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® MANAGER

Short Form Specification

Electronic Passport

Electronic Driving License

Electronic Residence Permit

Electronic ID

MTCOS® MANAGER – the SDK for secure handling and personalization of MTCOS® based chipsets. Supported applications are electronic passport according to ICAO DOC 9303 and BSI-Tr03110, electronic national ID with signature features, eDriver's license according to ISO/IEC 18013 and eResidence permit according to the relevant EU regulations.

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

MASKTECH MTCOS® MANAGER

Software development kit for secure handling and personalization of MTCOS® based chipsets and it's built-in applications

TECHNOLOGY

The MTCOS® MANAGER is a dynamic link library (DLL) to integrate MTCOS® into personalization infrastructures. The DLL is compatible with C / C++ development tools for Microsoft Windows operating systems.

APPLICATIONS	ePASSPORT	eID	eDRIVING LICENSE	eRESIDENCE PERMIT	CUSTOMIZED
DESCRIPTION	Personalization and life cycle API for the MTCOS® built-in ePassport application with support of all relevant security mechanisms, access control, crypto protocols and data formats defined in ICAO DOC 9303 and BSI Tr03110 standards.	API for a secure personalization of a PKCS#15 file system with multiple PINs, keys and certificates. All other MTCOS® applications may be added and personalized using MTCOS® and the SDKs feature set.	Personalization and life cycle API for MTCOS® built-in eDriving License application with support of the ISO/IEC 18013 and EU standards.	Personalization and life cycle API for the MTCOS® built-in eResidencePermit application. The library supports all relevant security mechanisms, access control, crypto protocols and data formats defined in the relevant EU regulations for the eRP.	The SDK will on request be extended to meet new personalization systems requirements and / or new functions, applications and cryptographic features.
FEATURES	• Image converter • ICAO converter • DOC9303 / Passive Authentication, Active Authentication, Basic Access Control • BSI Tr03110 – Extended Access Control • BSI Tr03110 – Supplemental Access Control / PACE [1] • 4-stage life cycle process • Common Criteria mode • 7816-4, chip writer functions • ISO/IEC 14443, 7816-3, PC/SC	• ISO/IEC 7816-15 • CEN 15480 • CEN 14890 • ISO/IEC 7816 multiapplication (e.g. ICAO + eSign) pre- and post issuance • 4-stage life cycle process • Common Criteria mode • 7816-4, chip writer functions • ISO/IEC 14443, 7816-3, PC/SC	• ISO/IEC 18013 converter • ISO/IEC 18013 / Passive Authentication, Basic Access Protection, Active Authentication, Extended Access Protection / Extended Access Control Supplemental Access Control / PACE 1 • 4-stage life cycle process • 7816-4, chip writer functions • ISO/IEC 14443, 7816-3, PC/SC	• Image converter • ICAO converter • DOC9303 / Passive Authentication, Active Authentication, Basic Access Control • BSI Tr03110 / Extended Access Control, Supplemental Access Control1 • 4-stage life cycle process • Common Criteria mode • 7816-4, chip writer functions • ISO/IEC 14443, 7816-3, PC/SC	Based on customer requirements and infrastructure.
OS VERSION AND CHIP TECHNOLOGY	All MTCOS® versions V2.1 and higher				

COMMON FEATURES

IMAGE CONVERTER

- BMP2JPEG, BMP2JPEG2k, BMP2WSQ
- JPEG2JPEG, JPEG2JPEG2k, JPEG2WSQ
- Auto-compression to specified size
- Easy exchange of input and output image formats

ICAO CONVERTER

- ISO/IEC 19794 and ISO/IEC 7816-11
- ICAO TrLDS data group formatting
- BAC keyfile assembly from MRZ

ISO/IEC 18013 CONVERTER

- ISO/IEC 18013-2,3
- BAP keyfile assembly from textfield / barcode / 1-line MRZ
- EAP / EAC

SECURE PERSONALIZATION

- 4-stage life cycle manager
- Transport key protection
- SAM

PASSIVE AUTHENTICATION (PA)

- Hash and signature generation with SHA 1 & 2 / RSA 1024 … 4096 Bit
- Import of DSCA and CSCA certificates
- Generation of DSCA and CSCA certificates
- EF.SOD assembly

ACTIVE AUTHENTICATION (AA)

- Generation of asymmetric public – private key pair / RSA and ECC
- EF.DG15 (ePass) and EF.DG13 (eDL) assembly

EXTENDED ACCESS CONTROL (EAC) & EXTENDED ACCESS PROTECTION (EAP)

- Generate asymmetric public – private keypair supporting RSA 1024 … 2048 Bit and Elliptic Curve up to 512 Bit
- EF.DG14 assembly

SUPPLEMENTAL ACCESS CONTROL (SAC)

- Key derivation from MRZ / CAN
- Assembly of EF.CARDACCESS and DG14

OTHER TOOLS

- Smart Platform scripter, file system tool

[1] requires MTCOS V2.2 and higher