Federal Office
for Information Security

Assurance Continuity Reassessment Report

BSI-DSZ-CC-0957-V2-2016-RA-01

TCOS Smart Meter Security Module Version 1.0 Release 2/P60C144PVE

from

Deutsche Telekom Security GmbH

SOGIS
Recognition Agreement

The IT product identified in this report certified under the certification procedure BSI-DSZ-CC-0957-V2-2016 [5] has undergone a re-assessment of the vulnerability analysis according to the current state of the art attack methods and based on the Security Target [6].

This reassessment confirms resistance of the product against attacks on the level of AVA_VAN.5 as stated in the product certificate.

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

This report is an addendum to the Certification Report BSI-DSZ-CC-0957-V2-2016.

Common Criteria
Recognition
Arrangement
for components up to
EAL 2 only

Bonn, 27 September 2021

The Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 99 9582-0 - Fax +49 228 9582-5477 - Infoline +49 228 99 9582-111

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 IT Security Evaluation Facility (ITSEF) SRC Security Research & Consulting GmbH, approved by BSI.

The following guidance specific for the technology has been applied as a refinement of CC and CEM:

- Composite product evaluation for Smart Cards and similar devices according to AIS 36 (see [4]). On base of this concept the relevant guidance documents of the underlying IC platform (refer to [9], [12]) and the document ETR for composite evaluation from the IC's evaluation ([10], [11]) have been applied in the TOE evaluation.
- Guidance for Smartcard Evaluation (AIS 37, see [4]).
- Attack Methods for Smartcards and Similar Devices (AIS 26, see [4]).
- Application of Attack Potential to Smartcards (AIS 26, see [4]).
- Application of CC to Integrated Circuits (AIS 25, see [4]).
- Security Architecture requirements (ADV_ARC) for smart cards and similar devices (AIS 25, see [4]).
- Evaluation Methodology for CC Assurance Classes for EAL5+ and EAL6 (AIS 34, see [4]).
- Functionality classes and evaluation methodology of physical and deterministic random number generators (AIS 20 and AIS 31, see [4]).
- Informationen zur Evaluierung von kryptographischen Algorithmen (AIS 46, see [4]).

Please note that the product TCOS Smart Meter Security Module Version 1.0 Release 2/ P60C144PVE is set up on the NXP chip P60C144PVE that was originally certified under the Certification ID BSI-DSZ-CC-0978-2016. In the meantime, the IC platform was re-certified under the Certification IDs BSI-DSZ-CC-0978-V2-2017 and BSI-DSZ-CC-0978-V3-2019 (refer to [9]). For the present reassessment, the corresponding updated ETR for composite evaluation [10] and IC user guidance documentation [12] were taken into account. In addition, a partial reassessment of the IC platform intended for specific support of the reassessment of the product TCOS Smart Meter Security Module Version 1.0 Release 2/P60C144PVE ([11]) was performed. All in all, the reassessment of the product was carried out in view of the product's intended operational use as a cryptographic service provider within a Smart Meter Gateway in the infrastructure for Smart Meter Systems according to the Protection Profile [13].

The results of the reassessment of the product TCOS Smart Meter Security Module Version 1.0 Release 2/P60C144PVE are documented in an updated version of the ETR [7].

Note: The developer's company name changed from T-Systems International GmbH to Deutsche Telekom Security GmbH.

Conclusion

This reassessment confirms resistance of the product against attacks on the level AVA_VAN.5 as claimed in the Security Target [6].

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] have to be considered by the user of the product.

In particular, as for the base evaluation BSI-DSZ-CC-0957-V2-2016 ([5]) the usage of the product TCOS Smart Meter Security Module Version 1.0 Release 2/P60C144PVE is restricted to Smart Meter Gateways in the infrastructure for Smart Meter Systems according to the Protection Profile [13] and the Security Target [6].

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[1]
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 4, September 2012[2]
https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen)
https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[3]
https://www.bsi.bund.de/AIS

[5] Certification Report BSI-DSZ-CC-0957-V2-2016 for TCOS Smart Meter Security Module Version 1.0 Release 2/P60C144PVE, 18 November 2016, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[6] Security Target BSI-DSZ-CC-0957-V2-2016, Specification of the Security Target TCOS Smart Meter Security Module Version 1.0 Release 2/P60C144PVE, Version 1.0.2, 26 October 2016, T-Systems International GmbH

1 as relevant for the base evaluation BSI-DSZ-CC-0957-V2-2016

2 as relevant for the base evaluation BSI-DSZ-CC-0957-V2-2016

3 specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document (under consideration of the current versions of the JIWG/JHAS documents 'Attack Methods for Smartcards and Similar Devices', Version 2.4 and 'Application of Attack Potential to Smartcards and Similar Devices', Version 3.1)
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluierungsmethodologie für die Vertrauenswürdigkeitsklasse EAL5+
- AIS 36, Version 5, ETR-Zusatz zur Unterstützung von Smartcard Kompositionszertifizierungen (ETR for composition) 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

[7] Evaluation Technical Report BSI-DSZ-CC-0957-V2-RA-01, Evaluation Report Re-Assessment – Evaluation Technical Report (ETR) – Summary for TCOS Smart Meter Security Module Version 1.0 Release 2/P60C144PVE, Version 1.1, 15 September 2021, SRC Security Research & Consulting GmbH (confidential document)

[8] Operational Guidance for users and administrators, Guidance Documentation of TCOS Smart Meter Security Module Version 1.0 Release 2, Version 1.4, 12 September 2016, T-Systems International GmbH

[9] Certification Report BSI-DSZ-CC-0978-V3-2019 for NXP Secure Smart Card Controller P60x144/080yVA/yVA(Y/B/X)/yVE with IC Dedicated Software from NXP Semiconductors Germany GmbH, 14 May 2019, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[10] Evaluation Technical Report for Composite Evaluation (ETR-COMP), BSI-DSZ-CC-0978-V3-2019, Version 2, 29 April 2019, TÜV Informationstechnik GmbH (confidential document)

[11] Evaluation Technical Report for Composite Evaluation (ETR-COMP) - Addendum, BSI-DSZ-CC-0978-V3-2019, Version 3, 5 July 2021, TÜV Informationstechnik GmbH (confidential document)

[12] NXP Secure Smart Card Controller P60x144/080 VA/VE, Information on Guidance and Operation, Rev. 2.9, 12 December 2018, NXP Semiconductors Germany GmbH

[13] Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP) - Schutzprofil für das Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen Version 1.03, 11 December 2014, BSI-CC-PP-0077-V2-2015, Bundesamt für Sicherheit in der Informationstechnik (BSI)