PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Maintenance Report DCSSI-2007/24-M02

E-passport (MRTD) configuration of the Xaica-Alpha64K platform embedded on the ST19WR66I secure microcontroller

Reference Certificate: DCSSI-2007/24

Courtesy Translation

Paris, 28th of August 2008

References

a) Assurance continuity procedure MAI/P/01.
b) Xaica-alpha64K Security Target (ePassport configuration), reference: NTTD-STep-XAICAALPHA64KST19, version 1.20, December 6, 2007, NTTDATA
c) Xaica-alpha64K Security Target Lite, reference: NTTD-STL-XAICAALPHA64K-ST19, Version 1.00, December 14, 2007, NTTDATA
d) Certification Report DCSSI-2007/24 - E-passport (MRTD) configuration of the Xaica-Alpha64K platform embedded on the ST19WR66I secure microcontroller, 14th of December 2007, DCSSI, and Maintenance Report DCSSI-2007/24-M01, 29th of May 2008, DCSSI
e) Xaica-alpha64K - Impact Analysis of READ BINARY command modification, reference: NTTD-IAR2-XAICAALPHA64K-ST19, version 1.00, August 7, 2008, NTTDATA

Identification of the maintained product

The maintained product is the e-Passport (MRTD) configuration of the Xaica-Alpha64K platform developed by NTTDATA Corporation, embedded on the ST19WR66I secure microcontroller developed and manufactured by STMicroelectronics.
The maintained version of the product can be identified by the following elements:
- Reference of the platform: SPEC5 V014;
- Reference of the patch: SM2 V013;
- IC manufacturer reference of the product: PQH;
- Reference of the microcontroller: ST19WR66I.

Description of changes

The software patch loaded in EEPROM has been adapted to fix a problem in the data format of the command "read binary", leading to some errors in particular cases.

Impacted deliverables

[CONF]	Xaica-alpha64K - TOE Configuration List, Reference: NTTD-TCL-XAICAALPHA64K-ST19 v1.70 NTTDATA
[ST]	Xaica-alpha64K Security Target (ePassport configuration) Reference: NTTD-STep-XAICAALPHA64KST19, version 1.40 NTTDATA

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.