Federal Office
for Information Security

# Certification Report

## BSI-DSZ-CC-1211-2023

for

## MTCOS Pro 2.6 SSCD / P71D352 (N7121)

from

## MaskTech International GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

# Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

**BSI-DSZ-CC-1211-2023** (*)

Secure Signature Creation Device (SSCD)

**MTCOS Pro 2.6 SSCD / P71D352 (N7121)**

| | |
|---|---|
| from | MaskTech International GmbH |
| PP Conformance: | EN 419211-2:2013 (BSI-CC-PP-0059-2009-MA-02),<br>EN 419211-3:2013 (BSI-CC-PP-0075-2012-MA-01),<br>EN 419211-4:2013 (BSI-CC-PP-0071-2012-MA-01)<br>EN 419211-5:2013 (BSI-CC-PP-0072-2012-MA-01),<br>EN 419211-6:2014 (BSI-CC-PP-0076-2013-MA-01) |
| Functionality: | PP conformant plus product specific extensions<br>Common Criteria Part 2 extended |
| Assurance: | Common Criteria Part 3 conformant<br>EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5 |
| valid until: | 26 October 2028 |

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

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

Bonn, 27 October 2023

For the Federal Office for Information Security

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

Sandro Amendola L.S.
Director-General

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

This page is intentionally left blank.

# Contents

# A. Certification

## 1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

## 2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs[3]
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

2 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

3 BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

# 3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

## 3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

## 3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2 and ALC_FLR components.

[4] Proclamation of the Bundesministerium des Innern und für Heimat of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

# 4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product MTCOS Pro 2.6 SSCD / P71D352 (N7121) has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1036-2019. Specific results from the evaluation process BSI-DSZ-CC-1036-2019 were re-used.

The evaluation of the product MTCOS Pro 2.6 SSCD / P71D352 (N7121) was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 20 October 2023. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the applicant is: MaskTech International GmbH.

The product was developed by: MaskTech International GmbH.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

# 5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 27 October 2023 is valid until 26 October 2028. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

[5] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

# 6. Publication

The product MTCOS Pro 2.6 SSCD / P71D352 (N7121) has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] MaskTech International GmbH
Nordostpark 45
90411 Nürnberg

# B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

# 1. Executive Summary

The Target of Evaluation (TOE) is the product MTCOS Pro 2.6 SSCD / P71D352 (N7121) provided by MaskTech International GmbH.

The TOE is a combination of hardware and software configured to securely create, use and manage signature creation data (SCD). The SSCD protects the SCD during its whole life cycle as to be used in a signature creation process solely by its signatory. The TOE comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the electronic signature. The TOE is used for creating digital signatures. The user called signatory can create signatures on digital documents to ensure their authenticity and provide means of integrity. Therefore the TOE operates in form of a smart card running a signature application.

The main security features of the TOE are:

- physical protection by the hardware (see below),
- initializing the RAD,
- secure storage of the RAD,
- generating key pairs,
- secure storage of key pairs,
- access control (PACE, Chip Authentication, Terminal Authentication),
- user authentication before signature creation,
- signature creation (qualified electronic signature, advanced electronic signature)
- trusted channels for secure data transfer during signature creation and SVD export and key import,
- importing of key pairs,
- configuration of keys (key attributes, usage parameters and key availability).
    - By this mechanism several TOE key configurations can be created by the administrator.

The TOE “MTCOS Pro 2.6 SSCD / P71D352 (N7121)”, which is realized by a smartcard, comprises of:

Hardware

- P71D352 (N7121) secure dual-interface controller of NXP Semiconductors Germany GmbH release packages R1, R2 and R3 (BSI-DSZ-CC-1136-V3-2022 [21]). Chip including cryptographic library are certified according to CC EAL6 augmented with ALC_FLR.1 and ASE_TSS.2 compliant to the Protection Profile BSI-CC-PP-0084-2014 [17]).

