



## Assurance Continuity Maintenance Report

BSI-DSZ-CC-0386-2006-MA-02

ZKA SECCOS Sig v1.5.3

from

**Sagem Orga GmbH**



Common Criteria Arrangement  
for components up to EAL4

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-0386-2006.

The change to the certified product is at the level of two additional initialisation tables which introduce customer specific changes. These changes have no effect on assurance.

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-0386-2006 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-0386-2006.

Bonn, 20. September 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 ZKA SECCOS Sig v1.5.3, Sagem Orga GmbH, 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 ZKA SECCOS Sig v1.5.3 was changed due to two additional Initialisation Tables.

The first new Initialisation Table named SDR001G0.A\_7 is the same as the already certified Initialisation Table named SDR001G0.A\_3 except of the following minor changes:

- Within the Cold EEPROM ATR the value for TA1 is set to 0x18 representing the new division factor  $372/12 = 31$  (instead of TA1 0x96 representing the division factor  $512/32 = 16$  in SDR001G0.A\_3).
- For the new Initialisation Table, the internal version number for identification of the Initialisation Table is inserted within the header of the table.
- The key length of four keys within the TOE's Signature Application has been increased from 1728 to 1984 bit. According to this change, the corresponding data fields for the related X.509 certificates have been extended.

The second new Initialisation Table named SWR001H0.A\_1 is the same as the already certified Initialisation Table named SDR001G0.A\_3 except of following minor changes:

- The three changes as described above.
- The applications GA Maestro and ec-Cash are not part of the new Initialisation Table. As a consequence, due to the SECCOS specification, some of the MF related data fields are adapted.

Both Initialisation Tables are added to the certified TOE.

The change is not significant from the standpoint of security. The new division factor influences only the data rate during data exchange. The new RSA key length of 1984 bit supersedes the former key length of 1728 bit and has been considered in general within the security evaluation of the SECCOS operating system platform. Finally, the applications GA Maestro and ec-Cash are explicitly not part of the CC-evaluation of the TOE, and the deletion of these applications and the adaptation of some MF data fields due to this deletion do not affect any security functionality of the TOE.

## Conclusion

The change to the TOE is at the level of two additional initialisation tables that introduce customer specific changes, the changes have no effect on assurance. Examination of

the evidence indicates that the changes required are limited to the inclusion of two additional Initialisation Tables named SDR001G0.A\_7 and SWR001H0.A\_1. Therefore, the Configuration List has been updated taking the new Initialisation Tables into account, see [5]. Additionally, the Appendix to the Configuration List was supplemented with a reference to the test scenarios relevant for the new Initialisation Tables, see [6] and [7], and new Data Sheets related to the new Initialisation Tables have also been created, see [8] and [9]. The Security Target [4] is still valid for the changed TOE. 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] Sagem ORGA GmbH; ZKA SECCOS Sig v1.5.3; Impact Analysis Report; Version: V1.02; Date: 18 September 2006 (confidential document)
- [3] Certification Report BSI-DSZ-CC-0386-2006 for ZKA SECCOS Sig v1.5.3 from Sagem Orga GmbH, Bundesamt für Sicherheit in der Informationstechnik, 08. September 2006
- [4] Security Target BSI-DSZ-CC-0386-2006, Version V1.01, 21 June 2006, Sagem Orga GmbH; ZKA SECCOS Sig v1.5.3; ST-Lite (sanitized public document)
- [5] ZKA SECCOS Sig v1.5.3 – Configuration List; Version: V1.05; Date: 18 September 2006; Sagem ORGA GmbH
- [6] Sagem ORGA GmbH; ZKA SECCOS Sig v1.5.3 - Configuration List - Appendix; Systemelement Test Description; Version: V1.04; Date: 14 September 2006 (confidential document)
- [7] Sagem ORGA GmbH; ZKA SECCOS Sig v1.5.3 - Configuration List - Appendix; Systemelement Test Description; Version: V1.05; Date: 18 September 2006 (confidential document)
- [8] ZKA SECCOS Sig v1.5.3; Data Sheet; 14.09.2006; Sagem ORGA GmbH; V1.03
- [9] ZKA SECCOS Sig v1.5.3; Data Sheet; 14.09.2006; Sagem ORGA GmbH; V1.04