Federal Office
for Information Security

# Certification Report

## BSI-DSZ-CC-1074-2019

for

## Xaica-α PLUS ePassport on MTCOS Pro 2.5 with SAC (BAC+PACE) and Active Authentication / ST31G480 C01

from

## MaskTech International GmbH

sponsored by

## NTT DATA CORPORATION

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-1074-2019** (*)

**Xaica-α PLUS ePassport on MTCOS Pro 2.5 with SAC (BAC+PACE) and Active Authentication / ST31G480 C01**

| | |
|---|---|
| from | MaskTech International GmbH |
| sponsored by | NTT DATA CORPORATION |
| PP Conformance: | None<br>based on the Protection Profile “JISEC C0500, version 1.00, Protection Profile for ePassport IC with SAC (BAC+PACE) and Active Authentication, JBMIA” (English translation) |
| Functionality: | Product specific Security Target<br>Common Criteria Part 2 extended |
| Assurance: | Common Criteria Part 3 conformant<br>EAL 4 augmented by ALC_DVS.2 |

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 4

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.

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

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, 25 January 2019

For the Federal Office for Information Security

Joachim Weber
Head of Branch

L.S.

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

**Bundesamt für Sicherheit in der Informationstechnik**
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (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[2]
- BSI Certification and Approval Ordinance[3]
- BSI Schedule of Costs[4]
- 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 licencing process (CC-Stellen) [3]

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

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

3 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

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1] also published as ISO/IEC 15408.
- 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.sogisportal.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.

[5] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2 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 2.5 with SAC (BAC+PACE) and Active Authentication / ST31G480 C01 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1073-2019. Specific results from the evaluation process BSI-DSZ-CC-1073-2019 were re-used.

The evaluation of the product Xaica-α PLUS ePassport on MTCOS Pro 2.5 with SAC (BAC+PACE) and Active Authentication / ST31G480 C01 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 18 December 2018. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] 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 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

[6] Information Technology Security Evaluation Facility

maximum validity of the certificate has been limited. The certificate issued on 25 January 2019 is valid until 24 January 2024. 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 2.5 with SAC (BAC+PACE) and Active Authentication / ST31G480 C01 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[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] MaskTech International GmbHNordostpark 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 2.5 with SAC (BAC+PACE) and Active Authentication / ST31G480 C01 provided by MaskTech International GmbH. The TOE is an electronic travel document representing a contactless smart card providing the Basic Access Control (BAC), 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 main security features of the TOE are:

- BAC function (mutual authentication and Secure Messaging),
- PACE function (mutual authentication and Secure Messaging),
- Active Authentication support function (prevention of copying the IC chip),
- Disabling function of BAC function (prohibition of operating BAC after issuing a passport),
- Write protection function (protection on writing data after issuing a passport),
- Protection function in transport (protection against attacks during transport before issuing the TOE) and
- Tamper resistance (protection against confidential information leak due to physical attacks).

The Security Target [6] and [7] is the basis for this certification. It is based on the Protection Profile “*JISEC C0500, version 1.00, Protection Profile for ePassport IC with SAC (BAC+PACE) and Active Authentication, JBMIA, 2016-03-08.*” (English translation) [9], which requires strict conformance. The security functionality of the TOE is in principle strict conformant to the Protection Profile [9]. For formal reasons no strict conformance to the original Japanese Protection Profile is claimed, because the English translation [9] is not officially certified[8]. Therefore the whole Security Target was evaluated. The additions to the Protection Profile [9] are described in [6] and [7], chapter 2.5.

Please note that in consistency to the protection profile [9] the security mechanism Basic Access Control is in the main focus of this evaluation process in addition to the security mechanisms Password Authenticated Connection Establishment and Active Authentication. These were subject of the separate evaluation process BSI-DSZ-CC-1073-2019 [14] and the corresponding results were reused during this evaluation.

