



Assurance Continuity Maintenance Report

BSI-DSZ-CC-1028-2017-MA-01

Sm@rtCafé® Expert 7.0 C3

from

Giesecke+Devrient Mobile Security GmbH



SOGIS
Recognition Agreement

The IT product identified in this report was assessed according to the *Assurance Continuity: CCRA Requirements*, version 2.1, June 2012 and the developer's 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-1028-2017 updated by a new ETR dated 18 July 2018.

The certified product itself did not change. The changes are related to the set of included development and production sites which are already certified.

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.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-1028-2017 dated 8 September 2017 is of relevance and has to be considered when using the product. Details can be found on the following pages.

This report is an addendum to the Certification Report BSI-DSZ-CC-1028-2017.

Bonn, 4 October 2018

The Federal Office for Information Security



Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2



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 product (Target of Evaluation, TOE) [3], its Security Target and the Evaluation Technical Report as outlined in [3].

The vendor for the Sm@rtCafé® Expert 7.0 C3, Giesecke+Devrient Mobile Security GmbH, submitted an IAR [2] to the BSI for approval. The IAR is intended to satisfy the requirements outlined in the document *Assurance Continuity: CCRA Requirements* [1]. In accordance with those requirements, the IAR describes (i) the changes made to the certified TOE, (ii) the evidence updated as a result of the changes and (iii) the security impact of the changes.

The certified product Sm@rtCafé® Expert 7.0 C3 itself did not change.

The TOE and the related documentation are developed at the site Giesecke+Devrient Mobile Security Development Center Germany (DCG). The production sites Veridos Matsoukis S.A. (VDMAT) and Giesecke & Devrient Iberica S.A. (GDIMS) were added to the scope of the certificate. The Site Certificates for Giesecke+Devrient Mobile Security Development Center Germany (DCG) and Giesecke+Devrient Secure Data Management GmbH (GDSDM) were updated. The production site Giesecke & Devrient Slovakia (GDSK) is still considered in this ALC re-evaluation. According to the official notification dated 16 May 2018 the validity of the Site Certificate for the site GDSK has been extended to 31 December 2018. After this expiration date the Site Certificate for GDSK can no longer be used.

The ALC re-evaluation was performed by the ITSEF TÜV Informationstechnik GmbH. The changes are related to an update of life cycle security aspects. The procedure led to an updated version of the Evaluation Technical Report (ETR) [7]. The Common Criteria assurance requirements for ALC are fulfilled as claimed in the Security Target [4] and [5].

The sites and related certificates listed in Annex B of Certification Report BSI-DSZ-CC-1028-2017 are replaced by the following development and production sites:

- a) Giesecke+Devrient Mobile Security GmbH, Development Center Germany (DCG), Prinzregentenstrasse 159, 81677 Munich, Germany, SW Development / Testing, BSI-DSZ-CC-S-0083-2017
- b) Giesecke & Devrient Slovakia s.r.o., (GDSK), Dolné Hony 11, 94901 Nitra, Slovakia, Production / Delivery, BSI-DSZ-CC-S-0062-2016
- c) Giesecke+Devrient Secure Data Management GmbH, (GDSDM), Austraße 101b, 96465 Neustadt bei Coburg, Germany, Production / Delivery, BSI-DSZ-CC-S-0100-2018
- d) Veridos Matsoukis S.A., (VDMAT), Dimocratias Ave. 69, 13122 Ilion, Attica, Greece, Production / Delivery, CCN-CC-019/2017

- e) Giesecke & Devrient Iberica S.A., (GDIMS), Carrer del Número 114, no. 27 / Poligon Pratenc, 08820 El Prat de Llobregat (Barcelona), Spain, Production / Delivery, CCN-CC-011/2018
- f) For development and production sites regarding the platform please refer to the certification reports BSI-DSZ-CC-0951-2015 [9], [10]

In their combination, above listed sites fulfil Common Criteria assurance requirements ALC – Life cycle support.

Conclusion

The maintained change is at the level of an update of life cycle security aspects covered by newer site certificates for each site of the life cycle considered herein. The change has no effect on product 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.

