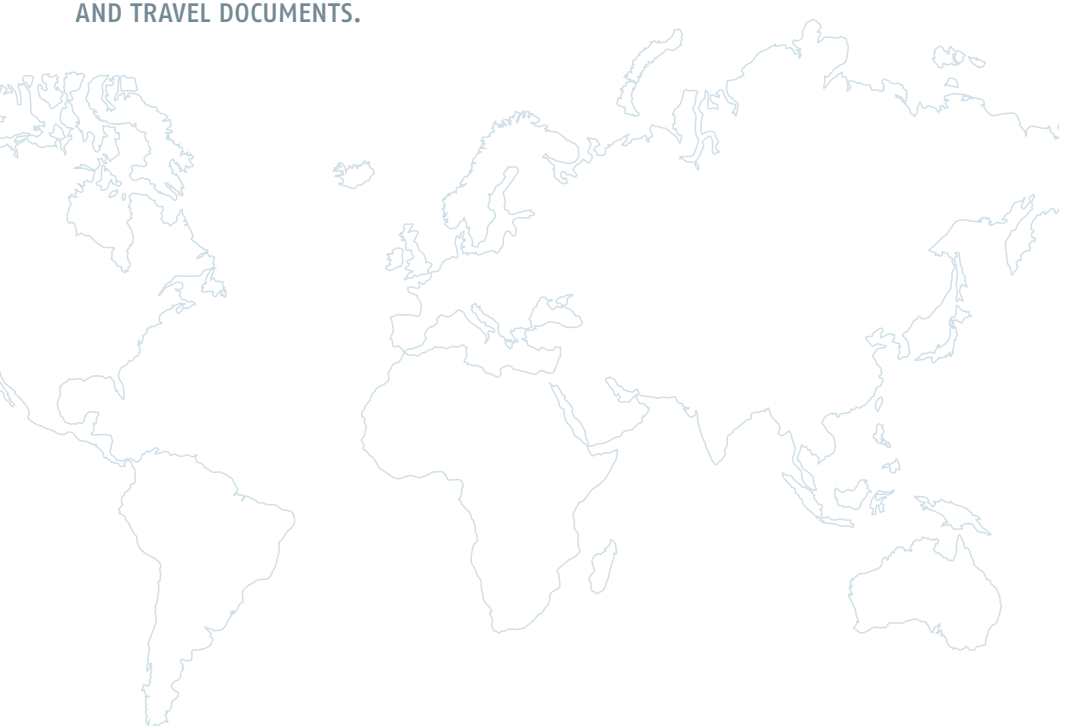
MASKTECH

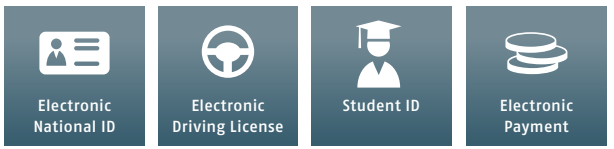
**SECURITY SOFTWARE – CERTIFIED AND MADE IN GERMANY.**

MASKTECH IS THE LEADING INDEPENDENT SUPPLIER OF SYSTEM-ON-CHIP AND OPERATING SYSTEMS FOR SMARTCARD ICs USED IN IDENTIFICATION APPLICATIONS AND TRAVEL DOCUMENTS.



# MTCOS® COMPACT

Short Form Specification




MTCOS® COMPACT – more succes for basic-ID systems. Designed for very cost efficient contact based chip card ICs without the advanced Common Criteria security requirements. MTCOS® Compact is a ISO / IEC 7816 multiapplication OS used in entry level eID, ePurse and driver's license smart cards.

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

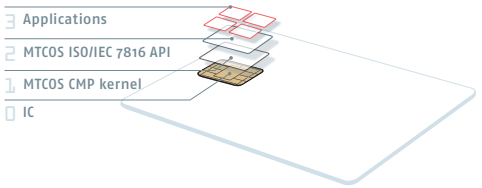
MaskTech GmbH · Germany · Support
Bahnhofstrasse 13 · 87435 Kempten · Germany
Phone +49 tba · Fax +49 tba
support@masktech.de

Visit us: www.masktech.de

MaskTech GmbH , Rev. 2.1, November 16

# MTCOS® COMPACT
## SHORT FORM SPECIFICATION

### TECHNOLOGY
MTCOS® supports cryptographic chipsets with contact interface.




| APPLICATIONS | MTCOS® eID(E) | MTCOS® eDRIVING LICENSE(E) | MTCOS® Student ID | MTCOS® ePAYMENT | CUSTOMIZED APPLICATIONS |
|---|---|---|---|---|---|
| DESCRIPTION | Designed for entry level eID applications and support of ISO / IE C 7816 data structures, applications, file life cycles and multiapplications. | Extends the security of traditional paper driving licenses with basic ISO / IEC 18013 features and passive authentication. | The ISO / IE C 7816 multiapplication file system allows universities to install and configure campus services such as payment (mensa, photocopier, etc) semester and exam registration and access to discounted services. | Our ePurse application supports a unique and extremely simple to use one commmand payment transaction. This significantly decreases the payment transaction times for contactless applications and reduces the overall product complexity to a minimum. | Additional applications can easily be added by the card issuer or delegated respectively. Installed applications can access the MTCOS® Compact feature set, data handling procedures and crypto protocols embedded in MTCOS® masks without additional code development. |
| APPLICATION FEATURES | • Basic features of DOC 9303<br>• Passive Authentication (PA)<br>• User authentication (PIN)<br>• Device authentication | • Basic ISO / IEC 18013 features<br>• Passive Authentication<br>• Device authentication | • Storage of student ID data<br>• Passive Authentication (PA)<br>• Increase / decrease features<br>• User authentication (PIN)<br>• Device authentication | • Single command transaction<br>• Full SAM support<br>• Transaction counters for the ePurse and SAM<br>• Transaction receipt<br>• Two certificate keys<br>• Key derivation with the SAM<br>• Increase / decrease limits<br>• AES and 3DES support | • ISO/IEC 7816 application directories and application specific files, keys and PINs |
| CHIP TECHNOLOGY | • 8-Bit / 80X51 CPU<br>• 30 MHz CPU clock<br>• ISO 7816-3 compliant interface (contact) | • Basic DPA and SPA countermeasures<br>• Over / under voltage sensors | • 10 years EEPROM data retention<br>• Hardware random number generator | • Unique chip ID<br>• 32k, 64k, 128k user EEPROM | |

### COMMON FEATURES

#### COMMUNICATION
- ISO/IEC 7816 contact based (T=1)
- Secure messaging
- PC/SC compatible

#### OS CHARACTERISTICS
- Highest performance through direct code processing
- Secure design

#### DATA HANDLING
- ISO/IEC 7816-4...9
- Transactions
- File sizes up to 4GB
- Individual file access rights

#### LIFE CYCLES
- ISO/IEC 7816 file life cycles

#### SECURITY
- PIN
- Various authentication schemes
- Random numbers

#### CRYPTOGRAPHY
- DES & 3DES

#### USER MEMORY
- 32k, 64k, 128k

#### DELIVERY TYPES
- Wafer
- Contact module

#### TOOLS
- Smart Platform scripter, file system tool
- MTCOS® MANAGER

#### PRODUCT UPGRADE 1
MTCOS® FlexID
- CC certified semiconductors
- MTCOS CC EAL4+
- Contactless
- BAC, BAP protocol

#### PRODUCT UPGRADE 2
MTCOS® Professional
- Public key features and applications

[E] entry level feature set