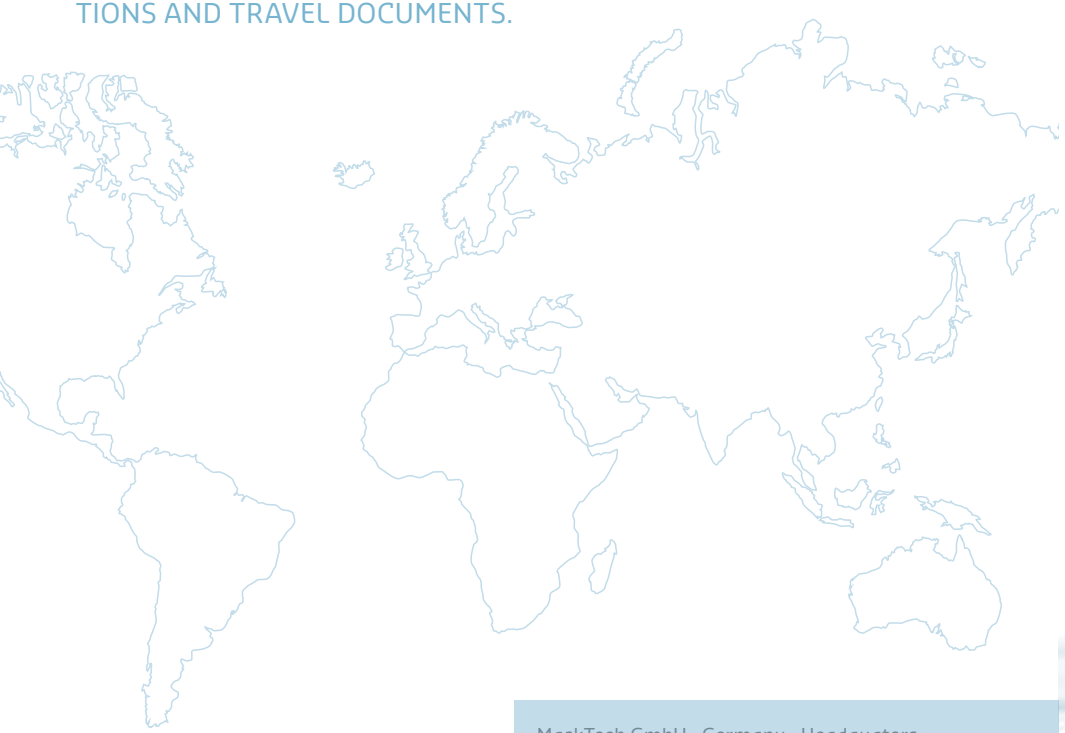
SECURITY SOFTWARE – CERTIFIED AND MADE IN GERMANY.

MASKTECH IS THE LEADING INDEPENDENT SUPPLIER OF OPERATING SYSTEMS FOR SMARTCARD ICS USED IN IDENTIFICATION APPLICATIONS AND TRAVEL DOCUMENTS.



MTCOS®V2.6 & V2.5 PROFESSIONAL

Short Form Specification

Electronic Passport | Electronic National ID | Health Card | Electronic Driving License | Electronic Payment | Electronic Residence Permit

Performance and security for smart cards with extended memory and processing capabilities. MTCOS®v2.6 PROFESSIONAL powers ROM and Flash based Common Criteria EAL6+ certified security chips used in eID documents, electronic authentication and health care solutions. The OS supports the latest security standards and is proven on multible chip platforms from different hardware manufacturers. All applications are built-in and can be activated on demand. MTCOS® has been licensed to eID and travel document projects in over 65 countries worldwide.

MaskTech GmbH · Germany · Headquaters
Nordostpark 45 · 90411 Nuernberg · Germany
Phone +49 911-955149-0 · Fax +49 911-955149-7
info@masktech.de

MaskTech GmbH · Germany · Support
Bahnhofstrasse 13 · 87435 Kempten · Germany
Phone +49 911 9551 490 · Fax +49 831 51 21 07 71
support@masktech.de

Visit us: www.masktech.de

MaskTech GmbH , Rev. 3.0, March 2024

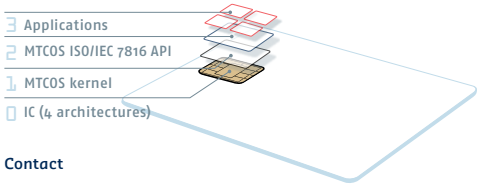
MTCOS®V2.6 & V2.5 PROFESSIONAL

SHORT FORM SPECIFICATION

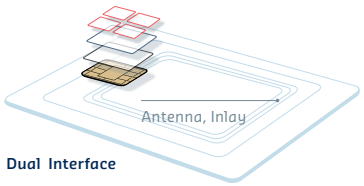
MASKTECH

TECHNOLOGY

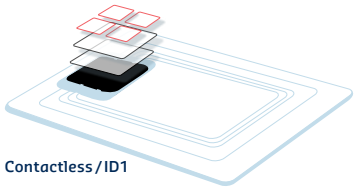
MTCOS® supports cryptographic smartcards with contact based, dual and contactless interface.

