Federal Office
for Information Security

Certificate of Conformity

pursuant to Article 29 (1), 39 (1) and Annex II of the Regulation (EU) No 910/2014 and Amendment Regulation (EU) 2024/1183

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189, 53175 Bonn, Germany[1]

confirms hereby, pursuant to Article 30 (1) and 39 (2) of the Regulation (EU) No 910/2014 and Amendment Regulation (EU) 2024/1183, that the product

CardOS V6.0 ID R1.2

from

Eviden Germany GmbH

fulfils the requirements of Annex II of Regulation (EU) No 910/2014 and Amendment Regulation (EU) 2024/1183[2] pursuant to Article 29 (1), 39 (1) as a Qualified Electronic Signature Creation Device and Qualified Electronic Seal Creation Device when considering the information stated in the report below.

The documentation of this Certificate of Conformity has been registered under **BSI-DSZ-CC-1162-V3-2024.**

This Certificate of Conformity is valid until 3 December 2029.

Bonn, 4 December 2024
For the Federal Office for Information Security

sgd. Sandro Amendola
Director-General

L.S.

[1] The Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security is a designated Body notified to the EU commission for the certification of Qualified Electronic Signature Creation Devices and Qualified Electronic Seal Creation Devices to be conformant to Regulation (EU) No 910/2014 and Amendment Regulation (EU) 2024/1183.

[2] For detailed references refer to [1].

This certification document comprises 8 pages.

1. Certification Scheme

Article 17 (4) of the national act on trust services (Vertrauensdienstegesetz)[3] states that the Federal Office for Information Security (BSI) is the public body according to Article 30 (1) and Article 39 (2) of the Regulation (EU) No 910/2014 and Amendment Regulation (EU) 2024/1183 [1]. Therefore, BSI has been notified to the EU commission for the certification of Qualified Electronic Signature Creation Devices and Qualified Electronic Seal Creation Devices to be conformant to Regulation (EU) No 910/2014 and Amendment Regulation (EU) 2024/1183.

Under the BSIG[4] act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products. The certification body of the Federal Office for Information Security (BSI) is accredited by “DAkkS Deutsche Akkreditierungsstelle GmbH” under ID D-ZE-19615-01-00 according to EN ISO/IEC 17065:2013 including certification of IT products (Software and Hardware) using Common Criteria / ISO/IEC 15408 [4]. The certification body performs its certification on the basis of the following accredited certification program [3]:

- „Verfahrensbeschreibung zur Zertifizierung von Produkten“ (VB-Produkte)
- „Anforderungen an Antragsteller zur IT-Sicherheitszertifizierung von Produkten, Schutzprofilen und Standorten” (CC-Produkte)

including the resulting conformity assessment tasks.

2. Information about the product

Name of the product:

CardOS V6.0 ID R1.2

Type of product

Smartcard chip with operating system and signature application usable as Qualified Electronic Signature Creation Device (QSigCD) or Qualified Electronic Seal Creation Device (QSealCD).

Manufacturer of the product

Eviden Germany GmbH, Otto-Hahn-Ring 6, 81739 München, Germany

Description of the product

For detailed information on the product, functional description and the overall architecture refer to the certification report [6] part B, chapters 1 to 8 and Security Target [6], specifically the chapters on ST Introduction including TOE Description, Security

[3] "Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist", https://www.gesetze-im-internet.de/vdg/

[4] "BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist", https://www.gesetze-im-internet.de/bsig_2009/

Requirements and TOE Summary Specification. The product provides several signature algorithms. Only those listed below are part of this conformity certification.

Delivery Items of the product

The parts of the product (hardware, software, documentation) delivered are listed in the certification report [6] part B, chapter 2, table 2.

