quality metric Shannon entropy may not appropriate for hybrid physical RNG with cryptographic post-processing.