Certification Report

EAL 4+(ALC_DVS.2) Evaluation of

TÜBİTAK BİLGEM UEKAE

AKIS GEZGIN_N v2.0 BAC Configuration and BAP Configuration 1 with Active Authentication

issued by

Turkish Standards Institution

Common Criteria Certification Scheme

Certificate Number: 21.0.03.0.00.00//TSE-CCCS-91

aikiz

TABLE OF CONTENTS

Document Information

Date of Issue	28.02.2024
Approval Date	29.02.2024
Certification Report Number	21.0.03/24-001
Sponsor and Developer	TÜBİTAK BİLGEM UEKAE
Evaluation Facility	TÜBİTAK BİLGEM TDD OKTEM
TOE Name	AKIS GEZGIN_N v2.0 BAC Configuration and BAP Configuration 1 with Active Authentication
Pages	18

Prepared by *(Common Criteria Inspection Expert)*	Merve Hatice KARATAŞ
Prepared by *(Common Criteria Candidate Inspection Expert)*	Almıla Beyza KARAKAPICI a.ikizoglu
Prepared by *(Common Criteria Candidate Inspection Expert)*	Yavuz AVCI Yavuz
Reviewed by *(Reviewer)*	Mehmet Kürşad ÜNAL

The experts whose names and signatures are shown as above prepared and reviewed this report.

Document Change Log

Release	Date	Pages Affected	Remarks/Change Reference
1.0	28.02.2024	All	Initial Release

DISCLAIMER

This certification report and the IT product defined in the associated Common Criteria document has been evaluated at an accredited and licensed evaluation facility conformance to Common Criteria for IT Security Evaluation, version 3.1, revision 5, using Common Methodology for IT Products Evaluation, version 3.1, revision 5. This certification report and the associated Common Criteria document apply only to the identified version and release of the product in its evaluated configuration. Evaluation has been conducted in accordance with the provisions of the CCCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report and its associated Common Criteria document are not an endorsement of the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria

aikiz

document, and no warranty is given for the product by the Turkish Standardization Institution, or any other organization that recognizes or gives effect to this report and its associated Common Criteria document.

FOREWORD

The Certification Report is drawn up to submit the Certification Commission the results and evaluation information upon the completion of a Common Criteria evaluation service performed under the Common Criteria Certification Scheme. Certification Report covers all non-confidential security and technical information related with a Common Criteria evaluation which is made under the ITCD Common Criteria Certification Scheme. This report is issued publicly to and made available to all relevant parties for reference and use.

The Common Criteria Certification Scheme (CCSS) provides an evaluation and certification service to ensure the reliability of Information Security (IS) products. Evaluation and tests are conducted by a public or commercial Common Criteria Evaluation Facility (CCTL = Common Criteria Testing Laboratory) under CCCS' supervision.

CCEF is a facility, licensed as a result of inspections carried out by CCCS for performing tests and evaluations which will be the basis for Common Criteria certification. As a prerequisite for such certification, the CCEF has to fulfill the requirements of the standard ISO/IEC 17025 and should be accredited by accreditation bodies. The evaluation and tests related with the concerned product have been performed by TÜBİTAK BİLGEM TDD OKTEM, which is a public/commercial CCTL.

A Common Criteria Certificate given to a product/PP means that such product/PP meets the security requirements defined in its security target/PP document that has been approved by the CCCS. The Security Target/PP document is where requirements defining the scope of evaluation and test activities are set forth. Along with this certification report, the user of the IT product should also review the security target document in order to understand any assumptions made in the course of evaluations, the environment where the IT product will run, security requirements of the IT product and the level of assurance provided by the product.

This certification report is associated with the Common Criteria Certificate issued by the CCCS for AKIS GEZGIN_N v2.0 BAC Configuration and BAP Configuration 1 with Active Authentication whose evaluation was completed on 18.01.2024 and whose evaluation technical report was drawn up by

aikiz

TÜBİTAK BİLGEM TDD OKTEM (as CCTL), and with the Security Target with version no. 11 of the relevant product.