Software

- IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated
- Support Software
- IC Embedded Software (Operating System MTCOS Pro 2.6)
- SSCD application

Documentation

- User Guidance – MTCOS Pro 2.6 SSCD / P71D352 (N7121) [19]
- MTCOS Pro 2.6 on P71D352 (N7121) – Manual [20]

The Security Target [6] and [7] is the basis for this certification. It is based on the following certified Protection Profiles:

- Protection profiles for secure signature creation device – Part 2: Device with key generation, EN 419211-2:2013, Certification-ID: BSI-CC-PP-0059-2009-MA-02 [9].
- Protection profiles for Secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, EN 419211-4:2013, Certification-ID: BSI-CC-PP-0071-2012-MA-01 [10]
- Protection profiles for Secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application , EN 419211-5:2013, Certification-ID: BSI-CC-PP-0072-2012-MA-01 [11]
- Protection profiles for secure signature creation device – Part 3: Device with key import, EN 419211-3:2013, Certification-ID: BSI-CC-PP-0075-2012-MA-01 [12]
- Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted communication with signature creation application, EN 419211-6:2014, Certification-ID: BSI-CC-PP-0076-2013-MA-01 [13]

Password Authenticated Connection Establishment (PACE) including PACE Chip Authentication Mapping and the Extended Access Control Version 1 (EACv1) (i.e. Chip Authentication Version 1 (CAv1) and Terminal Authentication Version 1 (TAv1)) functionality to provide a secure authentication protocol and a secure channel for the communication with authorized terminals in phase usage/operational has been added to the ST. This implies extensions, which are adapted from the protection profiles PP.0056-V2 [14], PP-0068-V2 [15] and PP-0086 [16]. These extensions were evaluated in the course of this certification procedure.

The product also contains an MRTD application, which is not part of the TOE, but subject to BSI-DSZ-CC-1147-V3 and BSI-DSZ-CC-1148-V3.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [7], chapter 8.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

| TOE Security Functionality | Addressed issue |
|---|---|
| F.IC_CL | This Security Function covers the security functions of the hardware (IC) as well as of the cryptographic library. |
| F.Access_Control | This TSF regulates all access by external entities to operations of the TOE which are only executed after this TSF allowed access. |
| F.Identification_Authentication | This function provides identification/authentication of user roles. |

| TOE Security Functionality | Addressed issue |
|---|---|
| | |
| F.Management | Provides management and administrative functionalities. |
| F.Crypto | This function provides a high-level interface to cryptographic functions. |
| F.Verification | TOE internal functions ensure correct operation by implementing internal hardware test routines. |

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [7], chapter 10.1.

The assets to be protected by the TOE are defined in the Security Target [6] and [7], chapter 5.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [7], chapter 5.2 to 5.4.

This certification covers the configurations of the TOE as outlined in chapter 8 of this report.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

# 2. Identification of the TOE

The Target of Evaluation (TOE) is called:

**MTCOS Pro 2.6 SSCD / P71D352 (N7121)**

The following table outlines the TOE deliverables:

| No | Type | Identifier | Release | Form of Delivery |
|---|---|---|---|---|
| 1 | HW/ SW | MTCOS Pro 2.6 SSCD / P71D352 (N7121) An IC module including the necessary basic software (OS) and SSCD application (file system) | | SW is implemented in NVM memory; chip is initialized and tested before delivery to Personalization Agent. Delivery type: The OS and application software flashed on the IC Platform |
| | | 1. Hardware Platform P71D352 (N7121) secure dual-interface controller of NXP Semiconductors Germany GmbH release packages R1, R2 and R3 (BSI-DSZ-CC-1136-V3-2022 [21]). Chip including cryptographic library are certified according to CC EAL6 augmented with ALC_FLR.1 and ASE_TSS.2 compliant to the Protection Profile BSI-CC-PP-0084-2014 [17]). | P71D352 (N7121) FW: 9.2.3 CL: 0.7.6 | |
| | | 2. TOE Embedded Software IC Embedded Software (the operating system MTCOS Pro 2.6, implemented in NVM of the IC) | MTCOS Pro Version 2.6 | |

