

SECURITY SOFTWARE – CERTIFIED AND MADE IN GERMANY.

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



MaskTech GmbH, Germany · Sales
Fischerstrasse 19 · 87435 Kempten · Germany
Phone +49 831-5121077-1 · Fax +49 831-5221077-5
sales@masktech.de

MaskTech GmbH · Germany · Headquarter
Nordostpark16 · 90411 Nürnberg · Germany
Phone +49 911-955149-0 · Fax +49 911-955149-7
support@masktech.de

Visit us: www.masktech.com

MASKTECH MTCOS SDK

Technical Data Sheet



Electronic
Passport



Electronic
Driving License



Electronic
Residence Permit



Electronic
ID





Masktech's MTCOS SDK is a software development kit offering a comprehensive set of functions for the secure handling and personalization of MTCOS® based chipcard ICs. Supported applications are electronic passport according to ICAO DOC 9303 and BSI-Tr03110, electronic national ID, eDriver's license according to ISO/IEC 18013 and eResidence permit according to the relevant EU regulations.

MASKTECH MTCOS SDK

Software development kit for secure initialization, pre-personalization and personalization of MTCOS® chipsets and applications

TECHNOLOGY

The MTCOS SDK is delivered as dynamic link library compatible with C / C++ development tools for Microsoft Windows 2000, XP, VISTA and 7 operating systems.

APPLICATIONS	 ePASSPORT & eID	 eDRIVING LICENSE	 eRESIDENCE PERMIT	 CUSTOMIZED
DESCRIPTION	Personalization DLL for MTCOS® based ePassport / eID chipsets with support of all relevant security mechanisms and data formatting defined in ICAO DOC 9303 and BSI Tro3110.	Personalization DLL for MTCOS® eDrivers License chipsets with support of the ISO/IEC 18013 standard.	Personalization DLL for MTCOS® eResidence Permit and eID chipsets. The library supports all security mechanisms defined in the relevant EU regulations.	The SDK can be easily extended to meet new personalization systems requirements and/or new functions, applications and cryptographic features.
FEATURES	<ul style="list-style-type: none"> • Image converter • ICAO converter • DOC9303 / Passive Authentication, Active Authentication, Basic Access Control • BSI Tro3110 / 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 	<ul style="list-style-type: none"> • ISO/IEC 18013 converter • ISO/IEC 18013 / Passive Authentication, Basic Access Protection, Active Authentication, Extended Access Protection¹ • 4-stage life cycle process • 7816-4, chip writer functions • ISO/IEC 14443, 7816-3, PC/SC 	<ul style="list-style-type: none"> • Image converter • ICAO converter • DOC9303 / Passive Authentication, Active Authentication, Basic Access Control • BSI Tro3110 / 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	<ul style="list-style-type: none"> • All MTCOS® versions V2.0 and higher • INFINEON SLE66 & SLE78, NXP SmartMX & SmartMX2, ST MICROELECTRONICS ST23 			¹ MTCOS V2.2 and higher

COMMON FEATURES

IMAGE CONVERTER

- BMP2JPEG, BMP2JPEG2k
- BMP2WSQ
- Autocompression 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 dedicated textfield / barcode
- EAP (refer to ePassport EAC)

LIFE CYCLES

1. Initialization
2. Prepersonalization
3. Personalization
4. Operational

PASSIVE AUTHENTICATION (PA)

- Hash and signature generation with SHA-1 ... 256 / 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

OTHER TOOLS

- Smart Platform: PC/SC scripser-, ISO/IEC 7816 file system and application tool