MASKTECH

MTCOS®
eDRIVING LICENSE

the high performance standard for e-driving license ICs

ISO/IEC 18013
EU Commission Directive 383/2012

MTCOS®
eDRIVING LICENSE

High security system on chip solutions for electronic drivers licenses.

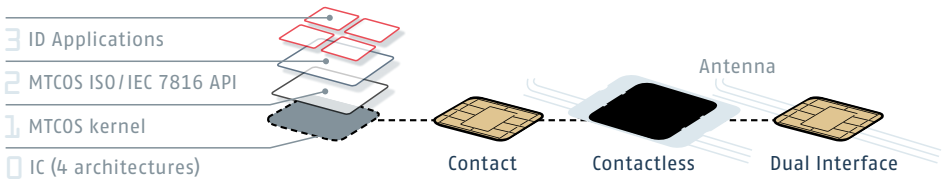
MaskTech is the leading developer of high security system on chip solutions (SoC) used in smart cards and contactless identification applications such as electronic passports, residence permits, national IDs, driving licenses and health cards.

Our product portfolio includes generic and customized masks / operating systems for state-of-the-art smartcard ICs of all leading semiconductor manufacturers, appropriate middleware and security certification services.

As one of the few, if not the only, **independent suppliers** of secure embedded operating systems, to date MTCOS® protects more than 100m eDocuments around the globe.

MTCOS® & eDriversLicense

MTCOS® with built-in eDrivingLicense application has been rolled out in several large volume national projects and with several million documents in circulation. The documents are designed strictly according to the ISO/IEC 18013 standard for a cost effective and flexible procurement process of all further system components.



Driving licenses are being used as primary form of identification in several countries. Unauthorized personnel could acquire private details like the holder's address by just viewing the information printed on the document or plastic card. Using an electronic driving license, sensitive information can be moved to an embedded chip that enforces state-of-the-art security mechanisms to safely store and access these data.

MTCOS® & Passive Authentication

The data are protected with an electronic signature guaranteeing integrity and authenticity.

MTCOS® & BAP

The Basic Access Protection mechanism (BAP) protects personal driving license holder data against unauthorized reading attempts and prevents skimming as well as eavesdropping by encrypting the communication between chip and terminal.

MTCOS® & AA

Active Authentication (AA) ensures that the driving license is not a clone of another driving license.

MTCOS® & EAC / EAP

Fingerprints and other sensitive data may be stored on the driving license's chip. The Extended Access Control and Extended Access Protection procedures strongly secure these data against unauthorized reading and copying in addition to the basic protection mechanisms. Compared to EAC, EAP allows protecting up to 24 data groups.

MTCOS® & SAC / PACE

The new Supplemantal Access Control (SAC) also known as Password Authenticated Connection Establishment (PACE) protocol is an alternative to BAP that offers advanced resistance against skimming and eavesdropping of the driving license. SAC / PACE provides strong session keys independent of the input string's (e.g. MRZ or Card Access Number) entropy.

MTCOS® & Security

MTCOS® implements a unique Anti-Skimming procedure to prevent the unauthorized reading of the eDriversLicense by brute-force attacks.

MTCOS® & Privacy

MTCOS® uses a random identification number (UID / PUPI) that is changed automatically with every new reading operation making tracking of the drivers license holder or compilation of a user profile impossible.

TECHNOLOGICAL COMPETENCE AND RELIABILITY

Highest security by modern cryptographic encryption.

Maximum flexibility in semiconductor support.

Large functional range.

Many years of experience.

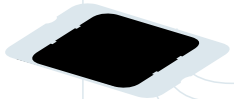
Standard solutions and customer specific development.

Independent.

MTCOS® eDL chip options:

MTCOS® supports cryptographic chipsets with contact-, contactless- and / or dual interface.

Contact



Contactless

Dual Interface

Passive Authentication	Extended Access Protection	RSA Cryptography	Anti-skimming software
Basic Access Protection	SAC / PACE	Elliptic Curve Cryptography	Global Platform
Active Authentication	3DES Cryptography	Data Privacy	
Extended Access Control	AES Cryptography	Support of all DGs	

1 Flexibility
Individual configuration of the security protocols like PA only, PA+BAP, PA+BAP+AA, PA+BAP+AA+EAC or EAP. All the proven protocols may be extended by SAC / PACE or SAC / PACE may be used independently if the infrastructure allows.

