life.augmented

STeID-MT2.5

Data brief

STeID MTCOS® 2.5 - secure native solutions for electronic ID and travel documents

Product status link
STeID-MT2.5

Features

Software

- Native MTCOS® operating system from Masktech GmbH
- Up to 144 Kbyte user memory
- Basic access control (BAC)
- Extended access control (EAC)
- Supplemental access control (SAC) / password authenticated connection establishment (PACE)
- Digital signature
- Key- and PIN-management
- Common criteria certified

Hardware

- ST31 flash product family
- Dual Core 32-bit Arm® SecurCore® SC000™
- Lockstep
- Memory protection unit (MPU)
- RSA coprocessor, AES and DES accelerators
- AIS-31 class PTG.2 compliant true random number generator (TRNG)
- Memory scrambling and encrypting
- Active shield
- Best-in-class RF performance
- Common criteria certified

Certification

- ST31 IC: CC EAL 5+ High, BSI-CC-PP-0084
- BAC: CC EAL 4+ High, BSI-CC-PP 55
- EAC, SAC/PACE: CC EAL 5+ High, BSI-CC-PP 56v2

Application

- ePassport
- National eID
- eResidence Permit
- eHealthcare
- eDriving License (eDL)

Compliance to standards

- ISO/IEC 7816
- ICAO Doc 9303, BSI TR-03110
- ISO/IEC 18013-3 (eDL)

Description

The STeID MTCOS® 2.5 is a secure smartcard and operating system featuring advanced public key authentication. Fully interoperable with ICAO-based systems, STeID MTCOS® 2.5 enables a wide range of security-sensitive applications, including electronic identification cards, travel documents, and authentication solutions:

- **Travel documents** ICAO application compliant to ICAO Doc 9303 and TR-03110
- **National ID** ICAO application complemented by digital signature, certificates, and strong PKI authentication for eGovernment usage
- **Health care** supporting modern health infrastructures, such as Card-to-Card authentication
- **Residence permit** compliant to the EU council regulation standards
- **Driving license** compliant to ISO/IEC 18013-3:2017
- **Customized applications** for tailor-made solutions, such as for public transport

STeID family

The STeID MTCOS® 2.5 is part of the STeID family. To offer unparalleled levels of security and performance, the family is based on the ST31 secure microcontroller, which features a dual-core 32-bit Arm® SecurCore® SC000™ (lockstep architecture). Its secure flash memory brings more flexibility to the supply chain and reduces time to market. The family enables long-lasting identity documents (10+ years) thanks to its non-volatile memory endurance (500,000+ cycles) and data retention (25+ years).

The STeID MTCOS® 2.5 has been developed in close cooperation with Masktech GmbH. The solution leverages the ST31 secure microcontroller family combined with an optimized implementation of the MTCOS® software

1 General information

The ST31 secure microcontrollers are based on Arm® SecurCore® .

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

MTCOS® is a registered trademark of Masktech GmbH

Masktech is an independent German supplier for highest security embedded chipsets, operating systems for electronic identification cards, travel documents and authentication solutions. The company supplies more than 30 major passport manufacturers and system integrators and holds a leading position in all its primary product categories. The MTCOS® solutions are used in more than 65 countries worldwide.

2 Application features

Authentication mechanisms as used for ePassports, eDriving License (eDL)s and other access control applications:

- **Basic access control** according to ICAO Doc 9303
- **Basic access protection** (configurations 1 - 4) as used for eDLs according to ISO/IEC 18013-3:2017
- **Password authenticated connection establishment** (PACEv2) according to ICAO and TR-03110 using ECDH for key agreement:
  - with generic mapping (GM) and chip authentication mapping (CAM)
  - including PIN and PUK user authentication.
- **Extended access control** (EACv1) according to TR-03110 including:
  - Chip authentication (DH with:
    - a key lengths up to 2048 bits
    - ECDH for key agreement with all supported curves and key sizes).
  - Terminal authentication using RSA with:
    - a key lengths up to 3072 bits
    - ECDSA with all supported curves and key sizes.
- **Extended access protection** for eDLs according to ISO/IEC 18013-3:2017
- **Card-to-Card authentication** as used for eHealth applications using RSA with key lengths up to 2048 bits
- **Active authentication** according to ICAO Doc 9303 or ISO/IEC 18013-3:2017 for eDL, respectively:
  - using RSA with key lengths up to 3072 bits
  - ECDSA with all supported curves and key sizes.
- **Hashed one-time-password** (HOTP).

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

- **RSA** with key lengths up to 3072 bits
- **ECDSA** with all supported curves and key sizes.

Key- and PIN-management with several security features and configuration possibilities enhancing the protection level of secret files:

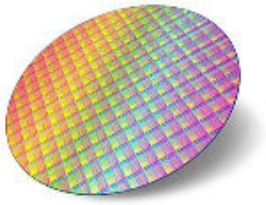
- **Usage limit** for key files and for session keys
- **Minimum length** for passwords
- **Reset limit** for the retry counter of key and password files
- **Failed authentication delay** for nonblocking secrets
- **Suspended-state support** for PACE-PIN and PACE-PUK

GlobalPlatform® SCP02 for key transfer.

3 Delivery forms

The product is available for delivery in several formats as detailed below:

- Wafer



- Contactless micromodule

- Contact and dual interface micromodule (8-pins and 6-pins)

8 pin interface

6 pin interface

Appendix A

A.1 Glossary

This section lists all the terms that are used in this document.

Table 1. Glossary

Term	Description
AES	Advanced encryption standard
BAC	Basic access control
DES	Data encryption standard
DH	Diffie-Hellman
EAC	Extended access control
ECDH	Elliptic curve Diffie–Hellman
ECDSA	Elliptic curve digital signature algorithm
GM	Generic mapping
HOTP	HASH one time password
ICAO	International Civil Aviation Organization
MPU	Memory protection unit
OS	Operating system
PACE	Password authenticated connection establishment
PIN	Personal identification number
PUK	PIN unlock key
RSA	Ron Rivest, Adi Shamir and Leonard Adleman Public-key cryptosystem
SAC	Supplemental access control
SSCD	Secure signature creation device
TRNG	True random number generator

A.2 ISO and ICAO references documents

- ISO/IEC 7816, ISO/IEC, Identification cards – Integrated circuit cards – Multipart Standard, International Organization for Standardization; International Electrotechnical Commission, 2008.
- ICAO Doc 9303, ICAO, Machine Readable Travel Documents, International Civil Aviation Organization, 2015.
- TR-03110, BSI, Advanced Security Mechanisms for Machine Readable Travel Documents, Bundesamt für Sicherheit in der Informationstechnik, 2015. Version 2.20.
- ISO/IEC 18013-3:2017, ISO/IEC, Information technology – Personal identification – ISOcompliant driving license – Part 3: Access control, authentication and integrity validation, International Organization for Standardization; International Electrotechnical Commission, 2017-04.
- ICAO, Technical Report: Supplemental Access Control for Machine Readable Travel

Revision history

Table 2. **Document revision history**

Date	Revision	Changes
23-Nov-2022	1	Initial release.
29-Nov-2022	2	Updated the Description

Contents

List of tables