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.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [7], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

[8] ECSEC evaluated the Japanese Protection Profile C0500. After certification, the Protection Profile C0500 has been translated into English for publishing on the Web site of JISEC. The translated version [9] was checked by the IPA (Japanese certification body). But it was not strictly checked if the English translation used the appropriate English words as the CC-specific technical expression.

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 | Regulates all access by external entities to operations of the TOE which are only executed after this TSF allowed access |
| F.Identification_Authentication | 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 | Provides a high-level interface to cryptographic functions |
| F.Verification | TOE internal functions to ensure correct operation |

Table 1: TOE Security Functionalities

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

The assets to be protected by the TOE are defined in the Security Target [6] and [7], 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 [6] and [7], 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 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:

**Xaica-α PLUS ePassport on MTCOS Pro 2.5 with SAC (BAC+PACE) and Active Authentication / ST31G480 C01**

The following table outlines the TOE deliverables:

| No | Type | Identifier | Release | Form of Delivery |
|---|---|---|---|---|
| 1 | HW/SW | Xaica-α PLUS ePassport on MTCOS Pro 2.5 with SAC (BAC+PACE) and Active Authentication / ST31G480 C01<br>An IC module including the necessary basic software (OS) and ePassport application (file system): | | |

| No | Type | Identifier | Release | Form of Delivery |
|---|---|---|---|---|
| | | 1. Hardware Platform<br>STMicroelectronics ST31G480 C01 secure dual-interface controller | ST31G480 C01<br>FW v2.1.0<br>CL: Neslib v5.2.0 | SW is implemented in NVM memory; chip is initialised and tested before delivery to IC Sheet Manufacturer.<br>Delivery type: The OS and application software flashed on the IC Platform |
| | | 2. TOE Embedded Software<br>IC Embedded Software (the operating system MTCOS Pro 2.5, implemented in NVM of the IC) | MTCOS Pro Version 2.5,<br>Build date 2018-03-02 | |
| | | 3. TOE Embedded Applications<br>IC Embedded Software / Part Application Software (containing the ePassport Application implemented in the NVM of the IC with the file system) | MTCOS Pro 2.5 with<br>SAC (BAC+PACE) and Active Authentication | |
| 2 | DOC | Xaica-α PLUS ePassport – User Guidance [11] | Version 1.3, 10.12.2018 | PGP encrypted email |
| 3 | SCRIPT | Configuration Script,<br>20180302-generic-patch0v0-temp2perm.txt | Revision 104 | |

Table 2: Deliverables of the TOE

The following delivery methods are used:

- Sensitive electronic documents: Delivery of sensitive electronic data is performed PGP encrypted 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 Personalisation: Chip card hardware is securely shipped to the IC Sheet Manufacturer.

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 personalisation can identify the product by:

- delivery note,
- correct working of the configuration script (20180302-generic-patch0v0-temp2perm.txt) which ensures a correct hardware,
- the correct working of the transport key (PIN #8) and
- using the command GET CHIP INFORMATION.

The response values of the command GET_CHIP_INFORMATION can be found in the guidance documentation [11], 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 personalisation 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 selected 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 [6] and [7], 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:

- OE.Administrative_Env
- OE.Disable_BAC
- OE.PKI
- OE.Personalization

Details can be found in the Security Target [6] and [7], chapter 4.2.

# 5. Architectural Information

The TOE is a composite product. It is composed from an Integrated Circuit, IC Embedded Software and IC Embedded Software / Part Application Software (containing the ePassport Application implemented in the NVM of the IC). While the IC Embedded software contains the operating system MTCOS Pro 2.5, 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 ST31G480 C01 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 ID ANSSI-CC-2017/61 [12].

