PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Maintenance Report DCSSI-2008/43-M01

JCLX80jTOP20ID smart card:
Java Trusted Open Platform on
SLE66CLX800PE microcontroller

Reference Certificate : 2008/43

Courtesy Translation

Paris, 6 July 2009

References

a) Assurance continuity procedure MAI/P/01.
b) Security Target: JCLX80jTOP20ID/JCLX36jTOP20ID - Security Target - version 1.8 (Developer’s reference is CP-2006-RT-389)
c) Public Security Target: JCLX80jTOP20ID/JCLX36jTOP20ID - Security Target Lite - version 1.4 (Developer’s reference is CP-2007-RT-075)
d) DCSSI-2008/43 certification report: JCLX80jTOP20ID smart card: Java Trusted Open Platform on SLE66CLX800PE microcontroller
e) Impact Analysis Report : JCLX80jTOP20ID Patch v1.6 Impact Analysis Report, version 1.0, 9 February 2009 (Developer’s reference is CP-2009-RT-073)

Identification of the maintained product

The maintained product is “JCLX80jTOP20ID smart card: Java Trusted Open Platform on SLE66CLX800PE microcontroller, IFXv#27_0.1, software revision v1.4” developed by Trusted Logic SA.

It is a dual-mode (contact/contactless) smart card comprising a platform compliant with Java Card 2.2.1 and VISA GlobalPlatform 2.1.1–Configuration 2 standards and which platform is embedded on Infineon Technologies’ SLE66CLX800PE microcontroller. The patch v1.4 is loaded on EEPROM (Electrically Erasable Programmable Read Only Memory).

Description of changes

All the modifications that were already included in Patch File v1.4 are also included `as is´in Patch File v1.6 except the one described in section 8.3 of [PV14]. The code of this modification was optimized in order to reduce the size of the Patch File in EEPROM. The functional behavior of this piece of code remains nevertheless the same.

In addition to the modifications introduced in the version v1.4 of the patch, the Patch File v1.6 also fixes the following functional problems identified by the customer:

- The card mutes during the processing of some extended APDUs. This modification is detailed in section 2.10 of [PV16];
- The READ BINARY command used by TL ICAO LDS and processed by the LDS FS API may return 2 or 3 bytes more than the answer size specified in the Le byte. This is described in section 5.7 of [PV16];
- The READ BINARY command may return an error when the offset specified in thecommand is equal to the file size. his is described in section 5.8 of [PV16].

Impacted deliverables

[ADV_LLD]	JCLX80jTOP20ID – Patch Description, Trusted Logic report CP-2007-RT-579, version 1.2 (edition for jTOP v27.01 – Patch File v1.4)
[ADV_IMP]	Tarball containing the sources of Patch File v1.4 deliverable reference ALCAZAR_V100_DELIVERY_SERMA_SOURCES_PATCH_V1_4_20080915
[PV14]	JCLX80jTOP20ID – Patch Description, Trusted Logic report CP-2007-RT-579, version 1.2 (edition for jTOP v27.01 – Patch File v1.4)
[PV16]	JCLX80jTOP20ID – Patch Description, Trusted Logic report CP-

	2007-RT-579, version 1.3 (edition for jTOP v27.01 – Patch File v1.6)

Conclusion

The above listed changes are considered as having a **minor** impact.
The assurance level of this product new version is thus identical to the one of the certified version, at the certification time.

Warning

The resistance level of a certified product is declining as time goes by. The vulnerability analysis of this product revision against 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:

IT Security Certified

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.