The certification report, certificate of product evaluation and security target document are posted on the ITCD Certified Products List at bilisim.tse.org.tr portal and the Common Criteria Portal (the official web site of the Common Criteria Project).

RECOGNITION OF THE CERTIFICATE

The Common Criteria Recognition Arrangement logo is printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA.

The CCRA has been signed by Turkey in 2003 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including *EAL2*. The current list of signatory nations and approved certification schemes can be found on:

https://www.commoncriteriaportal.org

1. EXECUTIVE SUMMARY

Developer of the IT product: TÜBİTAK BİLGEM UEKAE
Evaluated IT product: AKIS GEZGIN_N v2.0 BAC Configuration and BAP Configuration 1 with Active Authentication
IT Product Version: v2.0
Name of IT Security Evaluation Facility: TÜBİTAK BİLGEM TDD OKTEM
Completion date of evaluation: 18.01.2024
Assurance Package: EAL 4+ (ALC_DVS.2)

1.1. Brief Description

The TOE is the composition of contactless smartcard IC which is P71D352P of NXP N7121 P71D321 platform, platform crypto library, and the Embedded Operating System (EOS) supporting the electronic Machine Readable Travel Document (eMRTD) application and ISO-compliant Driving Licence (IDL) application.

1.2. Major Security Features

The TOE provides the following security services:

- Protection against modification, probing, environmental stress and emanation attacks,
- Passive Authentication (PA),
- Active Authentication (AA),
- Basic Access Control (BAC),
- Basic Access Protection (BAP),
- Hybrid Deterministic Random Number Generation,
- Signature generation with ISO 9796-2 Digital signature scheme 1,
- Signature generation with ECDSA.

1.3. Threats

The threats are;

- **T.Counterfeit**: An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine travel document's chip to be used as part of a counterfeit travel document. This violates the authenticity of the travel document's chip used for authentication of a traveler by possession of a travel document. The attacker may generate a new data set or extract completely or

aikiz

partially the data from a genuine travel document's chip and copy them on another appropriate chip to imitate this genuine travel document's chip.

- **T.Skimming:** An attacker imitates an inspection system in order to get access to the user data stored on or transferred between the TOE and the inspecting authority connected via the contactless interface of the TOE.
- **T.Tracing:**
  (i) An attacker is listening to the communication between the travel document and the PACE authenticated BIS-PACE in order to gain the user data transferred between the TOE and the terminal connected.
  (ii) An attacker might also be listening to an existing communication between the MRD's chip and an e-Signature terminal to capture the value(s) of PIN(s) used to authenticate for the use of asymmetric private keys to perform e-Signature generation operations.
- **T.Forgery:** An attacker fraudulently alters the User Data or/and TSF-data stored on the eMRD or/and exchanged between the TOE and the terminal connected in order to outsmart the PACE authenticated BIS PACE by means of changed MRD holder's related reference data (like biographic or biometric data). The attacker does it in such a way that the terminal connected perceives these modified data as authentic one.
- **T.Abuse-Func:** An attacker may use functions of the TOE which shall not be used in TOE operational phase in order to:

  (i) manipulate or to disclose the User Data stored in the TOE,

  (ii) manipulate or to disclose the TSF data stored in the TOE or

  (iii) manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.

  This threat addresses the misuse of the functions for the initialization and personalization in the operational phase after delivery to the MRD holder
- **T.Information_Leakage:** An attacker may exploit information which is leaked from the TOE during its usage in order to disclose confidential User Data or/and TSF-data stored on the travel document or/and exchanged between the TOE and the terminal connected.
- **T. Phys-Tamper:** An attacker may perform physical probing of the travel document in order to:

  (i) disclose TSF-data,

  (ii) disclose/reconstruct the travel document's chip Embedded Software.

