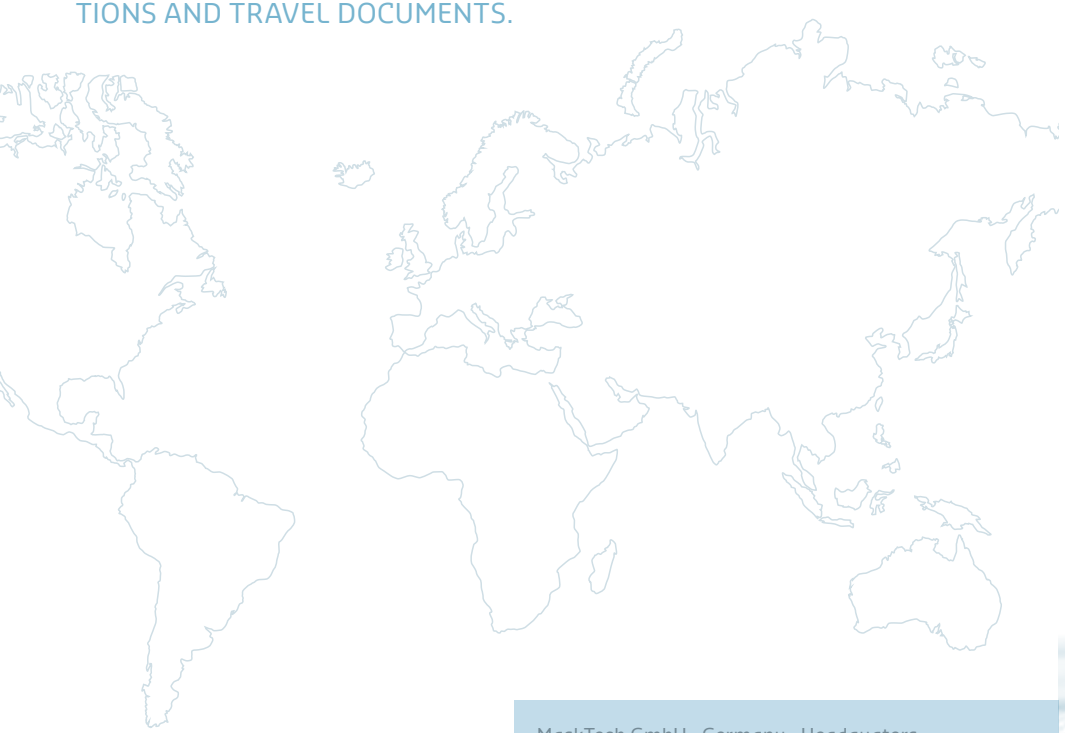
MASKTECH

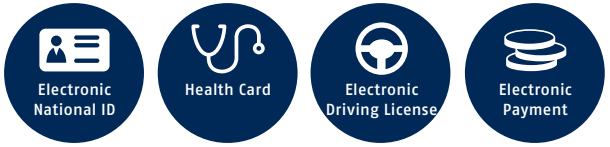
SECURITY SOFTWARE – CERTIFIED AND MADE IN GERMANY.

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



MTCOS® FLEX-ID

Short Form Specification



Performance and security for smart cards with limited memory and processing capabilities. MTCOS® FLEX-ID powers Flash Common Criteria EAL5+ and EAL6+ certified high security chips used in eID documents, authentication and social security solutions. The OS supports all essential features for cost-efficient electronic identification and is based on the latest security standards. All applications are built-in and can be activated by the personalizer on demand. MTCOS® secures over 65 eID projects 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

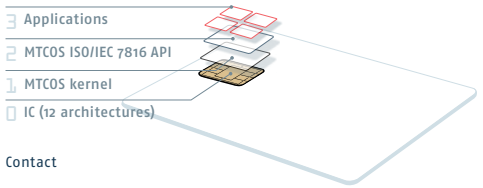
Visit us: www.masktech.com

MaskTech GmbH , Rev. 3.0, August 2024

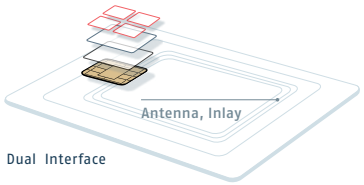
MTCOS® FLEX-ID
SHORT FORM SPECIFICATION

TECHNOLOGY

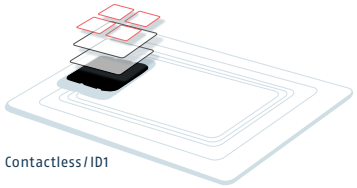
MTCOS® supports cryptographic smartcards with contact based, dual and contactless interface.