2 Project specific extensions
Possibility to add and adjust datagroup files with individual sizes.

3 Customer specific features
Addition of customer specific add-ons, functions and application directories during the init- and pre-personalization phase.

BEYOND THE MERE OPERATING SYSTEM...
Product procurement, product dependancies

4 Availability
MTCOS® is available on multiple semiconductors. We offer hardware ports to chip platforms with the best price-performance ratio.

5 Compatibility
Support of important international standards such as ISO / IEC 7816, ISO / IEC 14443. Open design free of third party rights and license costs.

INDIVIDUAL CONFIGURATION

Our core expertise and products cover embedded software development with comprehensive Common Criteria certifications – if required, application specific product extensions and setup of MTCOS® in complex security environments.

Our specialists assist in the integration of MTCOS® in any ePassport personalization and manufacturing infrastructure available today.

MTCOS® & standards:

- ISO / IEC 7816 – 3,4,6,8,9,15
- ISO/IEC 18013 – 1–4
- ISO/IEC 18013 – BAP Config 1 ... 4
- ISO / IEC 14443 Type A or B

MTCOS® & personalization:

- ISO / IEC 4–Stage life cycle manager
- Transport key protection with SAM & HSM
- Global Platform
- Fast personalization mode

MTCOS® & eDriversLicense masks:

- IFX SLE78 series (MTCOS PRO V2.2, 36k, 80k, 160k)
- IFX SLE77 series (MTCOS Flex ID V2.2, up to 64k)
- NXP P5 and P60 (MTCOS PRO V2.1 & 2.2, 40k, 80k)
- ST23Y series (MTCOS PRO V2.1, 48k, 80k)

SECURITY
IN EVERY PHASE

Challenges to be met – 4 examples:

1 PARTICULAR PERSONALIZATION INFRASTRUCTURES

2 CUSTOMER SPECIFIC FEATURES COMMON CRITERIA CERTIFIED

3 VARIETY OF CRYPTOGRAPHIC PROCEDURES AND SECURITY LEVELS

4 MULTIPLE CONFIGURATIONS

OUR APPROACH

MTCOS® supports the life cycle model specified by Common Criteria for the production process of modern electronic drivers licenses. All data communication is completely encrypted. Unauthorized access is prevented by transport keys.

MTCOS® can be upgraded flexibly at the customer's request without changing the ROM-mask. The changes are loaded completely encrypted during the OS-setup using a loading mechanism that is Common Criteria certified. The final product configuration is completely security tested and qualified.

MTCOS® supports a variety of cryptographic protocols by default, such as Elliptic Curves, RSA, 3DES and AES with key lengths meeting present and future security demands. Further customer specific crypto procedures can be loaded securely in initialization phase. On request we develop project specific masks, if required with Common Criteria certification.

MTCOS® can be configured to meet any ISO/IEC 18013 configuration: Just Passive Authentication and Basic Access Protocol compliance with or without Extended Access Control or Extended Access Protocol and, furthermore, with or without Active Authentication in both cases. SAC/PACE may be amended anytime and is processed at personalization level without the need of changes in the product itself or its configuration.

MASKTECH

MaskTech is an independent supplier of high-security embedded microprocessor operating systems. MaskTech licenses and sells embedded security products for the human identification market. The private company has its headquarters in Nürnberg, Germany.

MaskTech GmbH was founded in 2002 as a private company. Since 1990 the engineering team has gained profound knowledge and experience in the areas of cryptography, security, RFID and development of embedded and middle-ware solutions.

We are an independent company, not involved in smartcard, inlay or booklet manufacturing which may interfere with our clients portfolio.

MTCOS® supports various semiconductor manufacturers. The support of multiple chip platforms provides many advantages for the system integrators and end customers, like easier procurement and better availability, also during fab allocations.