3. Compliance with the requirements

The product identified in the Certificate of Conformity pursuant to Article 29 (1), 39 (1) and Annex II of the Regulation (EU) No 910/2014 and Amendment Regulation (EU) 2024/1183 (see above) has been certified according to Article 30 (3) a) using the standards: Common Criteria & CEM [4] and Protection Profiles as listed in [5]. These standards are taken from the COMMISSION IMPLEMENTING DECISION (EU) No 2016/650, Annex [2]. The CC certification results [6] outline the results of the CC evaluation and certification. Based on these results the concluding conformity assessment task came to the following result:

The product fulfils the requirements pursuant to the Regulation (EU) No 910/2014 and Amendment Regulation (EU) 2024/1183 as outlined in the following table:

Reference	Requirement / Description	Fulfillment
Article 29	Requirements for qualified electronic signature creation devices	
(1)	Requirement: Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.	Yes
(2)	Requirement: The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48 (2).	Yes
Article 39	Qualified electronic seal creation devices	
(1)	Requirement: Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.	Yes
Annex II	Requirements for qualified electronic signature creation devices	

Reference	Requirement / Description	Fulfillment
1.	Requirement: Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:	Yes
(a)	the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;	Yes
(b)	the electronic signature creation data used for electronic signature creation can practically occur only once;	Yes
(c)	the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;	Yes
(d)	the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.	Yes
2.	Requirement: Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.	Yes
3.	Requirement: Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.	n/a[5]
4.	Requirement: Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met:	n/a
(a)	the security of the duplicated datasets must be at the same level as for the original datasets;	n/a
(b)	the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.	n/a

Table 1: Fulfilment of the requirements of the Regulation (EU) No 910/2014 and Amendment Regulation (EU) No 2024/1183

Assurance level

The evaluation assurance level as claimed in the Protecton Profiles [5] has been confirmed by the CC certificate [6].

[5] n/a: not applicable for the product considered

Cryptographic algorithms and parameters

The cryptographic algorithms and parameters provided by the product are taken from the document SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms [7]. Considering the selection of cryptographic algorithms and the operational conditions on crypto below, the IT-product is technically suitable to be used as a Qualified Electronic Signature Creation Device (QSigCD) according to Article 30 (1) by 30 (3) a) and a Qualified Electronic Seal Creation Device (QSealCD) according to Article 39 (2) of Regulation (EU) No 910/2014 and Amendment Regulation (EU) 2024/1183.

Documents attached

The documents [6] outlining the CC certification of the product are attachments to this Conformity Certificate.

Operational conditions to be followed

- The obligations and notes for the usage of the product as stated in the CC certification results [6], i.e. certification report part B, chapter 10, as well as within the guidance documentation listed in the CC certification results [6], i.e. certification report part B, chapter 2, table 2 have to be followed.
- The trust service provider has to follow the operational requirements from the regulation as relevant for a qualified electronic signature creation device and a qualified electronic seal creation device as well as to follow all related obligations from its supervisory body.
- For the creation of qualified electronic signatures or qualified electronic seals the product has to use the cryptographic algorithms in accordance with the SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms [7] which are depicted in the table below.
- The trust service provider shall consider the results of the certification and the operational conditions listed above within the system risk management process for the product usage. Specifically:
  (i) The evolution of limitations of cryptographic algorithms and parameters has to be considered. Future updates of the catalogue [7] may shorten or extend the acceptance time frame. This may need actions for the usage of the product to be taken.
  (ii) The evolution of attack methods related to the product or to the type of product has to be considered.
  A regular technical re-assessment of the product assurance accompanied by a confirmation of the CC certification body e.g. by a re-certification shall cover these aspects.

No.	Cryptographic Mechanism	Key Size in Bits	Acceptability Deadline according to [7] as of today
1	RSASSA-PKCS1-v1_5 [8, 9, 10]	Modulus length = 3072, 4096	31 December 2030

No.	Cryptographic Mechanism	Key Size in Bits	Acceptability Deadline according to [7] as of today
2	RSASSA-PSS (PKCS#1 v2.1) [8, 9, 10]	Modulus length = 3072, 4096	None
3	ECDSA [11, 12]	ECC Key sizes corresponding to the used elliptic curve: BP P256r1, BP P384r1, BP P512r1 [13] NIST P-256, NIST P-384, NIST P-521 [16]	None
4	SHA-2, hash length (bits) = 256, 384, 512 [14, 15]		None

Table 2: Cryptographic algorithms of the product in accordance with [7] within the scope of this Certificate of Conformity to [1]

Out of this, the compliance of the QSigCD / QSealCD is confirmed under the conditions mentioned above within the following categories:

- Components and procedures for the generation of signature resp. seal creation data
- Components and procedures for the storage of signature resp. seal creation data
- Components and procedures for the processing of signature resp. seal creation data

Validity period of the Certificate of Conformity

The validity period of this Certificate of Conformity depends on the validity of the CC certificate [6] (i.e. 3 December 2029) and the strength and validity of the cryptographic algorithms implemented (see table 2 above).

