Certification Report

BSI-DSZ-CC-1073-V3-2026

for

Xaica-α PLUS ePassport on MTCOS Pro 2.6 with SAC (PACE) and Active Authentication / ST31N600

from

MaskTech International GmbH

sponsored by

NTT DATA CORPORATION

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1073-V3-2026 (*)

ePass

Xaica-α PLUS ePassport on MTCOS Pro 2.6 with SAC (PACE) and Active Authentication / ST31N600

from	MaskTech International GmbH
sponsored by	NTT DATA CORPORATION
PP Conformance:	None - Based on Protection Profile for ePassport IC with SAC (PACE) and Active Authentication, Version 1.00, March 8, 2016, JISEC C0499
Functionality:	Product specific Security Target Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_DVS.2, ALC_FLR.3 and AVA_VAN.5
valid until:	10 February 2031

SOGIS
Recognition Agreement
for components up to
EAL 4

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), CEM:2022 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), CC:2022. 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.

Bonn, 11 February 2026

For the Federal Office for Information Security

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

Fabian Hodouschek   L.S.   Sandro Amendola
Head of Certification   Director-General Directorate General S

Bundesamt für Sicherheit in der Informationstechnik

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

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 (Federal Ministry of the Interior)
- 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 licensing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), CC:2022 [4] [1] also published as ISO/IEC 15408

---

[1]   Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 2 December 2025, BGBl. 2025 , no. 301, p. 2

[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 02 December 2025, Bundesgesetzblatt 2025, no. 301

[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), CC:2022 [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.

---

4   Proclamation of the Federal Office for Information Security dated 14. April 2023 at https://www.bsi.bund.de.

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.   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 Xaica-α PLUS ePassport on MTCOS Pro 2.6 with SAC (PACE) and Active Authentication / ST31N600 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1073-V2-2020. Specific results from the evaluation process BSI-DSZ-CC-1073-V2-2020 were re-used.

The evaluation of the product Xaica-α PLUS ePassport on MTCOS Pro 2.6 with SAC (PACE) and Active Authentication / ST31N600 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 23 January 2026. 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 sponsor is: NTT DATA CORPORATION.

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 evaluated guidance documentation, are observed,

● the product is operated in the environment as specified 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. 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. Therefore the BSI reserves the right to revoke the certificate, especially if a exploitable vulnerability of the certified product gets to known.

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

---

[5]   Information Technology Security Evaluation Facility

maximum validity of the certificate has been limited. The certificate issued on 11 February 2026 is valid until 10 February 2031. 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,

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 Xaica-α PLUS ePassport on MTCOS Pro 2.6 with SAC (PACE) and Active Authentication / ST31N600 has been included in the BSI list of certified products, which is published regularly in the listing found at the BSI Website https://www.bsi.bund.de/dok/Zertifizierung-Gesamtlisten. Further information can be obtained from BSI-Infoline +49 (0)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 Xaica-α PLUS ePassport on MTCOS Pro 2.6 with SAC (PACE) and Active Authentication / ST31N600. The TOE is an electronic travel document representing a contactless smart card providing Password Authenticated Connection Establishment (PACE) and the Active Authentication protocol according to the 'ICAO 9303' and BSI TR-03110 and is programmed according to ICAO Technical Report "Supplemental Access Control".

The Security Target [5] is the basis for this certification. It is based on the certified Protection Profile Protection Profile for ePassport IC with SAC (PACE) and Active Authentication, Version 1.00, March 8, 2016, JISEC C0499 [7]. For formal reasons no strict conformance to the original Japanese Protection Profile is claimed, because the English translation of [7] is not officially certified

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 4 augmented by ALC_DVS.2, ALC_FLR.3 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [5] and [8], chapter 6.1. They are all selected from Common Criteria Part 2. Thus the claimed set of SFRs in the ST is CC Part2 conformant.

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.
F.Management	Provides management capabilities during development, usage/preparation and usage/operational phases to set file layout, security attributes, and writing of data groups.
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 [5] and [8], chapter 7.1.

The assets to be protected by the TOE are defined in the Security Target [5] and [8], chapter 3.1. 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 [5] and [8], chapter 3.