| No | Type | Identifier | Release | Form of Delivery |
|---|---|---|---|---|
| | | 3. TOE Embedded Applications IC Embedded Software / Part Application Software (containing the SSCD Application implemented in the NVM of the IC with the file system) | MTCOS Pro 2.6 SSCD<br>Build date:<br>Basic: 2022-08-11<br>Plus: 2022-10-14 | |
| 2 | DOC | 1. User Guidance – MTCOS Pro 2.6 SSCD / P71D352 (N7121), MaskTech International GmbH | [19] Version 1.3, 30.08.2023 | Password protected Secure Webserver |
| | | 2. MTCOS MANUAL – MTCOS 2.6 on P71D352 (N7121), MaskTech International GmbH | [20] Version 1.0, 07.08.2023 | |

Table 2: Deliverables of the TOE

## 2.1. Delivery items and associated delivery methods

Sensitive electronic documents: Delivery of sensitive electronic data is performed PGP encrypted via email. The guidance documentation can be obtained by password-protected download from the MaskTech International GmbH website (http://www.masktech.com).

Flash image production: The developer sends the flash image (HEX file) securely to NXP Semiconductors Germany GmbH via email.

TOE for Personalization: Chip card hardware is securely shipped to the Personalization Agent.

## 2.2. Identification of the TOE by the User

For the customer (Personalization Agent) to be able to check the correct delivery visually, a delivery note together with the hardware stating the product type and certification reference number is provided. Further checks can be done with the GET CHIP ID and the GET CHIP INFORMATION command. They return the chip identifier respectively additional information about the platform, the operating system and the patch level. Whether the chip contains the correct file system layout can be verified by checking the product identifier stored in the file EF.PROJID (see section 3.4 of [19]).

An example for possible response values of the command GET CHIP INFORMATION can be found in [19], Annex D. The chip-individual data, e.g. batch number, wafer number and coordinates may vary from the manual.

# 3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues: The TOE implements physical and logical security functionality in order to protect user data stored and operated on the smartcard when used in a hostile environment. Due to the nature of its intended application, i.e. the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. The TOE shall be shown to be highly resistant to penetration attacks to meet the security objectives. Specific details concerning the above mentioned security policies can be found in [6], sec. 6.3.

# 4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

| Security Objectives for the operational environment defined in Security Target | Description according to ST | Reference to Guidance |
|---|---|---|
| OE.SCD/SVD_Auth_Gen | Authorized SCD/SVD generation | Chapter 3.5.11, [19] |
| OE.SCD_Secrecy | SCD Secrecy | Chapter 3.5.11, [19] |
| OE.SCD_Unique | Uniqueness of the signature creation data | Chapter 3.5.11, [19] |
| OE.SCD_SVD_Corresp | Correspondence between SVD and SCD | Chapter 3.5.11, [19] |
| OE.SVD_Auth | Authenticity of the SVD | Chapter 3.5.11, [19] |
| OE.CGA_QCert | Generation of qualified certificates | Chapter 3.5.11, [19] |
| OE.SSCD_Prov_Service | Authentic SSCD delivered by SSCD-Provisioning service | Chapter 3.5.11, [19] |
| OE.Dev_Prov_Service | Authentic SSCD provided by SSCD-Provisioning Service | Chapter 3.5.11, [19] |
| OE.HID_TC_VAD_Exp | Trusted channel of HID for VAD export | Chapter 3.6.2, [19] |
| OE.DTBS_Intend | SCA sends data intended to be signed | Chapter 3.6.2, [19] |
| OE.Signatory | Security obligation of the Signatory | Chapter 3.6.2, [19] |
| OE.CGA_SSCD_Auth | Pre-initialization of the TOE for SSCD authentication | Chapter 3.5.11, [19] |
| OE.CGA_TC_SVD_Imp | CGA trusted channel for SVD import | Chapter 3.5.11, [19] |
| OE.HID_TC_VAD_Exp | Trusted channel of HID for VAD export | Chapter 3.6.2, [19] |
| OE.SCA_TC_DTBS_Exp | Trusted channel of SCA for DTBS export | Chapter 3.6.2, [19] |

Table 3: Security Objectives for the Operational Environment

Details can be found in the Security Target [6] and [7], chapter 6.2.