An attacker may physically modify the travel document in order to alter

(i) its security functionality (hardware and software part, as well)

(ii) the User Data or TSF-data stored on the travel document.

- **T.Malfunction:** An attacker may cause a malfunction of the travel document's hardware and Embedded Software by applying environmental stress in order to

  (i) deactivate or modify security features or functionality of the TOE' hardware

aikiz

(ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software.

- **T. Chip_ID:** An attacker trying to trace the movement of the MRD by identifying remotely the MRD's chip by establishing or listening to communications through the contactless communication interface.

1.4. Organizational Security Policies (OSPs)

Organizational Security Policies are;

- **P.Manufact (Manufacturing of the travel document's chip)**

The Initialization Data are written by the IC Manufacturer to identify the IC uniquely and to provide the keys for the authentication of the travel document Manufacturer. The MRD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

- **P.Personalization (Personalization of the MRD by issuing State or Organization only)**

  The issuing State or Organisation guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical travel document with respect to the travel document holder. The personalization of the travel document for the holder is performed by an agent authorized by the issuing State or Organisation only.

- **P.Personal_Data (Personal Data Protection Policy)**

  The biographical data and their summary printed in the MRZ and stored on MRD's chip, the printed portrait and the digitized portrait, the biometric reference data of finger(s), the biometric reference data of iris image(s) and data according to LDS stored on the MRD's chip are personal data of the MRD holder.

2. CERTIFICATION RESULTS

2.1 Identification of Target of Evaluation

Certificate Number	21.0.03.0.00.00//TSE-CCCS-91
TOE Name and Version	AKIS GEZGIN_N v2.0 BAC Configuration and BAP Configuration 1 with Active Authentication
Security Target Title	Security Target of AKIS GEZGIN_N v2.0 BAC Configuration and BAP Configuration 1 with Active Authentication
Security Target Version	11
Security Target Date	16.01.2024
Assurance Level	EAL 4+(ALC_DVS.2)
Criteria	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017
Methodology	Common Criteria for Information Technology Security Evaluation, Evaluation Methodology; CCMB-2017-04-004, Version 3.1, Revision 5, April 2017
Protection Profile Conformance	None
Common Criteria Conformance	• Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017 • Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components;

	CCMB-2017-04-002, Version 3.1, Revision 5, April 2017, extended • Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017, conformant
Platform	NXP N7121 P71D321, NXP Technologies
Security Target Title of the Platform Hardware	NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4), Security Target Lite
Security Target Version and Date of the Platform Hardware	Version 2.6, *June 13th* 2022
Protection Profile Conformance of the Platform Hardware	Security IC Platform Protection Profile with Augmentation Packages, Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014
Sponsor and Developer	TÜBİTAK BİLGEM UEKAE
Evaluation Facility	TÜBİTAK BİLGEM TDD OKTEM
Certification Scheme	TSE CCCS

2.2 Security Policy

Organizational Security Policies are;

- **P.Manufact (Manufacturing of the travel document's chip)**

  The Initialization Data are written by the IC Manufacturer to identify the IC uniquely and to provide the keys for the authentication of the travel document Manufacturer. The MRD Manufacturer writes the Pre-personalization Data which contains at least the Personalization Agent Key.

- **P.Personalization (Personalization of the MRD by issuing State or Organization only)**

  The issuing State or Organisation guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical travel

aikiz

document with respect to the travel document holder. The personalization of the travel document for the holder is performed by an agent authorized by the issuing State or Organisation only.

- **P.Personal_Data (Personal Data Protection Policy)**

The biographical data and their summary printed in the MRZ and stored on MRD's chip, the printed portrait and the digitized portrait, the biometric reference data of finger(s), the biometric reference data of iris image(s) and data according to LDS stored on the MRD's chip are personal data of the MRD holder.