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

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 52, 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:

Xaica-α PLUS ePassport on MTCOS Pro 2.6 with SAC (PACE) and Active Authentication / ST31N600

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/SW	Hardware Platform STMicroelectronics ST31N600 secure dual-interface controller	ST31N600 A03 FW v3.1.2	SW is implemented in NVM memory; chip is initialised and tested before delivery to IC Sheet Manufacturer. Delivery type: The OS and application software flashed on the IC Platform
		Hardware Platform Cryptographic Library STMicroelectronics cryptographic library NesLib 6.7.4	6.7.4	
		TOE Embedded Software IC Embedded Software (the operating system MTCOS Pro 2.6, implemented in NVM of the IC)	MTCOS Pro 2.6	
		TOE Embedded Applications IC Embedded Software / Part Application Software (containing the ePassport Application implemented in the NVM of the IC with the file system)	MTCOS Pro 2.6 with SAC (PACE) and Active Authentication	
2	DOC	User Guidance –Xaica-α PLUS ePassport on MTCOS Pro 2.6 / ST31N600	Version 1.1, 07.01.2026	PGP encrypted email
3	SCRIPT	Configuration Script generic-patch0v0-temp2perm.txt	Revision 36142 [9]	

Table 2: Deliverables of the TOE

Delivery items and associated delivery methods

Sensitive electronic documents: Delivery of sensitive electronic data is performed PGP en-crypted via email. This delivery method also applies for the guidance documentation.

Flash image production: The developer sends the flash image (HEX file) PGP-authenticated and encrypted.

TOE for Pre-issuance Personalization: Chip card hardware is securely shipped to the IC Sheet Manufacturer.

Identification of the TOE by the User

The sensitive electronic documents are retrieved by the IC Sheet Manufacturer via PGP encrypted mail. The delivery process of the IC from manufacturer to IC Sheet Manufacturer is supervised by STMicroelectronics.

The IC Sheet Manufacturer responsible for pre-issuance personalization can identify the product by:

● delivery note,

● correct working of the configuration script (generic-patch0v0-temp2perm.txt) which ensures a correct hardware

● the correct working of the transport key (PIN #8) and

● using command GET CHIP INFORMATION.

The response values of the command GET CHIP INFORMATION can be found in [10], Annex A.2. The chip-individual data, e.g. the Chip ID, and possibly the Initialization Key Identifier may be different from the manual.

After pre-issuance personalization the product is delivered securely to the Booklet Manufacturer supervised by the IC Sheet Manufacturer. The Booklet Manufacturer is able to check the correct delivery visually by the labelling of the TOE. Further, the Booklet Manufacturer must perform a VERIFY command to authenticate himself against the post-issuance transport key PIN #1.

For the customer 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.

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 smart-card 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 the ST [5], chapter 6.3.1.2.

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:

● OE.Administrative_Env

● OE.PKI

● OE.Personalization

Details can be found in the Security Target [5] and [8], chapter 4.2.

5. Architectural Information

The TOE is a composite product. It is composed from an Integrated Circuit (TOE-IC), IC Embedded Software (TOE-ES/BS) and IC Embedded Software / Part Application Software (containing the ePassport Application implemented in the NVM of the IC) (TOE-ES/AS). While the IC Embedded software contains the operating system MTCOS Pro 2.6, the Part Application Software contains the ePassport 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 STMicroelectronics ST31N600 secure dual-interface controller. For details concerning the CC evaluation of the STM IC and its cryptographic libraries see the evaluation documentation under the Certification IDs ANSSI-CC-2022/21-R02 [13] and ANSSI-CC-2022/42-R02 [14]. 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 (cf. Table 1) are enforced by the following subsystems:

Subsystem	TSF supported
Application data	F.Access_Control, F.Identification_Authentication
Operation System Kernel	F.Access_Control,F.Identification_Authentication, F.Management, F.Crypto, F.Verification
HAL	F.IC_CL, F.Crypto, F.Identification_Authentication, F.Verification
Hardware	F.IC_CL

Table 3: 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

The TOE has only one file system layout, namely the ePassport application. Note that in the operational usage phase, two different TOE configurations are present, which differ in the availability of the BAC functionality. The present evaluation process BSI-DSZ-CC-1073-V3 deals with only the PACE functionality enabled. The BAC functionality is disabled in the post-issuance personalisation phase, resulting in a TOE configuration which only uses the PACE mechanism. This BAC+PACE configuration is evaluated in the parallel performed evaluation course BSI-DSZ-CC-1074-V3.

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. 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). The evaluators decided to focus their own independent tests on tests with real cards. For these tests the evaluators derived some test ideas from the developer tests under consideration of the described security functionality.

