



PREMIER MINISTRE

General Secretariat for Defence and National Security

French Network and Information Security Agency

Maintenance Report ANSSI-2010/02-M01

Secured microcontrollers SA23YR48/80B and SB23YR48/80B, including the cryptographic libraries NesLib v2.0 or v3.0, in SA or SB configurations

Reference Certificate : ANSSI-2010/02

Courtesy Translation

Paris, 19th March 2010



References

- a) Procédure MAI/P/01 Continuité de l'assurance
- b) « Sx23YRxxB Security Target - Public Version », reference : SMD_Sx23YRxx_ST_09_002, version 02.01
- c) « Rapport de certification ANSSI-CC-20010/02 - Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB », février 2010 T
- d) [SOG-IS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, version 2.0, April 1999, Management Committee of Agreement Group.
- e) [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 certificate is ANSSI_2010/02 (see reference c) related to the “Secured microcontrollers SA23YR48/80B and SB23YR48/80B, including the cryptographic libraries NesLib v2.0 or v3.0, in SA or SB configurations”, developed by STMicroelectronics.

Description of changes

The products haven't been changed since the evaluation.

The current report only addresses modification of one of the certified guidance, which identified a too restrictive usage recommendation regarding the admissible solutions.

Impacted deliverables

[GUIDES]	« Addendum 1 – ST23 Platform Security Guidance », reference : AN_SECU_23_AD1, version 2
----------	---

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 agreement¹, 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 [CCRA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries², 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.