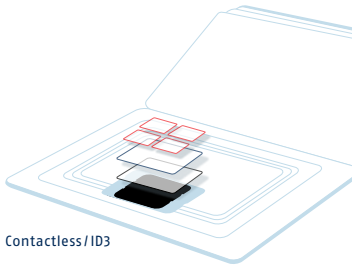


Contact



Dual Interface


Contactless / ID1


Contactless / ID3

APPLICATIONS	MTCOS® ePASSPORT	MTCOS® eID	MTCOS® eRESIDENCE PERMIT	MTCOS® eDRIVING LICENSE	MTCOS® ePAYMENT	MTCOS® eHEALTH	CUSTOMIZED APPLICATIONS
DESCRIPTION	Worldwide first and today the most popular operating system for ePassports. Security features can be combined or used stand-alone for maximum flexibility and interoperability. Supports of various crypto setups and crypto migration.	ICAO application for holder ID data complemented by eGovernment applications such as signature, certificates, strong PKI authentication and multiapplication features.	MTCOS® offers full compliance to the EU and international eResidence Permit standards.	MTCOS® eDL application supports all access and protection protocols according to t he internal standard ISO/IEC 18013 and the latest EU regulations. Like in all our applications the security features can be combined or used stand-alone.	Our ePurse application supports a unique and extremely simple to use one command payment transaction. This significantly decreases the payment transaction times for contactless applications and reduces the overall product complexity to a minimum.	Secure storage of personal patient data in the IC secure memory offers a maximum of data privacy in modern health infrastructures.	Additional applications can easily be added by the card issuer or delegated respectively. Installed applications can access a large set of OS functions, data handling procedures and crypto protocols embedded in MTCOS® masks without additional code development.
APPLICATION FEATURES	• DOC9303 & BSI TR03110 • Support of all DGs • Passive Authentication (PA) • Basic Access Control (BAC) • Active Authentication (AA) • Extended Access Control (EAC) • Supplemental Access Control (SAC) / PACE	• DOC9303 and BSI TR03110 (PA, BAC, AA, EAC, SAC/PACE) • Digital Signature (CEN 14890, PKCS#15, SSCD) • PKI and SKI authentication • PIN/PUK (user) authentication • ISO/IEC Multi-application (pre- and post issuance) Optional: • MINEX II / Match-on-Card	• DOC9303 and BSI TR03110 • Passive Authentication (PA) • Basic Access Control (BAC) • Active Authentication (AA) • Extended Access Control (EAC) • Supplemental Access Control (PACE / SAC) • Various crypto setups	• ISO/IEC 18013-2,3,4 • Support of all DGs • Passive Authentication • Basic Access Protection • Active Authentication • Extended Access Control / Extended Access Protection[1] • Supplemental Access Control (SAC) / PACE	• Single command transaction • SAM support • Transaction counters for the ePurse and SAM • Transaction receipt • Two certificate keys • Key derivation with the SAM • Increase / decrease limits • AES and 3DES support	• Trusted Medic • Card2Card health professional/patient authentication • Digital Signature (CEN 14890, PKCS#15, SSCD) • Copy protection • Emergency data • ISO/IEC 21549	• ISO/IEC 7816 application directories and application specific files, keys and PINs Optional: • Executables • PlugIns using MTCOS® sandbox technology
CHIP TECHNOLOGY	• IFX SLE78 Flash & SLC37 series • NXP P71D352 • ST Microelectronics ST31 Series	• 36k ... 160k[1] user EEPROM • up to 20 years EEPROM data retention[1]	• 8, 16, 32 Bit CPUs[1] • DES, AES, PKI crypto engines • DPA,SPA,EPA,UV,IR resistance[1]	• True random number generator • Active shield, V, F, T, C sensors[1]	• ISO/IEC 7816-3 contact • ISO/IEC 14443 contactless • Unique chip ID	• Hardware MMU • MIFARE Classic or DESFIRE emulation[1]	• EAL6+ certified • Customized ROM masks and FLASH products

COMMON FEATURES

COMMUNICATION
- ISO/IEC 7816 contact based
- ISO/IEC 14443 contactless
- Extended APDUs
- Secure messaging (CEN 14890)

OS CHARACTERISTICS
- Highest performance through direct code processing
- CC security design

DATA HANDLING
- ISO/IEC 7816-4 ... 9, 15
- Transactions
- File sizes up to 4GB
- Individual file access rights
- Dynamic file size configuration at personalisation stage

LIFE CYCLES
- 4-stage life cycle manager
- ISO/IEC 7816 file life cycles

SECURITY
- PIN/PUK, Trusted PIN
- PACE: CAM, suspended-state
- Various authentication schemes
- Random numbers
- Random UID / PUPI
- Strong resistance against DPA,DFA, SPA, EPA, UV, IR attacks
- RSA and EC key generation

CRYPTOGRAPHY
- DES & 3DES
- AES
- SHA 1 & 2
- RSA up to 4096 Bit
- Elliptic Curve up to 521 Bit

MEMORY
- up to 160k Bytes[1]

DELIVERY TYPES
- Wafer
- Contactless module
- Contact module
- Dual interface module

SECURITY ACCREDITATIONS
EAL6+ / ISO 15408

TOOLS
- Smart Platform scripting & file system tool
- MTCOS® MANAGER

[1] depends on semiconductor