2.3 Assumptions and Clarification of Scope

Assumptions for the operational environment of the TOE are;

- **A.MRD_Manufact (MRD manufacturing on steps 4 to 6)**

It is assumed that appropriate functionality testing of the MRD is used. It is assumed that security procedures are used during all manufacturing and test operations to maintain confidentiality and integrity of the MRD and of the manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorized use).

- **A.MRD_Delivery (Delivery of the MRD during steps 4 to 6)**

Procedures shall guarantee the control of the TOE delivery and storage process and conformance to its objectives:

  - Procedures shall ensure protection of TOE material/information under delivery and storage.
  - Procedures shall ensure that corrective actions are taken in case of improper operation in the delivery process and storage.
  - Procedures shall ensure that people dealing with the procedure for delivery have got the required skill.

- **A.Pers_Agent (Personalization of the MRD's chip)**

The Personalization Agent ensures the correctness of:

i. the logical MRD with respect to the MRD holder,
ii. the Document Basic Access Keys,
iii. the Chip Authentication Public Key (EF.DG14) if stored on the MRD's chip,
iv. and the Document Signer Public Key Certificate (if stored on the MRD's chip).

aikiz

- **A.Insp_Sys (Inspection Systems for global interoperability)**

  The Inspection System is used by the control officer of the receiving State or Organization for eMRD:

  i. examining an MRD presented by the user and verifying its authenticity,

  ii. and verifying the traveller as the MRD holder.

- **A.BAC-Keys (Cryptographic quality of BAC/BAP Keys)**

  The Document BAC/BAP Keys being generated and imported by the issuing State or Organization have to provide sufficient cryptographic strength.

- **A.Pers_Agent_AA(Cryptographic quality of asymmetric keys used for e-Signature generation)**

  The Personalization Agent ensures the correctness of the Active Authentication Public Key (EF.DG15 for eMRTD and EF.DG13 for IDL) if stored on the MRD's chip. The Personalization Agent bears the Personalization Agent Authentication to authenticate himself to the TOE by mechanisms mentioned in A.Pers_Agent.

- **A.Insp_Sys_AA (Inspection Systems for global interoperability with Active Authentication)**

  The Inspection System may also implement the terminal part of the Active Authentication Protocol if it wants to ensure the TOE is not cloned.

2.4 Architectural Information

TOE will be in form of a paper book or plastic card with an embedded chip and possibly an antenna. It presents visual readable data including (but not limited to) personal data of the MRTD holder:

- The biographical data on the biographical data page of the passport book/card,
- The printed data in the Machine-Readable Zone (MRZ) that identifies the MRTD and
- The printed portrait.

For further information see ST.

2.5 Documentation

Documents below are provided to the customer by the developer alongside the TOE;

Name of Document	Version Number	Date

Security Target Lite of AKIS GEZGIN_N v2.0 BAC Configuration and BAP Configuration 1 with Active Authentication	V1	16.02.2024
AKIS GEZGIN_N v2.0 Yönetici ve Kullanıcı Kılavuzu	V7	16.01.2024
AKIS GEZGIN_N v2.0 Kişiselleştirme Kılavuzu	V5	13.12.2023
AKIS GEZGIN_N v2.0 BAC Configuration and BAP Configuration 1 with Active Authentication Teslim ve İşletim Dokümanı	V2	08.08.2023

2.6 IT Product Testing

IT Product Testing is mainly described in two parts:

2.6.1 Developer Testing

Developer has prepared TOE Test Document according to the TOE Functional Specification documentation, TOE Design documentation which includes TSF subsystems and its interactions. All SFR-Enforcing TSFIs have been tested by developer. Developer has conducted 117 functional tests in total.

2.6.2 Evaluator Testing

- **Independent Testing:** Evaluator has chosen 27 developer tests to conduct by itself. Additionally, evaluator has prepared 23 independent tests. TOE has passed all 50 functional tests to demonstrate that its security functions work as it is defined in the ST.
- **Penetration Testing**: TOE has been tested against common threats and other threats surfaced by vulnerability analysis. As a result, 24 penetration tests have been conducted.