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

| Subsystem | TSF supported |
|---|---|
| Application data | F.Access_Control, F.Identification_Authentication |

| Subsystem | TSF supported |
|---|---|
| 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

## 7.1. Developer Test concept

### TOE test configuration

The TOE test configuration is defined by the notation: *Xaica-α PLUS ePassport on MTCOS Pro 2.5 with SAC (BAC+PACE) and Active Authentication / ST31G480 C01*. The TOE has only one file system layout, namely the ePassport application. In this configuration the BAC+PACE functionality is enabled. The BAC functionality can be disabled in the post-issuance personalisation phase, resulting in a TOE configuration which only uses the PACE mechanism. This PACE only configuration is subject of the separate evaluation process BSI-DSZ-CC-1073-2019 [14].

### 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 performed

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 matched the expected result.

## 7.2. Evaluator Tests

### Independent Testing according to ATE_IND

### TOE test configuration

The TOE test configuration is defined by the notation: *Xaica-α PLUS ePassport on MTCOS Pro 2.5 with SAC (BAC+PACE) and Active Authentication / ST31G480 C01*. The TOE has only one file system layout, namely the ePassport application. In this configuration the BAC+PACE functionality is enabled. The BAC functionality can be disabled in the post-issuance personalisation phase, resulting in a TOE configuration which only uses the PACE mechanism. This PACE only configuration is subject of the separate evaluation process BSI-DSZ-CC-1073-2019 [14].

**Testing approach**

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.

Real TOE: Completely installed TOEs in their uniquely defined operational state have been used and are therefore considered to be in a proper and known state.

Emulated TOE: Since these tests use data loaded into an emulator the task of the evaluators here is to determine, whether the initial condition of each test is satisfied. Since the configuration management system guarantees that the same initial data is used for the same test every time the state of the emulated card is well defined.

Based on the developer tests, which were partially repeated, the evaluators decided to focus their own independent tests on tests with real cards. For the tests with real cards some test ideas derived from the developer tests under consideration of the described security functionality were developed by the evaluators. Tests using the APDU Interface concerning the correctness of implementation of TSF code were conducted.

Furthermore, the evaluators used fuzz testing to determine the correct implementation of the TOE.

**Testing Results**

All test cases have been conducted successfully and all the actual test results (resulting from evaluator’s repetition of the tests) 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. The repetition of tests showed that 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. All possible attack methods against an authentic operational TOE were analysed.

**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, 7] provided that all measures required by the developer are applied. Potential vulnerabilities cannot be exploited during the phases development, manufacturing and personalisation.

# 8. Evaluated Configuration

This certification covers the following configuration of the TOE: Xaica-α PLUS ePassport on MTCOS Pro 2.5 with SAC (BAC+PACE) and Active Authentication / ST31G480 C01. It consists of:

- STMicroelectronics ST31G480 C01 secure dual-interface controller,
- cryptographic library NesLib 5.2.0,
- 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 2.5 and an application layer, consisting of the ePassport application.

# 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).

*(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) Minimum Requirements for Evaluating Side-Channel Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations*

*(vi) 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 [12, 13],) 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 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-1073-2019, re-use of specific evaluation tasks was possible. In addition to the *Password Authenticated Connection Establishment* and *Active Authentication* functionality addressed in BSI-DSZ-CC-1073-2019, the *Basic Access Control* functionality was taken into account. The TOE itself did not change.

The evaluation has confirmed:

- PP Conformance: None[9]
- for the Functionality: Product specific Security Target
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_DVS.2

The cryptographic algorithms (outlined in table presented in appendix A of the Security Target [6] and [7]) except the post-processing of the PTG.3 random number generator, the cryptographic protocols and the ECC key generation (private key only) are implemented in the ST31G480 C01 secure controller that is part of the TOE. The security evaluation of these cryptographic algorithms was performed in the framework of the certification of the STMicroelectronics ST31G480 C01 secure dual-interface controller (refer to the Certification Report [12] and the corresponding Security Target [15]). The TOE relies on the correct (i.e. standard-conform) and secure implementation of these cryptographic algorithms.

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 and therefore relies on the platform certifications of the used platform (certification ID ANSSI-CC-2017/61) [12, 13].

