

**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.**



MaskTech GmbH • Germany • Headquarters  
Nordostpark 45 • 90411 Nuernberg • Germany  
Phone +49 911-955149-0 • Fax +49 911-955149-7  
[info@masktech.de](mailto:info@masktech.de)

MaskTech GmbH • Germany • Support  
Bahnhofstrasse 13 • 87435 Kempten • Germany  
Phone +49 911 955149-0 • Fax +49 831 5121077-1  
[support@masktech.de](mailto:support@masktech.de)

**Visit us: [www.masktech.com](http://www.masktech.com)**

# MTCOS® FLEX-ID

Short Form Specification



Electronic  
National ID



Health Card



Electronic  
Driving License



Electronic  
Payment

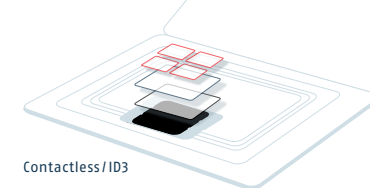
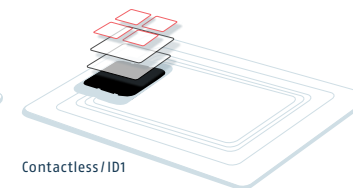
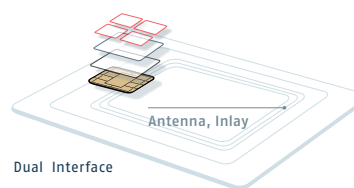
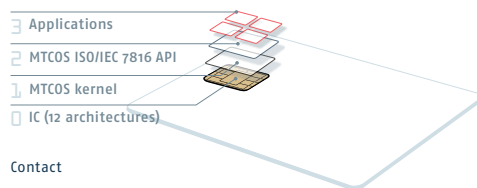
Performance and security for smart cards with limited memory and processing capabilities. MTCOS® FLEX-ID powers Flash and ROM based Common Criteria EAL5+ certified high security chips used in eID documents, authentication and social security solutions. The OS supports all essential features for cost-efficient 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.

# MTCOS® FLEX-ID

## SHORT FORM SPECIFICATION

### TECHNOLOGY

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



| APPLICATIONS         | MTCOS® eID                                                                                                                                                                                                                                                                                                                                                                   | MTCOS® eHEALTH                                                                                                                                                                                              | MTCOS® eDRIVING LICENSE                                                                                                                                                                                                                                         | MTCOS® ePAYMENT                                                                                                                                                                                                                                                                                                                               | CUSTOMIZED APPLICATIONS                                                                                                                                                                                                                                                       |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DESCRIPTION          | <p>ICAO application complemented by signature, certificates and strong PKI authentication for eGovernment usage.</p> <p>Features available for all applications installed in the OS.</p> <p>Pre- and post issuance personalization of additional applications.</p>                                                                                                           | <p>Secure storage of personal patient data in the IC secure memory offers a maximum of data privacy in modern health infrastructures.</p> <p>Strong protection against cloning of the health card.</p>      | <p>Support of the international standard ISO/IEC 18013 and the latest EU regulations.</p> <p>Individual configuration of the ISO/IEC 18013 security protocols.</p> <p>Support of various cryptographic protocols and keylengths.</p>                            | <p>Simple to use one command payment transaction.</p> <p>Short transaction times for contactless applications.</p> <p>Reduced overall product complexity.</p>                                                                                                                                                                                 | <p>Secure pre- and post issuance of customized applications by the card issuer or delegatee.</p> <p>New applications can reuse all functions embedded in MTCOS®. No code development required.</p> <p>Optional: application development by MaskTech security specialists.</p> |
| APPLICATION FEATURES | <ul style="list-style-type: none"> <li>• DOC9303 and BSI TR03110 (PA, BAC, AA, SAC)</li> <li>• Signatures and certificates</li> <li>• PKI and SKI authentication</li> <li>• PIN (user) authentication</li> <li>• ISO/IEC Multi-application (pre- and post issuance)</li> </ul> <p>Optional:</p> <ul style="list-style-type: none"> <li>• MINEX II / Match-on-Card</li> </ul> | <ul style="list-style-type: none"> <li>• Trusted Medic</li> <li>• Signatures and certificates</li> <li>• Copy protection</li> <li>• Emergency data</li> <li>• ISO/IEC 21549 Control (SAC) / PACE</li> </ul> | <ul style="list-style-type: none"> <li>• ISO/IEC 18013-2,3,4</li> <li>• Support of all DGs</li> <li>• Passive Authentication</li> <li>• Basic Access Protection</li> <li>• Active Authentication</li> <li>• Supplemental Access Control (SAC) / PACE</li> </ul> | <ul style="list-style-type: none"> <li>• Single command transaction</li> <li>• Full SAM support</li> <li>• Transaction counters for the ePurse and SAM</li> <li>• Transaction receipt</li> <li>• Two certificate keys</li> <li>• Key derivation with the SAM</li> <li>• Increase / decrease limits</li> <li>• AES and 3DES support</li> </ul> | <ul style="list-style-type: none"> <li>• ISO/IEC 7816 multi-application architecture</li> <li>• Global Platform</li> <li>• PlugIns using MTCOS® sandbox technology</li> </ul>                                                                                                 |
| CHIP TECHNOLOGY      | <ul style="list-style-type: none"> <li>• Infineon SLE77 Flash Series</li> <li>• NXP P60D042 (ROM)</li> <li>• Samsung S3 Flash Series</li> </ul>                                                                                                                                                                                                                              | <ul style="list-style-type: none"> <li>• 100...256k<sup>1</sup> Flash</li> <li>• up to 20 years EEPROM data retention<sup>1</sup></li> </ul>                                                                | <ul style="list-style-type: none"> <li>• DES, AES<sup>1</sup>, PKI<sup>1</sup> crypto engines</li> <li>• DPA,SPA,EPA,UV,IR resistance<sup>1</sup></li> <li>• True random number generator</li> </ul>                                                            | <ul style="list-style-type: none"> <li>• Active shield, V, F, T, C sensors<sup>1</sup></li> <li>• CC EAL 6+ or EAL5+ certified<sup>1</sup></li> <li>• MIFARE Classic or DESFIRE emulation<sup>1</sup></li> </ul>                                                                                                                              | <ul style="list-style-type: none"> <li>• ISO/IEC 7816-3 contact<sup>1</sup></li> <li>• ISO/IEC 14443 contactless<sup>1</sup></li> <li>• Unique chip ID</li> </ul>                                                                                                             |

### 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<sup>1</sup>

#### CRYPTOGRAPHY

- DES & 3DES
- AES
- SHA 1 & 2<sup>1</sup>
- RSA up to 3072 Bit<sup>1</sup>
- Elliptic Curve up to 512 Bit

#### USER MEMORY

- 8k... 64k Bytes<sup>1</sup>

#### DELIVERY TYPES

- Wafer
- Contactless module
- Contact module
- Dual interface module

#### TOOLS

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

<sup>1</sup> depends on semiconductor