2.7 Evaluated Configuration

The evaluated TOE configuration is composed of;

- the IC Embedded Software including operating system and eMRTD application (AKIS GEZGIN_N v2.0 BAC Configuration and BAP Configuration 1with Active Authentication),
- Secure IC (NXP Technologies, N7121 P71D321),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- Guidance documents
- Activation data

aikiz

2.8 Results of the Evaluation

The table below provides a complete listing of the Security Assurance Requirements for the TOE. These requirements consists of the Evaluation Assurance Level 4 (EAL 4) components as specified in Part 3 of the Common Criteria, augmented with ALC_DVS.2.

Assurance Class	Component	Component Title	Result
ADV: Development	ADV_ARC.1	Security Architecture Description	PASS
	ADV_FSP.4	Complete Functional Specification	PASS
	ADV_IMP.1	Implementation representation of the TSF	PASS
	ADV_INT.2	Well-structured internals	PASS
	ADV_TDS.3	Basic Modular Design	PASS
	ADV_COMP.1	Design Compliance with the Platform Certification Report, Guidance and ETR_COMP	PASS
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance	PASS
	AGD_PRE.1	Preparative Procedures	PASS
ALC: Life-Cycle Support	ALC_CMC.4	Production Support, Acceptance Procedures and automation	PASS
	ALC_CMS.4	Problem tracking CM coverage	PASS
	ALC_DEL.1	Delivery Procedures	PASS
	ALC_DVS.2	Sufficiency of security measures	PASS
	ALC_LCD.1	Developer defined life-cycle model	PASS
	ALC_TAT.2	Compliance with implementation standards	PASS
	ALC_COMP.1	Integration of the Application into the Underlying Platform and Consistency Check for Delivery And Acceptance Procedures	PASS
ASE: Security Target Evaluation	ASE_CCL.1	Conformance Claims	PASS
	ASE_ECD.1	Extended Components Definition	PASS

	ASE_INT.1	ST Introduction	PASS
	ASE_OBJ.2	Security Objectives	PASS
	ASE_REQ.2	Derived Security Requirements	PASS
	ASE_SPD.1	Security Problem Definition	PASS
	ASE_TSS.1	TOE Summary Specification	PASS
	ASE_COMP.1	Consistency of Security Target Objectives	PASS
ATE: Tests	ATE_COV.2	Analysis of Coverage	PASS
	ATE_DPT.1	Testing: Basic Design	PASS
	ATE_FUN.1	Functional Testing	PASS
	ATE_IND.2	Independent Testing - Sample	PASS
	ATE_COMP.1	Composite Functional Testing	PASS
AVA: Vulnerability Analysis	AVA_VAN.3	Focused Vulnerability Analysis	PASS
	AVA_COMP.1	Composite Product Vulnerability Assessment	PASS

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL 4+ (ALC_DVS.2) assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer about the issues requiring resolution or clarification within the evaluation evidence. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. So for TOE "AKIS GEZGIN_N v2.0 BAC Configuration and BAP Configuration 1 with Active Authentication", the results of the assessment of all evaluation tasks are "Pass".

2.9 Evaluator Comments / Recommendations

It is recommended that all guidance outlined in the Guidance Documents be followed and all assumptions are fulfilled in order to secure usage of the TOE.