The composite TOE takes care of the recommendations and requirements imposed by the guidance documentation and ETR for composition of the underlying platform to be resistant against attackers with attack potential enhanced-basic.

### 9.2. Results of cryptographic assessment

The table presented in appendix A of the Security Target [6] and [7] 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. The strength of these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

## 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

[9] Note that the ST [6,7] is based on the Protection Profile “JISEC C0500, version 1.00, Protection Profile for ePassport IC with SAC (BAC+PACE) and Active Authentication, JBMIA, 2016-03-08.” (English translation) [9], which requires strict conformance. For formal reasons no strict conformance to the original Japanese Protection Profile is claimed, because the English translation [9] is not officially certified.

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 [7] 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. Definitions

## 12.1. 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 |
| **ICAO** | International Civil Aviation Organisation |
| **IPA** | Information-Technology Promotion Agency, Japan |
| **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 |
| **SFP** | Security Function Policy |
| **SFR** | Security Functional Requirement |
| **SHA** | Secure Hash Algorithm |
| **SM** | Secure Messaging |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TSF** | TOE Security Functionality |

## 12.2. 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.

# 13. 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[10] 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-1074-2019, Version 1.1, 2018-12-10, Xaica-αPLUS ePassport on MTCOS Pro 2.5 with SAC (BAC+PACE) and Active Authentication / ST31G480 C01, MaskTech International GmbH (confidential document)

[7] Security Target BSI-DSZ-CC-1074-2019, Version 1.3, 2018-12-10, Xaica-αPLUS ePassport on MTCOS Pro 2.5 with SAC (BAC+PACE) and Active Authentication / ST31G480 C01, MaskTech International GmbH (sanitised public document)

[8] Evaluation Technical Report, BSI-DSZ-CC-1074, Version 0.7, 14.12.2018, Evaluation Technical Report (ETR) - Xaica-α PLUS ePassport on MTCOS Pro 2.5 with SAC (BAC+PACE) and Active Authentication / ST31G480 C01, SRC Security Research & Consulting GmbH, (confidential document)

[9] JISEC C0500, version 1.00, Protection Profile for ePassport IC with SAC (BAC+PACE) and Active Authentication, JBMIA, 2016-03-08.

[10] 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 9, 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 38, Version 2, Reuse of evaluation results

[10] Configuration list - Xaica- α PLUS ePassport, Supporting Document - Life Cycle Support, MaskTech International GmbH, Version 0.5, 10.12.2018 (confidential document)

[11] Xaica-α PLUS ePassport – User Guidance, MaskTech International GmbH, Version 1.3, 10.12.2018

[12] Rapport de certification ANSSI-CC-2017/61 – ST31G480 C01 including optional cryptographic library NESLIB and optional technologies MIFARE DESFire EV1 and MIFARE Plus X; Agence nationale de la sécurité des systèmes d'information; 2017-10-05.

[13] ETR lite for Composition, Elixir-2 Project, Certification ID ANSSI-CC-2017/61, TOE ST31G480 C01; Serma Safety & Security; Version 1.0, 21.09.2017

[14] Certification Report BSI-DSZ-CC-1073-2019 for *Xaica-αPLUS ePassport on MTCOS Pro 2.5 with SAC (PACE) and Active Authentication / ST31G480 C01* from MaskTech International GmbH, 25.01.2019, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[15] ST31G480 C01 including optional cryptographic library NESLIB, and optional technologies MIFARE® DESFire® EV1 and MIFARE Plus® X – Security Target for composition; STMicroelectronics; ANSSI-CC-2017/61; 2017-06-23

# 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 detailled 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-1074-2019

## Evaluation results regarding development and production environment

The IT product Xaica-α PLUS ePassport on MTCOS Pro 2.5 with SAC (BAC+PACE) and Active Authentication / ST31G480 C01 (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 25 January 2019, 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 of the TOE 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-2017/61 [12]

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.

Note: End of report