MTCOS® APPLICATIONS OVERVIEW

MTCOS® built-in applications

MTCOS® ePASSPORT

Worldwide first and today the most popular operating system for ePassports.

It supports various semi-conductor manufacturers.

- ICAO DOC 9303
- BSI TR03110
- Basic Access Control
- Active Authentication
- Extended Access Control
- Supplemental Access Control / PACE

MTCOS® eID

ICAO application supple-mented by eGovernment applications.

- ICAO DOC 9303, BSI TR03110
- Digital Signature
- Certificates
- Match on Card
- Multiapplication, pre- and post issuance personalization

MTCOS® eHEALTH

Highest security and data privacy for sensitive patient health records and personal data.

- Innovative Pin Management
- Trusted Medic
- Digital Signature
- Certificates
- Card2Card Authentica-tion

MTCOS® eDRIVING LICENSE

Strong protection against forgery for electronic drivers licence with chip and a maxi-mum of data privacy for the license holder.

- ISO 18013 compliant
- Basic Access Protection
- Active Authentication
- Extended Access Control
- Supplemental Access Control / PACE

MTCOS® ePAYMENT

Easy to use "single command" ePurse for best transaction times complemented by our secure MTCOS®-SAM.

- Single command transaction
- Transaction counters
- Transaction receipt
- Two certificate keys
- Key derivation with SAM
- Increase/Decrease limits
- 3DES & AES support

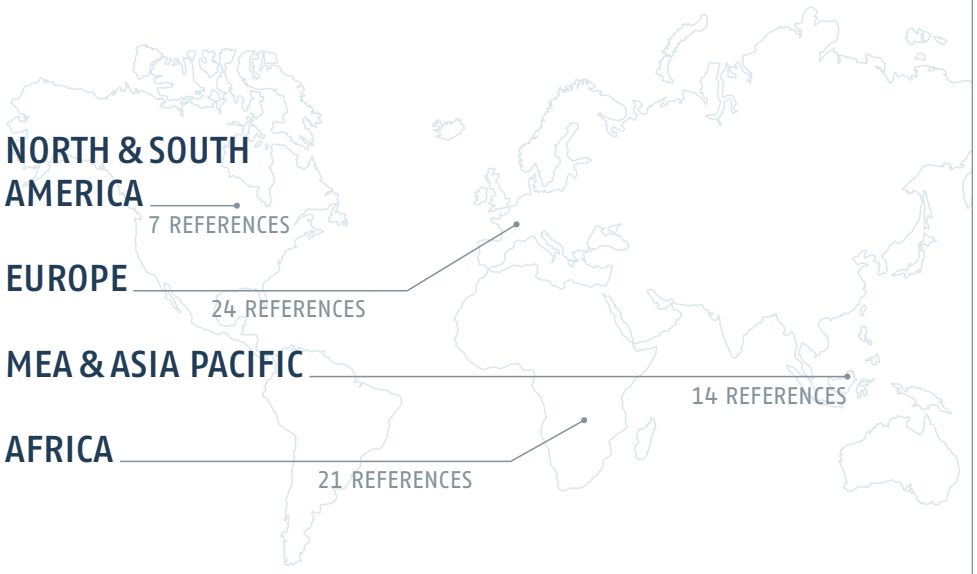
MTCOS® eRESIDENCE PERMIT

MTCOS® interoperable with the EU eResidence Permit regulation and other international standards.

- ICAO DOC 9303
- BSI TR03110
- Basic Access Control
- Active Authentication
- Extended Access Control
- Supplemental Access Control / PACE

REFERENCES

MTCOS® is one of the most frequently used chip operating system for eID documents. More than 65 ICAO member countries have issued their ID- and travel documents with MaskTech secure OS.



MaskTech's MTCOS® is embedded in 45 countries ePassports worldwide and more than 20 countries eHealth, eResidence Permit, eNational ID, eDrivers License, welfare and authentication solutions in a unique variety of configurations and infrastructures.

WE MAKE CHIPS INTELLIGENT.

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

Visit us: www.masktech.com

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**
Nordostpark 16 · 90411 Nürnberg · Germany
Phone +49 911-955149-0 · Fax +49 911-955149-7
support@masktech.de