# 5. Architectural Information

The TOE is a composite product. It is composed from an Integrated Circuit P71D352 (N7121), IC Dedicated Software including Test and Support Software, IC Embedded Software (Operating System) and the SSCD Application. While the IC Embedded software contains the operating system MTCOS Pro 2.6, the NVM contains the SSCD application. As all these parts of software are running inside the IC, the external interface of the TOE to its environment can be defined as the external interface of this IC, the P71D352 (N7121) secure dual-interface controller of NXP Semiconductors Germany GmbH release packages R1, R2 and R3 (BSI-DSZ-CC-1136-V3-2022 [21]). Chip including cryptographic library are certified according to CC EAL6 augmented with ALC_FLR.1 and ASE_TSS.2 compliant to the Protection Profile BSI-CC-PP-0084-2014 [17]). For details concerning the CC evaluation of the NXP IC and its cryptographic libraries see the evaluation documentation under the Certification ID BSI-DSZ-CC-1136-V3-2022 (see also sec. 1.4.1). This chapter gives an overview of the TOE's Embedded Software and the corresponding TSFs which were objects of this evaluation.

The security functions of the TOE are enforced by the following subsystems:

| **Subsystem** | **TSF supported** |
|---|---|
| Application data | SP.Access_Control, SP.Identification_Authentication |
| Operation System Kernel | SP.Access_Control, SP.Crypto, SP.Identification_Authentication, SP.Management, SP.Verification |
| HAL | SP.IC_CL, SP.Crypto, SP.Identification_Authentication, SP.Verification |
| Hardware | SP.IC_CL |

Table 4: Subsystems enforcing TSF

# 6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

# 7. IT Product Testing

## 7.1. Developer Test concept

### Test Configuration

Suitable samples were chosen from the described configurations (chapter 8) to test all security functions.

### Testing approach

Each security function is covered by at least one test case. The tests performed can be categorized into two groups: tests with the real card and tests with the emulator. The latter are used for situations that cannot be achieved in a real card's life.

**Amount of developer testing performing**

The test cases are dedicated to the demonstration of the proper implementation of all security functions, card commands and operating system functionalities. For all commands resp. Functionality, test cases are specified in order to demonstrate the expected behaviour including error cases.

**Testing results**

All test cases were executed successfully and produced the expected result.

## 7.2. Evaluator Tests

**Independent Testing according to ATE_IND**

**Test Configuration**

Suitable samples were chosen from the described configurations (chapter 8) to test all security functions.

**Testing approach**

The test cases are dedicated to the demonstration of the proper implementation of all security functions, card commands and operating system functionalities. For all commands resp. Functionality, test cases are specified in order to demonstrate the expected behaviour including error cases. Each security function is covered by at least one test case. From all existing file system setups, a representative subset of setups was chosen for evaluator testing. The conducted tests can be categorized into two groups: tests with the real card and tests with the emulator. The latter are used for situations where the test result cannot be verified externally (e.g. the secure deletion of data). For the chosen setups the evaluators conducted all test cases of the developer’s test suite for non-interactive tests using the test equipment provided by the developer. The evaluators decided to focus their own independent tests on tests with real cards, but emulator tests were also conducted. For these tests the evaluators derived some test ideas from the developer tests under consideration of the described security functionality. Furthermore, the evaluators used fuzz testing to determine the correct implementation of the TOE.

**Testing Results**

All test cases developed by the evaluator were executed successfully and ended up with the expected result.

All repeated developer tests have been conducted successfully and all the actual test results were as the expected ones (as gained by the developer). For the test results of the emulator tests the evaluator repeated the emulator tests executed by the developer during the base evaluation. The repetition of tests showed the test results are consistent. Fuzz testing did not reveal any flaws in the TOE’s implementation.

