Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

General Secretariat for Defence and National Security

French Network and Information Security Agency

Maintenance Report ANSSI-CC-2008/37-M01

Linqus USIM 128K SmartCard, reference T1004530 B1 / version 1.1

Reference Certificate : DCSSI-2008/37

Courtesy Translation

Paris, 12th March 2010

SÉCURITÉ CERTIFICATION

References

a) Assurance continuity procedure MAI/P/01.
b) "ASE – Security Target ; TOE: ESIGN PKI signature application on GemXplore Generations G152B-EP3B OS platform, running on Infineon SLE88CFX4002P/m8834b17 chip; Ref T1004530 A3 / Version 1.0; Product: Linqus USIM 128K smartcard ; Based on SSCD Type 3", reference ASE10448, version 1.4
c) "Rapport de certification DCSSI-2008/37 - Carte Linqus USIM 128K, reference T1004530 A3 / version 1.0", 3 octobre 2008
d) "Impact Analysis Report - Clock stop issue on GemXplore Generations G152B-EP3B", reference T1004530_RD-IAR_09-0910.1, version 1.0
e) [SOG-IS] "Mutual Recognition Agreement of Information Technology Security Evaluation Certificates", version 2.0, April 1999, Management Committee of Agreement Group.
f) [CC RA] "Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security", May 2000.

Identification of the maintained product

The maintained product is the "LINQUS USIM 128K Smartcard: ESIGN PKI signature application loaded on GemXplore Generations G152B-EP3B platform embedded on SLE88CFX4002P/m8834b17, version 1.1" developed by GEMALTO and Infineon Technologies AG.

Description of changes

The product's modification regards the management of the "low power consumption" mode of the chip. In specific condition, the implementation of the initial evaluated product leads to a card mute. This mute was caused by a too long processing time between the call of a data block sending function and the call of another function that set the chip in low power consumption mode as in the mean time the external clock is stopped. The use of an other data block sending function for the last data block allow to set automatically the chip in low power consumption mode after sending the last bytes, and before the external clock is stopped. As this last event happens after the emission process is finished, the chip doesn't consider that the behaviour is abnormal, and then the mute mechanism is not triggered.
The GemXplore Generations G152B-EP3B platform is corrected by a EEPROM patch of the ROM executable

Impacted deliverables

[ST]	ASE – Security Target ; TOE: ESIGN PKI signature application on GemXplore Generations G152B-EP3B OS platform, running on Infineon SLE88CFX4002P/m8834b17 chip; Ref T1004530 A3 / Version 1.0; Product: Linqus USIM 128K smartcard ; Based on SSCD Type 3", reference ASE10448, version 1.4
[CONF]	"Bosphore project - List of evaluation documentation", reference BOS_DOC_10448, version 1.6

Conclusions

The above listed changes are considered as having a **minor** impact.
The assurance level of this new product revision is thus identical to the certified revision.

Warning

The resistance level of a certified product is declining as time goes by. The vulnerability analysis of this product revision versus the new attacks that would have appeared since the certificate release has not been conducted in the frame of this current maintenance. Only a re-evaluation or a "surveillance" of the new product revision would allow maintaining the assurance level in a timely and efficient manner.

Recognition of the certificate

European recognition (SOG-IS)

The reference certificate was issued in accordance with the provisions of the SOG-IS agreement [SOG-IS].

The European Recognition Agreement made by SOG-IS in 1999 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable up to ITSEC E6 and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:

International common criteria recognition (CCRA)

The reference certificate was released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries[2], of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:

This maintenance report is released in accordance with the document: « Assurance Continuity: CCRA Requirements, ref. CCIMB-2004-02-009, version 1.0, February 2004 ».

1 The signatory countries of the SOG-IS agreement are: Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Spain, Sweden and United Kingdom.
2 The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, Netherlands, New-Zealand, Norway, Pakistan, the Republic of Korea, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.