3. SECURITY TARGET

The Security Target associated with this Certification Report is identified by the following terminology:

Title: Security Target of AKIS GEZGIN_N v2.0 BAC Configuration and BAP Configuration 1 with Active Authentication

aikiz

Version: 11

Date of Document: 16.01.2024

A public version has been created and verified according to ST-Sanitizing:

Title: Security Target Lite of AKIS GEZGIN_N v2.0 BAC Configuration and BAP Configuration 1with Active Authentication

Version: 01

Date of Document: 16.02.2024

4. GLOSSARY

AA : Active Authentication

ADV : Assurance of Development

AES : Advanced Encryption Standard

AGD : Assurance of Guidance Documents

ALC : Assurance of Life Cycle

ASE : Assurance of Security Target Evaluation

ATE : Assurance of Tests Evaluation

AVA : Assurance of Vulnerability Analysis

BAC : Basic Access Control

BAP : Basic Access Protection

BİLGEM : Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi

CC : Common Criteria (Ortak Kriterler)

CCCS : Common Criteria Certification Scheme (TSE)

CCRA : Common Criteria Recognition Arrangement

CCTL : Common Criteria Test Laboratory

CEM : Common Evaluation Methodology

CMC : Configuration Management Capability

aikiz

CMS : Configuration Management Scope

DEL : Delivery

DES : Data Encryption Standard

DF : Dedicated File

DVS : Development Security

EAC : Extended Access Control

EAL : Evaluation Assurance Level

EF : Elementary File

ICAO : International Civil Aviation Organization

MAC : Message Authentication Code

MRTD: Machine Readable Travel Document

OKTEM : Ortak Kriterler Test Merkezi

OPE : Operational User Guidance

OSP : Organizational Security Policy

PP : Protection Profile

PRE : Preparative Procedures

PP : Protection Profile

SAC : Supplemental Access Control

SAR : Security Assurance Requirements

SFR : Security Functional Requirements

ST : Security Target

TDD: Test ve Değerlendirme Direktörlüğü

TOE : Target of Evaluation

TSF : TOE Secirity Functionality

TSFI : TSF Interface

TUBİTAK : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

UEKAE : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

5. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017

[2] Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017

[3] Composite Product Evaluation for Smart Cards and Similar Devices, v1.5.1, May 2018

[4] Application of Attack Potential to Smartcards, v3.2, November 2022

[5] DTR 96 TR 01 AKIS GEZGIN_N v2.0 BAC Configuration and BAP Configuration 1 with Active Authentication EAL 4+ (ALC_DVS.2, AVA_VAN.5) Evaluation Technical Report, Rev1.0, 18 January 2024

[6] 1136-V3_ETR-COMP_220825_v2, ETR for Composite Evaluation V2: N7121 B1, NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) B1, v2, 25 August 2022

[7] Common Criteria Protection Profile Machine Readable Travel Document with ICAO Application, Extended Access control, BSI-PP-0056-V2-2012, version 1.3.2, 5 December 2012

[8] Security IC Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, version 1.0, 19 February 2014

[9] ICAO Doc 9303, Machine Readable Travel Documents, Part 1 – Machine Readable Travel Passports, Sixth Edition, 2006, ICAO

[10] Technical Guideline TR-03110-3 Advanced Security Mechanisms for Machine Readable Travel Documents, Part 3: Common Specifications, Version 2.10, 10 March 2012

[11] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) Security Target Lite, NXP Semiconductors, rev. 2.6, 13 June 2022

[12] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) from NXP Semiconductors Germany GmbH, BSI-DSZ-CC-1136-V3-2022, v3, 2022

[13] Assurance Continuity Maintenance Report, NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) from NXP Semiconductors Germany GmbH, BSI-DSZ-CC-1136-V3-2022-MA-01, v3, 2022

[14] NXP Secure Smart Card Controller N7121 Information on Guidance and Operation, rev.3.2, 28 May 2019

[15] SmartMX3 Family N7121 Wafer and Delivery Specification, rev. 3.3, 3 November 2021

[16] N7121 Crypto Library Information on Guidance and Operation, rev.3.4, 4 May 2022

[17] N7121 Crypto Library Errata sheet, rev.1.0, 2 February 2023

[18] N7121 Crypto Library ECC over GF(p) Library, rev.2.3, 4 May 2022

6. ANNEXES

There is no additional information which is inappropriate for reference in other sections.

aikiz