Out of this the validity of this Certificate of Conformity is limited to 3 December 2029.

At a given time, the validity period can be extended or shortened if there are new findings regarding the validity of the CC certificate [6] and the suitability of security mechanisms or cryptographic algorithms.

4. References

[1] REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, Official Journal of the European Union

REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework, Official Journal of the European Union

[2] COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30 (3) and 39 (2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

[3] BSI certification Scheme documentation:
“Verfahrensbeschreibung zur Zertifizierung von Produkten“ (VB-Produkte)
“Anforderungen an Antragsteller zur IT-Sicherheitszertifizierung von Produkten, Schutzprofilen und Standorten” (CC-Produkte)

https://www.bsi.bund.de/zertifizierung

[4] ISO-Version:
ISO/IEC 15408, Information technology — Security techniques — Evaluation criteria for IT security
Part 1: Introduction and general model: 2009/2014
Part 2: Security functional components: 2008/2011
Part 3: Security Assurance components: 2008/2011
ISO/IEC 18045: Information technology — Security techniques — Methodology for IT security evaluation, 2008/2014

https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

CCRA-Version:
Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017

https://www.commoncriteriaportal.org

[5] Protection Profiles:
EN 419211-2:2013 - Protection profiles for secure signature creation device — Part 2: Device with key generation, Certification-ID: BSI-CC-PP-0059-2009-MA-02

EN 419211-4:2013 - Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application, Certification-ID: BSI-CC-PP-0071-2012-MA-01

EN 419211-5:2013 - Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application, Certification-ID: BSI-CC-PP-0072-2012-MA-01

https://www.sogis.eu/uk/pp_en.html

[6] Common Criteria Certificate: BSI-DSZ-CC-1162-V3-2024 for CardOS V6.0 ID R1.2 from Eviden Germany GmbH, Version 1.0, Bundesamt für Sicherheit in der Informationstechnik

Common Criteria Certification Report: BSI-DSZ-CC-1162-V3-2024 for CardOS

V6.0 ID R1.2 from Eviden Germany GmbH, Version 1.0, Bundesamt für Sicherheit in der Informationstechnik

Security Target for BSI-DSZ-CC-1162-V3-2024, Security Target ’CardOS V6.0 ID R1.2’, Revision 2.40R, 2024-11-20, Eviden Germany GmbH

Guidance Documentation as referenced in the Common Criteria Certification Report, part B, chapter 6 and 2

https://www.bsi.bund.de/zertifizierung

[7] SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms, Version 1.3, February 2023

https://www.sogis.eu/uk/supporting_doc_en.html

[8] Public-Key Cryptography Standard PKCS #1, RSA Cryptography Specifications, Version 2.1, 2003, J. Jonsson and B. Kaliski

[9] Public-Key Cryptography Standard PKCS #1, RSA Cryptography Standard, Version 2.2, 2012, RSA Laboratories

[10] ISO/IEC 9796-2:2010 – Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, 2010, ISO

[11] FIPS PUB 186-5: Digital Signature Standard (DSS), 2023, National Institute of Standards and Technology (NIST)

[12] ISO/IEC 14888-3:2006 – Information technology – Security techniques – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms, 2006, ISO

[13] RFC 5639: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, 2010, M. Lochter and J. Merkle

[14] FIPS PUB 180-4: Secure Hash Standard (SHS), 2012, National Institute of Standards and Technology (NIST)

[15] ISO/IEC 10118-3:2004 – Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions, 2004, ISO

[16] NIST Special Publication 800-186, Recommendations for Discrete Logarithm-Based Cryptography, October 2019, National Institute of Standards and Technology (NIST)

Note: End of document