The resistance to attacks has not been re-assessed in the course of this maintenance process. Therefore, the assurance statement as outlined in the Certification Report BSI-DSZ-CC-1028-2017 dated 8 September 2017 is of relevance and has to be considered when using the product. As a result of this maintenance with ALC re-evaluation, the ETR for the Composite TOE [7] was updated and an Addendum to the ETR for Composition [8] is provided. Please note that the eighteen month time frame is related to the date of the initial version of the ETR for Composite Evaluation [11] as the updates made afterwards are not related to updates of AVA evaluation tasks.

Obligations and notes for the usage of the product:

All aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

Some security measures are partly implemented in the TOE and require additional configuration or control or measures to be implemented by the applications running on the TOE.

For this reason the TOE includes guidance documentation which contains guidelines for the developer of the applications running on the TOE on how to securely use the TOE and which measures have to be implemented in the applications in order to fulfil the security requirements of the Security Target of the TOE.

In the course of the evaluation of the composite product or system it must be examined if the required measures have been correctly and effectively implemented by the software. Additionally, the evaluation of the composite product or system must also

consider the evaluation results as outlined in the document ETR for composite evaluation [8] according to AIS 36.

According to the scheme rules, evaluation results outlined in the document ETR for composite evaluation as listed above can usually be used for composite evaluations building on top, as long as the document ETR for composite evaluation is not older than eighteen months¹ and an attack assumed to be not feasible within the scope of these evaluations has not been performed successfully.

Additional Note: The strength of the cryptographic algorithms was not rated in the course of the product certification and this maintenance procedure (see BSIG² Section 9, Para. 4, Clause 2).

This report is an addendum to the Certification Report [3].

- 1 In this case the eighteen month time frame is related to the date of the initial version [11] of the Evaluation Technical Report for Composite Evaluation as the updates made afterwards are not related to updates of AVA evaluation tasks.
- 2 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

References

- [1] Common Criteria document “Assurance Continuity: CCRA Requirements”, version 2.1, June 2012
- [2] Impact Analysis Report BSI-DSZ-CC-1028-2017-MA-01, Sm@rtCafé® Expert 7.0 C3, Version 1.3, 7 May 2018, G+D Mobile Security GmbH (confidential document)
- [3] Certification Report BSI-DSZ-CC-1028-2017 for Sm@rtCafé® Expert 7.0 C3, 8 September 2017, Bundesamt für Sicherheit in der Informationstechnik
- [4] Security Target Sm@rtCafé® Expert 7.0 C3, Version 2.9, 16 August 2017, BSI-DSZ-CC-1028-2017, Giesecke+Devrient Mobile Security GmbH (confidential document)
- [5] Security Target Lite Sm@rtCafé® Expert 7.0 C3, Version 2.9, 16 August 2017, BSI-DSZ-CC-1028-2017, Giesecke+Devrient Mobile Security GmbH (sanitized public document)
- [6] Configuration List Sm@rtCafé® Expert 7.0 C3, Version 3.0, 18 May 2018, Giesecke+Devrient Mobile Security GmbH (confidential document)
- [7] Evaluation Technical Report for Sm@rtCafé® Expert 7.0 C3, Version 8, 18 July 2018, BSI-DSZ-CC-1028-2017-MA-01, TÜV Informationstechnik GmbH (confidential document)
- [8] Evaluation Technical Report for Composite Evaluation Addendum for Sm@rtCafé® Expert 7.0 C3, Version 1, 18 July 2018, BSI-DSZ-CC-1028-2017-MA-01, TÜV Informationstechnik GmbH (confidential document)
- [9] Certification Report – BSI-DSZ-CC-0951-2015 for Infineon Security Controller M5073 G11 with optional RSA2048/4096 v2.03.008, EC v2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG, 11 November 2015, Bundesamt für Sicherheit in der Informationstechnik
- [10] Assurance Continuity Reassessment Report, BSI-DSZ-CC-0951-2015-RA-01, Infineon Security Controller M5073 G11 with optional RSA2048/4096 v2.03.008, EC v2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG, 31 May 2017, Bundesamt für Sicherheit in der Informationstechnik
- [11] Evaluation Technical Report for Composite Evaluation according to AIS 36 for Sm@rtCafé® Expert 7.0 C3, Version 3, 16 August 2017, BSI-DSZ-CC-1028-2017, TÜV Informationstechnik GmbH (confidential document)