**Penetration Testing according to AVA_VAN**

**Penetration testing approach**

The penetration testing was performed using the test environment of the evaluation facility. All relevant information as well as evaluation documentation was taken into account for the analysis by the evaluators. For the penetration analysis the evaluator analysed the CC

deliverables for potential vulnerabilities already during the evaluation work for the corresponding aspects. The evaluators found no exploitable vulnerabilities in the evaluation deliverables. The evaluator used the potential vulnerabilities from the JIL document as the lead for further investigations. All possible attack methods against an authentic operational TOE were analysed. Thereby the results and experience of the ISCI working group were taken into account. Potential vulnerabilities cannot be exploited during the phases development, manufacturing and personalization.

**Testing Results**

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential *High* was actually successful in the TOE's operational environment as defined in [6] and [7] provided that all measures required by the developer are applied.

# 8. Evaluated Configuration

This certification covers the following configuration of the TOE: MTCOS Pro 2.6 SSCD / P71D352 (N7121) consisting of

- Operating system and a file system in the context of the SSCD application with the NXP Semiconductors Germany GmbH P71D352 (N7121) Chip; software completely contained in NVM
- User guidance [19], including File system layout as well as Initialization/Pre-Personalization Guidance
- Product Manual [20]

The IC embedded software consists of the operating system MTCOS Pro 2.6 and an application layer, consisting of the SSCD application.

## 8.1. TOE configurations

In order to meet customer requirements, the product is provided in various configurations differing in:

- **Terminal Authentication Version 1** for the communication between the TOE and the signature creation application (SCA) or the certificate generation application (CGA), respectively, as well as for key import.
- Inclusion of an additional **decryption key.**

The decryption key and the corresponding security functionality are not in the scope of this certification. The TOE has the following main SSCD configurations:

- MRTD-LayoutA-SSCD-Std
- MRTD-LayoutFlex-SSCD-Std
- MRTD-LayoutFlex-SSCD-TA
- MRTD-LayoutFlex-SSCD-DEC-DUALUSE
- MRTD-LayoutFlex-SSCD-DEC-TA-DUALUSE

The key files to be used for asymmetric cryptography can be configured by the Personalization Agent. During personalization, the Personalization Agent sets the configuration options for the layout combinations, which were decided by the

Initialization/Pre-personalization Agent. There are no restrictions in options setting. Further details are given in the User Guidance [19].

# 9. Results of the Evaluation

## 9.1. CC specific results

The Evaluation Technical Report (ETR) [8] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

*(i) Composite product evaluation for Smart Cards and similar devices (see AIS 36). According to this concept the relevant guidance documents of the underlying platform and the documents ETR for Composition from the platform evaluations (i.e. on hardware [22,23], have been applied in the TOE evaluation.*

*(ii) Security Architecture requirements (ADV_ARC) for smart cards and similar devices (see [4], AIS 25),*

*(iii) Application of CC to Integrated Circuits, (see [4], AIS 25)*

*(iv) Attack Methods for Smartcards and Similar Devices,(see [4], AIS 26)*

*(v) Application of Attack Potential to Smartcards,(see [4], AIS 26)*

*(vi) Evaluation Methodology for CC Assurance Classes for EAL5+ and EAL6, (see [4], AIS 34)*

*(vii) Minimum Requirements for Evaluating Side-Channel Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations (see [4], AIS 46)*

*(viii) Informationen zur Evaluierung von kryptographischen Algorithmen (see [4], AIS 46).*

*(ix) Guidance for Smartcard Evaluation (see [4], AIS 37).*

For RNG assessment the scheme interpretations AIS 31 and AIS 20 were used (see [4]).

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 5 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_DVS.2 and AVA_VAN.5 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1036-2019, re-use of specific evaluation tasks was possible. Subject to the re-evaluation are changes to the certified product with respect to actual development and findings:

- Porting of the embedded software to NXP Semiconductors Germany GmbH hardware P71D352 (N7121) (certification-ID: BSI-DSZ-CC-1136-V3), which implies a different delivery procedure.