All test cases were executed successfully and ended up with the expected result. If necessary the developer gave additional annotations.

Based on this the evaluators decided to focus their own independent tests on tests with real cards. Developer tests with real cards and with emulated cards using the APDU Interface concerning the correctness of implementation of TSF code were repeated by the evaluators. During their independent testing, the evaluators covered:

- testing APDU commands related to Access Control,

- testing APDU commands related to Identification and Authentication,

- testing APDU commands related to Management,

- testing APDU commands related to Cryptographic Functions and Verification,

- fuzzy testing related to verify Reliability of the TOE,

- source code analysis performed by the evaluators,

- testing the commands which are used to execute the different authentication proto-cols,

- fault injection attacks (laser attacks and EM Glitches),

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 the ST [5] provided that all measures required by the developer are applied.

8.   Evaluated Configuration

This certification covers the following configurations of the TOE:

Xaica-α PLUS ePassport on MTCOS Pro 2.6 with SAC (PACE) and Active Authentication / ST31N600 consisting of

- STMicroelectronics ST31N600 secure dual-interface controller

- cryptographic library NesLib 6.7.4

- the basic software (OS) implemented on the IC,

- a file system in the context of the ePassport application,

- the configuration script and

- the associated guidance documentation.

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

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [6] 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)   *Application of CC to Integrated Circuits,*

(ii)   *Attack Methods for Smartcards and Similar Devices,*

(iii)   *Application of Attack Potential to Smartcards,*

(iv)   *Evaluation Methodology for CC Assurance Classes for EAL5+ and EAL6,*

(v)   *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 [11, 12], have been applied in the TOE evaluation.*

(see [4], AIS 25, AIS 26, AIS 34, AIS 36, AIS 46).

For smart card specific methodology the scheme interpretations AIS 25, AIS 26 and AIS 36 were used (see [4]). 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 4 package including the class ASE as defined in the CC (see also part C of this report)

● The components ALC_DVS.2, ALC_FLR.3 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-1073-V2-2020, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the following:

● The platform of STMicroelectronics was changed from ST31G480 D01 to ST31N600. Certification used for the composite procedure is therefore updated to ANSSI-CC-2022/21-R02.

● The cryptographic library of STMicroelectronics is updated from NesLib version 6.2.1 to version 6.7.4 which is certified under ANSSI-CC-2022/42-R02.

The evaluation has confirmed:

● PP Conformance: None [7]

---

[7]Note that the ST is based on the Protection Profile Protection Profile for ePassport IC with SAC (PACE) and Active Authentication, Version 1.00, March 8, 2016, JISEC C0499 [7], which requires strict conformance. For formal reasons no strict conformance to the original Japanese PP is claimed, because the English translation of [7] is not officially certified.

- for the Functionality: Product specific Security Target
                            Common Criteria Part 2 conformant

- for the Assurance: Common Criteria Part 3 conformant
                            EAL 4 augmented by ALC_DVS.2, ALC_FLR.3 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.

9.2.   Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 52, Para. 4, Clause 2). But 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 crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The table A1 presented in chapter A of the Security Target gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines the standard of application where its specific appropriateness is stated.

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 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 [8] 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 [5] 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)

None.

13. Definitions

13.1. Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
APDU	Application Protocol Data Unit
BAC	Basic Access Control
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
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
DES	Data Encryption Standard; symmetric block cipher algorithm
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
JBMIA	Japan Business Machine and Information System Industries Association
JISEC	Japan Information Technology Security Evaluation and Certification Scheme
MAC	Message Authentication Code
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
SAC	Supplemental Access Control
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SM	Secure Messaging
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

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.

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/CC
        ISO-Version:
        ISO 15408:2022, Common Criteria for Information Technology Security Evaluation
        - Part 1: Introduction and general model
        - Part 2: Security functional components
        - Part 3: Security assurance components
        - Part 4: Framework for the specification of evaluation methods and activities
        - Part 5: Pre-defined packages of security requirements
        https://www.iso.org/standard/72891.html
        https://www.iso.org/standard/72892.html
        https://www.iso.org/standard/72906.html
        https://www.iso.org/standard/72913.html
        https://www.iso.org/standard/72917.html
        CCRA-Version:
        CC:2022 R1, Common Criteria for Information Technology Security Evaluation
        - Part 1: Introduction and general model
        - Part 2: Security functional components
        - Part 3: Security assurance components
        - Part 4: Framework for the specification of evaluation methods and activities

