MASKTECH

MTCOS® PRODUCT BRIEF

MTCOS 2.5 on ST31G480 | Version 1.2

MTCOS 2.5

Confidential

MaskTech GmbH | Nordostpark 45 | Nuernberg | www.masktech.com | +49 (0)911 95 51 49-0

Introduction

MTCOS Pro is a fully interoperable multi-application smart card operating system compliant to ISO/IEC 7816 [1]. It provides public and secret key cryptography and supports a variety of security-sensitive applications like

Travel Documents ICAO application compliant to ICAO Doc 9303 and TR-03110 [2, 3]

National ID ICAO application complemented by digital signature, certificates and strong PKI authentication for eGovernment usage

Health Care supporting modern health infrastructures, e.g. by Card-to-Card authentication

Driving License compliant to ISO/IEC 18013-3 [4]

Payment including Secure-Authentication-Module support

Residence Permit compliant to the EU Council Regulation Standards

Customized Applications for tailor-made solutions, e.g. for public transport

To meet the requirements of evolving regulations and standards as well as to counter the continuously increasing potential of attackers, MTCOS Pro undergoes a proactive and ongoing software development. Furthermore, the operating system implementation is a made-to-measure product on the ST31G480 chip in order to exploit the hardware functionality as best as possible. MTCOS 2.5 on ST31G480 has been developed with continuous feedback from STMicroelectronics.

This document gives an overview over the supported features, security mechanisms and relevant technical details of MTCOS 2.5 / ST31G480. For detailed information an extensive **MTCOS product manual** is provided, please contact MaskTech for further support (note that a *Non-Disclosure Agreement* is required to obtain the documentation).

Common Criteria Certification

MTCOS 2.5 / ST31G480 is subject to the following procedures (EAC: EAL5+, BAC: EAL4+):

Compliant to protection profile	Certification-ID	Certification date
BSI-CC-PP-0056-V2-2012 (incl. BSI-CC-PP-0068-V2-2011)	BSI-DSZ-CC-1064	expected Q3/2020
BSI-CC-PP-0055-2009	BSI-DSZ-CC-1065	expected Q3/2020

Application Features

Authentication Mechanisms as used for *ePassports*, *eDriving Licenses* and other access control applications:

Basic Access Control according to [2]

Basic Access Protection (configurations 1 - 4) as used for eDLs according to [4]

Password Authenticated Connection Establishment (PACEv2) according to [3, 5] using ECDH for key agreement

- with Generic Mapping (GM) and Chip Authentication Mapping (CAM)
- including PIN and PUK user authentication »New Feature in MTCOS Pro 2.5«

Extended Access Control (EACv1) [3] including

- Chip Authentication (DH with key lengths up to 2048 bits and ECDH for key agreement with all supported curves and key sizes)
- Terminal Authentication using RSA with key lengths up to 3072 bit and ECDSA with all supported curves and key sizes

Extended Access Protection for eDLs according to [4]

Card-to-Card Authentication as used for *eHealth* applications according to [6] using RSA with key lengths up to 2048 bits

Active Authentication according to [2] or [4] for eDL, respectively

- using RSA with key lengths up to 3072 bit
- ECDSA with all supported curves and key sizes

Hashed One-Time-Password (HOTP) as specified in [7] »New Feature in MTCOS Pro 2.5«

Digital Signature as used for *Secure Signature Creation Devices* (SSCD), *eHealth Cards* or *eCitizen Cards* supporting:

RSA as specified in [8] with key lengths up to 3072 bit

ECDSA as specified in [9] with all supported curves and key sizes

Key- and PIN-Management a number of security features and configuration possibilities enhance the protection level of secret files:

- **Usage limit** for key files and for session keys »New Feature in MTCOS Pro 2.5«
- **Minimum length** for passwords
- **Reset limit** for the retry counter of key and password files
- **Failed authentication delay** for non-blocking secrets
- **Suspended-state support** for PACE-PIN and PACE-PUK »New Feature in MTCOS Pro 2.5«

Miscellaneous Further applications are available:

- **ePurse** for *ePayment* according to [10]
- **1Purse** MaskTech proprietary *ePayment* solution
- **Global Platform** SCP02 for key transfer

Security Features

Hardware Functionality The platform ST31G480 is certified according to Common Criteria with an assurance level of EAL5 augmented (certification ID: ANSSI-CC-2019/12).