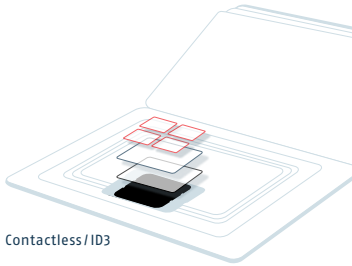


Contact



Dual Interface


Contactless / ID1


Contactless / ID3

APPLICATIONS	MTCOS® eID	MTCOS® eHEALTH	MTCOS® eDRIVING LICENSE	MTCOS® ePAYMENT	CUSTOMIZED APPLICATIONS
DESCRIPTION	ICAO application complemented by signature, certificates and strong PKI authentication for eGovernment usage. Features available for all applications installed in the OS. Pre- and post issuance personalization of additional applications.	Secure storage of personal patient data in the IC secure memory offers a maximum of data privacy in modern health infrastructures. Strong protection against cloning of the health card.	Support of the international standard ISO/IEC 18013 and the latest EU regulations. Individual configuration of the ISO/IEC 18013 security protocols. Support of various cryptographic protocols and keylengths.	Simple to use one command payment transaction. Short transaction times for contactless applications. Reduced overall product complexity.	Secure pre- and post issuance of customized applications by the card issuer or delegatee. New applications can reuse all functions embedded in MTCOS®. No code developement required. Optional: application development by MaskTech security specialists.
APPLICATION FEATURES	• DOC9303 and BSI TR03110 (PA, BAC, AA, SAC, EAC) • Signatures and certificates • PKI and SKI authentication • PIN (user) authentication • ISO/IEC Multi-application (pre- and post issuance) Optional: • MINEX II / Match-on-Card	• Trusted Medic • Signatures and certificates • Copy protection • Emergency data • ISO/IEC 21549 Control (SAC) / PACE	• ISO/IEC 18013-2,3,4 • Support of all DGs • Passive Authentication • Basic Access Protection/Control • Active Authentication • Supplemental Access Control (SAC) / PACE • Extended Access Control	• Single command transaction • Full 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	• ISO/IEC 7816 multi-application architecture • Global Platform • PlugIns using MTCOS® sandbox technology
CHIP TECHNOLOGY	• STM ST31P450 (Flash) • SLE77 Flash Series	• 100 ... 256k[1] Flash • up to 20 years EEPROM data retention[1]	• DES, AES[1], PKI[1] crypto engines • DPA,SPA,EPA,UV,IR resistance[1] • True random number generator	• Active shield, V, F, T, C sensors[1] • CC EAL 6+ or EAL5+ certified[1] • MIFARE Classic or DESFIRE emulation[1]	• ISO/IEC 7816-3 contact[1] • ISO/IEC 14443 contactless[1] • Unique chip ID

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 64KB
- Individual file access rights
- Global Platform

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

SECURITY
- PIN, Trusted PIN
- Various authentication schemes
- Signature (CEN 14890, CEN 15480, PKCS#15)
- Random numbers
- Random UID / PUPI
- Strong resistance against DPA,DFA, SPA, EPA, UV, IR attacks
- RSA and EC key generation
- Anti-skimming feature[1]

CRYPTOGRAPHY
- DES & 3DES
- AES
- SHA 1 & 2[1]
- RSA up to 3072 Bit[1]
- Elliptic Curve up to 512 Bit

USER MEMORY
- up to 144kB[1]

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

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

[1] depends on semiconductor