Assurance Continuity Maintenance Report

BSI-DSZ-CC-0281-2005-MA-01

JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 2.01

from

Gemplus SA

Common Criteria Arrangement

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements,* version 1.0, February 2004 and the developers Impact Analysis Report (IAR). The baseline for this assessment was the Certification Report, the Security Target and the Evaluation Technical Report of the product certified by the Federal Office for Information Security (BSI) under BSI-DSZ-CC-0281-2005.

The change to the certified product is at Source Code level where the format of a data field was not compliant to an expected standard, a change that has no effect on assurance. The identification of the maintained product is indicated by a new version number compared to the baseline certification.

Consideration of the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

Therefore, the assurance as outlined in the Certification Report BSI-DSZ-CC-0281-2005 is maintained for this version of the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-0281-2005.

Bonn, 18 July 2006

Assessment

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements* [1] and the Impact Analysis Report (IAR) [2]. The baseline for this assessment was the Certification Report of the certified TOE [3], the Security Target [4] and the Evaluation Technical Report as outlined in [3].

The vendor for the JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 2.01, Gemplus SA, submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy requirements outlined in the document *Assurance Continuity: CCRA Requirements* [1]. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated as a result of the changes and the security impact of the changes.

The JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 2.01 was changed due to the format of a data field which has been specified by Gemplus as part of the Functional Specification documentation in a way that was not compliant to the expected standard PKCS#1. The change is not significant from the standpoint of security, however Configuration Management procedures required a change in the version number from 1.0 to 2.01. Relevant documents were updated and the Security Target [5] was updated due to editorial changes.

The TOE deliverables have changed as follows (the numbers refer to table 15 in [3] where the items there are exchanged for the following items):

No	Type	Identifier	Release	Form of Delivery
3	SW	Digital Signature application GemSAFE V2	V2 version 2.01	Software in ROM and EEPROM
4	DOC	Card Initialization Specification For GemXpresso Pro R3.2 E64 PK CC	A15	Document in paper / electronic form [7]
9	DOC	GemSafe V2 Applet Reference Manual	6	Document in paper / electronic form [8]

Table 1: Deliverables of the TOE

Conclusion

The change to the TOE is at Source Code level where the format of a data field was not compliant to an expected standard, a change that has no effect on assurance. Examination of the evidence indicates that the changes required are limited to the items listed in table 1. Consideration of the nature of the change leads to the conclusion that it is classified as a minor change and that certificate maintenance is the correct path to continuity of assurance.

Therefore, BSI agrees that the assurance as outlined in the Certification Report [3] is maintained for this version of the product. This report is an addendum to the Certification Report [3].

References

[1]   Common Criteria document CCIMB-2004-02-009 "Assurance Continuity: CCRA Requirements", version 1.0, February 2004

[2]   Security Impact Analysis GXP3.2-E64PK-CC GemSAFE V2, Ref: SIA01A10190C, Version: 0.1, Date 1/02/06, Project code: R10438 (confidential document)

[3]   Certification Report BSI-DSZ-CC-0281-2005 for JavaCard Platform GXP3.2-E64PK-CC with GemSAFE V2 Version 1.0 from Gemplus SA, Bundesamt für Sicherheit in der Informationstechnik, 22 December 2005

[4]   Security Target BSI-DSZ-CC-0281, Version 1.0, 14.11.2005, ASE - Security Target, TOE - GXP3.2-E64PK-CC GemSafe V2, Product - GXP3.2-E64PK-CC, SSCD Type 2 (option a) and SSCD Type 3 (option b), Gemplus (sanitized public document)

[5]   Security Target BSI-DSZ-CC-0281, Version 2.01, 20.02.2006, ASE - Security Target, TOE - GXP3.2-E64PK-CC GemSafe V2, Product - GXP3.2-E64PK-CC, SSCD Type 2 (option a) and SSCD Type 3 (option b), Gemplus (sanitized public document)

[6]   G155CI Configuration Items History G155 (dev_file_modified_012006.htm, export_file_modified_012006.htm, file_modified_012006.htm, gemesign_file_modified_012006.htm, valid_file_modified_012006.htm), 11.05.2006, Gemplus (confidential document)

[7]   Card Initialization Specification For GemXpresso Pro R3.2 E64 PK CC, Version A15, 25.04.2006, Gemplus

[8]   GemSafe v2 Applet Reference Manual, Version 6, 10.02.2006, Gemplus