



# AMENDMENT

Amendment 1 to the Certification  
SRC.00032.QSCD.12.2018 of 18.12.2018

SRC Security Research & Consulting GmbH  
Emil-Nolde-Straße 7  
D-53113 Bonn  
Germany

**confirms hereby, pursuant to  
Articles 29 (1), 39 (1) and Annex II of the Regulation (EU) No. 910/2014  
that for the**

Qualified Signature / Seal Creation Device  
TCOS 3.0 Signature Card Version 2.0  
Release 2/SLE78CLX1440P

**the above mentioned Certification has been extended as follows.**

Bonn, 24 April 2019

\_\_\_\_\_  
Gerd Cimiotti

SRC Security Research & Consulting GmbH is a Designated Body notified to the EU commission for the certification of qualified electronic signature creation devices to be conformant with the Regulation (EU) No. 910/2014.

---

<sup>1</sup> 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.

**Description of the Qualified Signature Creation Device (QSCD):****1. Product Name and Scope of Delivery****1.1 Product Name**

No changes compared to the reference certificate.

**1.2 Delivery**

No changes compared to the reference certificate.

**1.3 Delivery Items**

No changes compared to the reference certificate.

**1.4 Manufacturer**

No changes compared to the reference certificate.

**2. Functional Description****2.1 Functionality and Architecture**

The support of standardised domain parameters is extended as follows:

„Sig Card“ supports the standardised domain parameters according to [RFC 5639] (Brainpool curve family), the NIST P-256 curve, as specified in [TR-03110], appendix A.2.1.1 as well as the curve Secp256k1 (Certicom) as defined in [SEC 2] (cf. [ST], ch. 1.3).

**2.2 Security Functions and Security Properties of „Sig Card“**

No changes compared to the reference certificate.

**3. Fulfilment of the relevant Requirements of Regulation (EU) No. 910/2014****3.1 Fulfilled Requirements**

No changes compared to the reference certificate.

**3.2 Conditions of Use**

No changes compared to the reference certificate.

**3.3 Cryptographic Algorithms and Parameters**

No changes compared to the reference certificate.

**3.4 Assurance Level and Attack Potential**

No changes compared to the reference certificate.

#### **4. References**

The indicated references are extended or changed as follows:

- [ETR] SRC, Evaluation Report, Evaluation Technical Report (ETR), TCOS 3.0 Signature Card Version 2.0 Release 2/SLE78CLX1440P, Version 1.2, 12.03.2019, SRC.00032.QSCD.12.2018
- [SEC 2] Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters Certicom Research, Contact: Daniel R. L. Brown (dbrown@certicom.com), January 27, 2010, Version 2.0
- [ST] Specification of the Security Target TCOS 3.0 Signature Card Version 2.0 Release 2/SLE78CLX1440P, T-Systems International GmbH, Version 2.0.2M1, 07.03.2019

**End of amendment 1**