- The TOE supports import of signing keys and the creation of electronic signatures with the imported key.
- Flexible file sizes can be set during personalization.
- The hardware-depending tools have changed, which leads to changes in the Configuration Management System

The evaluation has confirmed:

- PP Conformance: EN 419211-2:2013 - Protection profiles for secure signature creation device - Part 2: Device with key generation, BSI-CC-PP-0059-2009-MA-02 [9],

  EN 419211-3:2013 - Protection profiles for secure signature creation device - Part 3: Device with key import, BSI-CC-PP-0075-2012-MA-01 [12],

  EN 419211-4:2013 - Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application 1.0.1, CEN / CENELEC (TC224/WG17), BSI-CC-PP-0071-2012-MA-01 [10],

  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, CEN / ISSS - Information Society Standardization System, BSI-CC-PP-0072-2012-MA-01 [11],

  EN 419211-6:2014 - Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application, BSI-CC-PP-0076-2013-MA-01 [13]
- for the Functionality: PP conformant plus product specific extensions
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

The evaluation was performed as a composite evaluation according to AIS 36 (see [4]) and therefore relies on the platform certification of the used IC including its cryptographic libraries. Refer to certification ID BSI-DSZ-CC-1136-V3-2022 and subsequent BSI-DSZ-CC-1136-V3-2022-MA-01 ([22], [24], [23]).

## 9.2. Results of cryptographic assessment

The Table A.1 presented in the Security Target [6], chapter A gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy.

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

For the TOE's cryptographic functionalities, Table A.1 in the Security Target outlines - where applicable - the standard of application where their specific appropriateness is stated. According to the referenced standards these algorithms are suitable for authentication, key agreement, authenticity, integrity, confidentiality and trusted channel. An explicit validity period is not given at this point.

For the rows no 3, 4 and 6 in Table A.1 of the Security Target that address RSA and ECC based signature generation and key generation regards the TOE's SSCD functionality, the security level of these algorithms as a kind of rating from cryptographic point of view is of relevance. Cryptographic functionalities with a security level of lower than 120 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related cryptographic operations are appropriate for the intended system. Further hints and guidelines on the respective security level and validity period of the cryptographic algorithms can be derived from the document 'Technische Richtlinie BSI TR-02102-1' (refer to https://www.bsi.bund.de) and as well from the SOG-IS crypto catalogue [25].

The cryptographic algorithms and protocols as outlined in Table A.1 of the Security Target are implemented in the card operating system and hereby make use of the P71D352 (N7121) secure dual-interface controller and its related cryptographic libraries (V0.7.6) from NXP Semiconductors Germany GmbH certified under ID BSI-DSZ-CC-1136-V3-2022 and subsequent BSI-DSZ-CC-1136-V3-2022-MA-01. In particular, the core routines for RSA (signature generation and verification, RSA key generation, RSA DH), ECC (ECDSA signature generation and verification, ECC key generation, ECDH), the SHA hash calculation, the symmetric cryptographic algorithms AES and 3DES encryption and decryption in CBC mode and the PTG.3 random number generation are taken from the cryptographic libraries. The security evaluation of these cryptographic algorithms was performed in the framework of the certification of the IC with its related cryptographic libraries (refer to [22], [24]). The TOE relies on the correct (i.e. standard-conform) and secure implementation of these cryptographic algorithms. The remaining cryptographic implementation was analysed in the framework of the present composite evaluation of the TOE.

# 10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs 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, in particular the card issuing organisation and the national organisation responsible for the risk management, 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 of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

# 11. Security Target

For the purpose of publishing, the Security Target [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

# 12. Regulation specific aspects (eIDAS, QES)

This certificate is not a confirmation of conformity to the EU eIDAS Regulation. Nevertheless, this certificate and the technical results may be reused for issuing a certificate of conformity to the EU eIDAS regulation in a separate process by a designated certification body notified to the EU Commission.

# 13. Definitions

## 13.1. Acronyms

| | |
|---|---|
| **AIS** | Application Notes and Interpretations of the Scheme |
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany |
| **BSIG** | BSI-Gesetz / Act on the Federal Office for Information Security |
| **CA** | Chip Authentication |
| **CCRA** | Common Criteria Recognition Arrangement |
| **CC** | Common Criteria for IT Security Evaluation |
| **CEM** | Common Methodology for Information Technology Security Evaluation |
| **CGA** | Certificate generation application |
| **cPP** | Collaborative Protection Profile |
| **DOC** | Documents |
| **DTBS** | Data to be signed |
| **EAL** | Evaluation Assurance Level |
| **ETR** | Evaluation Technical Report |
| **HEX** | Hexadecimal |
| **HID** | Human Interface Device |
| **HW** | Hardware |
| **IC** | Integrated Circuit |
| **IT** | Information Technology |
| **ITSEF** | Information Technology Security Evaluation Facility |
| **MRTD** | Machine Readable Travel Documentation |
| **NVM** | Non-Volatile Memory |
| **PACE** | Password Authenticated Connection Establishment |

| | |
|---|---|
| **PP** | Protection Profile |
| **RAD** | Reference authentication data |
| **SAR** | Security Assurance Requirement |
| **SCA** | Signature creation application |
| **SCD** | Signature Creation Data |
| **SFP** | Security Function Policy |
| **SFR** | Security Functional Requirement |
| **SM** | Secure Messaging |
| **SSCD** | Secure Signature Creation Data |
| **ST** | Security Target |
| **SVD** | Signature verification data |
| **SW** | Software |
| **TA** | Terminal Authentication |
| **TOE** | Target of Evaluation |
| **TSF** | TOE Security Functionality |
| **VAD** | Verification authentication data |

## 13.2. Glossary

**Augmentation** - The addition of one or more requirement(s) to a package.

**Collaborative Protection Profile -** A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

**Extension** - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

**Formal** - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

**Informal** - Expressed in natural language.

**Object** - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

**Package** - named set of either security functional or security assurance requirements

**Protection Profile** - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

**Security Target** - An implementation-dependent statement of security needs for a specific identified TOE.

**Semiformal** - Expressed in a restricted syntax language with defined semantics.

**Subject** - An active entity in the TOE that performs operations on objects.

**Target of Evaluation** - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

**TOE Security Functionality** - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

# 14. Bibliography

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

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, 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[7] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-1211-2023, Version 0.8, 13 September 2023, Security Target – Secure signature creation device with key generation and key import, MTCOS Pro 2.6 SSCD / P71D352 (N7121), MaskTech International GmbH (confidential document)

[7] 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
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- 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 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 38, Version 2, Reuse of evaluation results
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren
- AIS 47, Version 1.1, Regelungen zu Site Certification

[7] Security Target BSI-DSZ-CC-1211-2023, Version 1.3, 30 August 2023, Security Target – Secure signature creation device with key generation and key import (Public Version), MTCOS Pro 2.6 SSCD / P71D352 (N7121), MaskTech International GmbH (sanitised public document)

[8] Evaluation Technical Report, Version 1.6, 20 October 2023, Evaluation Technical Report (ETR), SRC Security Research & Consulting GmbH (confidential document)

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

[10] EN 419211-4:2013 - Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application 1.0.1, CEN / CENELEC (TC224/WG17), BSI-CC-PP-0071-2012-MA-01

[11] 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, CEN / ISSS - Information Society Standardization System, BSI-CC-PP-0072-2012-MA-01

[12] EN 419211-3:2013 - Protection profiles for secure signature creation device - Part 3: Device with key import, BSI-CC-PP-0075-2012-MA-01

[13] EN 419211-6:2014 - Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted channel to signature creation application, BSI-CC-PP-0076-2013-MA-01

[14] Common Criteria Protection Profile – Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE, BSI, Version 1.3.2, 05 December 2012, Certification-ID: BSI-CC-PP-0056-v2-2012

[15] Common Criteria Protection Profile - Electronic Passport using Standard Inspection Procedure with PACE (ePass PACE PP), Version 1.01, 22 July 2014, Certification-ID: BSI-CC-PP-0068-V2-2011-MA01

[16] BSI-CC-PP-0086-2015, Common Criteria Protection Profile / Electronic document implementing Extended Access Control Version 2 (EAC2) based on BSI TR-03110 (EAC2_PP), BSI, Version 1.01, 20 May 2015