- Part 5: Pre-defined packages of security requirement
https://www.commoncriteriaportal.org

[2] Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology
ISO-Version:
ISO 18045:2022: Information technology Security techniques Methodology for IT security evaluation
https://www.iso.org/standard/72889.html
CCRA-Version:
CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
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 licensing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8]
https://www.bsi.bund.de/AIS

[5] Security Target BSI-DSZ-CC-1073-V3-2026, Version 0.4, 25 August 2025, Security Target – Xaica-α PLUS ePassport on MTCOS Pro 2.6 with SAC (PACE) and Active Authentication / ST31N600, MaskTech International GmbH (confidential document)

[6] Evaluation Technical Report, Version 1.0, 19.01.2026, Evaluation Report- Evaluation Technical Report (ETR), SRC Security Research & Consulting GmbH, (confidential document)

[7] Protection Profile for ePassport IC with SAC (PACE) and Active Authentication, Version 1.00, March 8, 2016, JISEC C0499

[8] Security Target BSI-DSZ-CC-1073-V3-2026, Version 1.0, 24 November 2025, Xaica-α PLUS ePassport on MTCOS Pro 2.6 with SAC (PACE) and Active Authentication / ST31N600, MaskTech International GmbH (sanitised public document)

[8]specifically

- AIS 20, Version 4, 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 4, 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 38, Version 2, Reuse of evaluation results

[9] Configuration list, Version 0.4, 07 January 2026, Configuration list - Xaica-α PLUS ePassport on MTCOS Pro 2.6 / ST31N600 MaskTech International GmbH (confidential document)

[10] User Guidance, Version 1.1, 07 January 2026, User Guidance –Xaica-α PLUS ePassport on MTCOS Pro 2.6 / ST31N600, MaskTech International GmbH,

[11] ETR lite for Composition, Revision 1.0, 21 March 2025, RANGOLI Reevaluation 2024, Certification ID ANSSI-CC-2022/21-R02 for ST31N600 of STMicroelectronics, THALES SIX GTS FRANCE SAS

[12] ETR lite for Composition, Revision 3.0, 26 May 2025, BRUGES Reevaluation 2024, Certification ID ANSSI-CC-2022/42-R02 for cryptographic library NesLib 6.7.4 on ST31N600 IC of STMicroelectronics, THALES SIX GTS FRANCE SAS

[13] Certification Report, 07 March 2025, Rapport de certification ANSSI-CC-2022/21-R02 for ST31N600 of STMicroelectronics, Agence nationale de la sécurité des systèmes d'information

[14] Certification Report, 04 June 2025, Rapport de certification ANSSI-CC-2022/42-R02 for cryptographic library NesLib 6.7.4 on ST31N600 IC of STMicroelectronics, Agence nationale de la sécurité des systèmes d'information

C.   Excerpts from the Criteria

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

- On conformance claim definitions and descriptions refer to CC:2022 part 1 chapter 10.5

- On the concept of assurance classes, families and components refer to CC:2022 Part 3 chapter 6.1

- On the concept and definition of pre-defined assurance packages (EAL) refer to CCRA CC:2022 Part 5.

- On the assurance class ASE for Security Target evaluation refer to CC:2022 Part 3 chapter 9

- On the detailed definitions of the assurance components for the TOE evaluation refer to CC:2022 Part 3 chapters 7 to 15

- The table 1 in CC:2022 part 5, Chapter 4.2 summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published as the CCRA Version at
https://www.commoncriteriaportal.org/cc/index.cfm

The CC are published as the ISO/IEC Version at
https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

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-1073-V3-2026

Evaluation results regarding development and production environment

The IT product Xaica-α PLUS ePassport on MTCOS Pro 2.6 with SAC (PACE) and Active Authentication / ST31N600 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), CEM:2022 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), CC:2022.

As a result of the TOE certification, dated 11 February 2026, 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.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1, ALC_COMP.1)

are fulfilled for the development and production sites <u>of the TOE</u> listed below:

   a)   MaskTech International GmbH, Nordostpark 45, 90411 Nuremberg, Germany (Development)

   b)   The manufacturing and installation steps are completely performed by STMicroelectronics. For development and production sites regarding the platform please refer to the certification report ANSSI-CC-2022/21-R02 [13]

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [5] and [8]. 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 [5] and [8]) are fulfilled by the procedures of these sites.

Note: End of report