- Active Shield
- Monitoring of environmental parameter
- Three-key Triple DES accelerator
- AES accelerator
- AIS-31 Class PTG.2 compliant true random number generator (TRNG)
- NESCRYPT coprocessor for public key cryptography algorithm
- ISO/IEC 13239 CRC calculation block
- Jamming smoothing current regulator (JSCR)
- Watchdog timer (WDT)
- Clock random jitter
- ARM® SecurCore® SC000 memory protection unit (MPU)
- Library Protection Unit (LPU)
- Memory scrambling and encrypting
- Error Detection Code (EDC) mechanism
- Data bus encryption

Software Functionality

- AIS-31 Class PTG.2 compliant random number generator
- Flow control against manipulation
- Transport key protection

Technical Details

Communication and File System Features

Communication	
Interfaces	Contact based (T=1) according to [11]
	Contactless type A and B according to [12]
APDU	Supporting extended APDUs up to 64 kbytes
	Buffer size up to 2039 bytes
Memory	
NVM size (available for file system)	Up to 188 kbytes
Miscellaneous	
	VHBR support

Cryptography

Symmetric	
DES/3DES	ECB or CBC mode with CBC-MAC (Retail-MAC) or CMAC
AES-128, -192, -256	ECB or CBC mode with CBC-MAC or CMAC
Asymmetric	
EC (ECDH, ECDSA)	Key generation is supported
	Supported EC-curves: Brainpool P160r1, Brainpool P192r1, Brainpool P224r1, Brainpool P256r1, Brainpool P320r1, Brainpool P384r1, Brainpool P512r1, NISTP192 (SEC P192r1), NISTP224 (SEC P224r1), NISTP256 (SEC P256r1), NISTP384 (SEC P384r1), NISTP521 (SEC P521r1)
RSA	Key generation is supported
	Private key operations (CRT) with a maximum key length of 3072 bits
	Public key operations with a maximum key length of 3072 bits
DH	Maximum key length of 2048 bits
Hash functions	
	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512

Bibliography

[1] ISO/IEC 7816, ISO/IEC, Identification cards – Integrated circuit cards – Multipart Standard, International Organization for Standardization; International Electrotechnical Commission, 2008.

[2] ICAO Doc 9303, ICAO, Machine Readable Travel Documents, International Civil Aviation Organization, 2015.

[3] TR-03110, BSI, Advanced Security Mechanisms for Machine Readable Travel Documents, Bundesamt für Sicherheit in der Informationstechnik, 2015. Version 2.20.

[4] ISO/IEC 18013-3:2017, ISO/IEC, Information technology – Personal identification – ISO-compliant driving license – Part 3: Access control, authentication and integrity validation, International Organization for Standardization; International Electrotechnical Commission, 2017-04.

[5] ICAO, Technical Report: Supplemental Access Control for Machine Readable Travel Documents, International Civil Aviation Organization, 2014-04-15. TR-SAC V1.1.

[6] 1.4ech, Santésuisse, Versichertenkarte – Detailspezifikationen Version 1.4ech, 2010-08-09.

[7] RFC 4226, D. M'Raihi, D. and Bellare, M. and Hoornaert, F. and Naccache. D. and Ranen, O., HOTP: An HMAC-Based One-Time Password Algorithm, Internet Engineering Task Force, 2005.

[8] PKCS#1 v2.2, RSA Cryptography Standard, RSA Laboratories, 2012-10-27.

[9] ANSI X9.62-2005, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standards Institute, 2005-11-16.

[10] EN 726:1994, 1995, 1999, CEN, Identification Card Systems - Telecommunications Integrated Circuits Cards and Terminals - Multipart standard, European Commitee for Standardization, 1994, 1995, 1999.

[11] ISO/IEC 7816-3:2006, ISO/IEC, Identification cards – Integrated circuit cards – Part 3: Cards with contacts – Electrical interface and transmission protocols, International Organization for Standardization; International Electrotechnical Commission, 2006-10.

[12] ISO/IEC 14443, ISO/IEC, Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Multipart Standard, International Organization for Standardization; International Electrotechnical Commission, 2016-2018.

Revision History

Revision	Date	Changes
1.0	2018-06-18	First version
1.1	2018-11-19	Updated version
1.2	2020-07-02	Updated version

Contact

MaskTech GmbH – **Headquarters**

Nordostpark 45	Phone	+49 911 955149 0
D-90411 Nuernberg	Fax	+49 911 955149 7
Germany	Email	info@masktech.de

MaskTech GmbH – **Support**

Bahnhofstr. 13	Phone	+49 911 955149 0
D-87435 Kempten	Fax	+49 831 5121077 1
Germany	Email	support@masktech.de

MaskTech GmbH – **Sales**

Lauenburger Str. 15	Phone	+49 4151 8990858
D-21493 Schwarzenbek	Fax	+49 4151 8995462
Germany	Email	stimm@masktech.de

Grażyna Renata Rafalska

Elektronicznie podpisany przez Grażyna Renata Rafalska
Data: 2022.02.28 09:24:19 +01'00'