[17] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, 13 January 2014, Certification-ID: BSI-CC-PP-0084-2014

[18] Configuration list for the TOE, Version 0.4, 13 October 2023, Configuration List of MTCOS Pro 2.6 SSCD / P71D352 (N7121), MaskTech International GmbH (confidential document)

[19] User Guidance – MTCOS Pro 2.6 SSCD / P71D352 (N7121), Version 1.3, 30 August 2023, MaskTech International GmbH

[20] MTCOS MANUAL – MTCOS 2.6 on P71D352 (N7121), Version 1.0, 07.08.2023, MaskTech International GmbH

[21] NXP Semiconductors, Security Target Lite ’NXP Secure Smart Card Con-troller N7121 with IC Dedicated Software and Crypto Library’, BSI-DSZ-CC-1136-V3-2022, Rev. 2.6, 13 June 2022

[22] Certification Report, BSI-DSZ-CC-1136-V3-2022 for NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library from NXP Semiconductors Germany GmbH, 07 September 2022

[23] ETR for Composition NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (N7121) – EAL6+ according to AIS36, TÜV Informationstechnik GmbH, BSI-DSZ-CC-1136-V3-2022, Version 2, 25 August 2022

[24] Assurance Continuity Maintenance Report - BSI-DSZ-CC-1136-V3-2022-MA-01 NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) from NXP Semiconductors Germany GmbH, 17 May 2023

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

[26] CHANGES AND IMPACT ANALYSIS, MTCOS Pro 2.6 SSCD / P71D352 (N7121), Secure signature creation device with key generation, Version 0.1, 09 September 2022, MaskTech International GmbH (confidential document)

# C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

# D. Annexes

## List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

# Annex B of Certification Report BSI-DSZ-CC-1211-2023

## Evaluation results regarding development and production environment

The IT product MTCOS Pro 2.6 SSCD / P71D352 (N7121) (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 27 October 2023, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2, ALC_COMP.1)

are fulfilled for the development and production sites of the TOE listed below:

a) MaskTech International GmbH, Nordostpark 45, 90411 Nuernberg Germany, Re-use of complete Site Audit of BSI-DSZ-CC-1064-2020-MA-01, Site certificate valid until 15 January 2024 (Software)

b) Linxens (Thailand) Co Ltd., 142 Moo, Hi-Tech Industrial Estate, Tambon Ban Laean, Am-phor Bang-pa-in, 13160 Ayutthaya, Thailand, BSI-DSZ-CC-S-0207-2021, Site certificate valid until 1 November 2023 (Initialization/Pre-personalization)

c) HID Global Ireland, Teoranta Pairc Tionscail na Tullaigh, Baile na hAbhann, Co. Galway, Ireland, BSI-DSZ-CC-S-0232-2023, Site certificate valid until 22 September 2025 2024 (Initialization/Pre-personalization)

d) HID Global Sdn. Bhd. No. 2, Jalan i-Park 1/1 Kawasan Perindustrian i-Park Bandar Indahpura 81000 Kulai, Johor Malaysia, BSI-DSZ-CC-S-0233-2023, Site certificate valid until 10 July 2025 2024 (Initialization/Pre-personalization)

e) NXP Semiconductors GmbH, Business Unit security and connectivity (BU S&C) Troplowitzstraße 20 22529 Hamburg Germany, Site Certificate Re-use of ALC aspect from BSI-DSZ-CC-1136-V3-2022, Site certificate valid until 6 September 2027[8] (Manufacturer, Initialization/Pre-personalization)

f) Linxens Germany GmbH, Manfred-von-Ardenne-Ring 12, 01099 Dresden, BSI-DSZ-CC-S-0214-2022, Site certificate valid until 22 September 2024 (Initialization/Pre-personalization)

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [7]) are fulfilled by the procedures of these sites.

[8]Expiration date of the IC certificate. The NXP site in Hamburg is also equipped with a site certificate with certification ID BSI-DSZ-CC-S-0181-2022. This site certificate is valid until 29.02.2024

Note: End of report