



Assurance Continuity Partial-Reassessment Report

BSI-DSZ-CC-1022-2018-RA-01

**NXP eDoc Suite v3.0 - cryptovision ePasslet Suite -
Java Card applet configuration providing Machine
Readable Travel Document with "ICAO Application",
Extended Access Control with PACE**

from

NXP Semiconductors Germany GmbH



SOGIS
Recognition Agreement

The IT product identified in this report certified under the certification procedure BSI-DSZ-CC-1022-2018 [5] has undergone a partial-reassessment of the vulnerability analysis.

This reassessment confirms that the resistance of the product against attacks on the level of AVA_VAN.5 as stated in the product certificate is not adversely affected by certain changes to the user guidance.

More details are outlined on the following pages of this report.

This report is an addendum to the Certification Report BSI-DSZ-CC-1022-2018.



Common Criteria
Recognition
Arrangement
recognition for
components up to EAL
2 and ALC_FLR only

Bonn, 7 January 2019

The Federal Office for Information Security



Assessment

The reassessment was performed based on CC [1], CEM [2] and relevant AIS [4] and according to the BSI Certification Procedures [3] by the ITSecurity Evaluation Facility (ITSEF) TÜV Informationstechnik GmbH, approved by BSI.

The results are documented in an updated version of the ETR [7].

Within the scope of this reassessment the guidance documentation related to the product has been updated (see [8], [9]) replacing the guidance documentation (reference [11] and [12] as listed in [5]). Note that only these two guidance documents have been updated, all other guidance documents and other TOE constituents remain unchanged.

This re-assessment therefore only analysed the impact of these guidance changes; no new vulnerability analysis or testing activities have been carried out.

Conclusion

This reassessment confirms that the changes made to the guidance documentation do not adversely affect the security claim of the certificate.

The obligations and recommendations as outlined in the certification report [5] are still valid and have to be considered.

The obligations and recommendations as outlined in the guidance documentation [8] (especially 3.3.4 “Additional Requirements”) and [9] (especially 3.3.4 “Additional Requirements”) have to be considered by the user of the product.

Bibliography

- [1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
<http://www.commoncriteriaportal.org>
- [2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012,
<http://www.commoncriteriaportal.org>
- [3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) <https://www.bsi.bund.de/zertifizierung>
- [4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE¹ <https://www.bsi.bund.de/AIS>

1 specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 26, Version 9, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document

- [5] Certification Report BSI-DSZ-CC-1022-2018 for NXP eDoc Suite 3.0 - cryptovision ePasslet Suite - Java Card applet configuration providing Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE, Bundesamt für Sicherheit in der Informationstechnik, 18 May 2018
- [6] Security Target Lite BSI-DSZ-CC-1022-2018, Version 1.7, 22 February 2018, NXP eDoc Suite v3.0 - cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application“, Extended Access Control with PACE – Security Target Lite, cv cryptovision GmbH (sanitised public document)
- [7] Evaluation Technical Report BSI-DSZ-CC-1022-2018-RA-01, Version 4, 24 October 2018, NXP eDoc Suite v3.0 - cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application“, Extended Access Control with PACE 3.0, TÜV Informationstechnik GmbH – Evaluation Body for IT Security (confidential document)
- [8] Guidance Document for the TOE: NXP eDoc Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing an ICAO MRTD application with Extended Access Control (EACv1) or with Basic Access Control (BAC) and Supplemental Access Control (SAC) Operational Guidance (AGD_OPE), Version 3.0.8, 09 October 2018, cv cryptovision GmbH
- [9] Guidance Document for the TOE: NXP eDoc Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing an ICAO MRTD application with Extended Access Control (EACv1) or with Basic Access Control (BAC) and Supplemental Access Control (SAC) Preparation Guidance (AGD_PRE), Version 3.0.11, 09 October 2018, cv cryptovision GmbH

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren