MASKTECH

MTCOS®
national ID

cryptographic – contact & contactless – biometric ID

High security / Common Criteria certified embedded operating system and ICs for national ID cards.

MTCOS®
eID

Contactless and highly secure identification applications custom-built for electronic national ID cards.

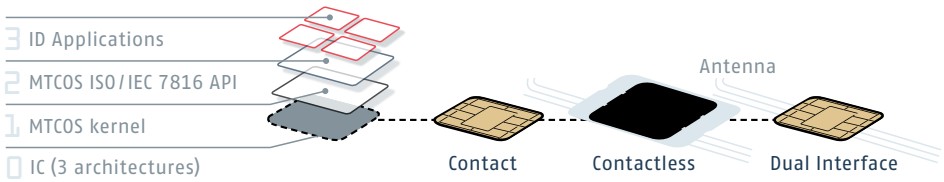
MaskTech is the leading developer of high security system on chip solutions (SoC) used in smart cards and contactless identification applications such as electronic passports, residence permits, national IDs, driving licenses and health cards.

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® & eID

MTCOS® eID is used in various microprocessor based ID card projects worldwide. MTCOS® masks include a large variety of eGovernment services and applications available on a single chip. All OS security-, file system- and life-cycle features are available for new applications that may be added securely during or after issuance.



Since decades the identity of individual citizens is confirmed by their personal identity documents. Nowadays an eID, this is a National ID card with sophisticated visible and invisible security features and an embedded secure microprocessor, takes over this role. Smart card microprocessors are virtually impossible to be counterfeited. Thus the security of the electronic document (eID) is increased to an unrivaled level. The chip securely stores the biographic data of the document holder, usually the readable data printed on the document. Moreover the biometric features which can be stored in the chip as well, create more confidence and improve user-friendliness as already successfully demonstrated with ePassports. The eID can act as interoperable travel document and enables access to e-government services.

MTCOS® & ICAO DOC 9303

Personal data stored in the chip memory are protected against unauthorized reading (BAC and SAC). An electronic signature (PA) guarantees integrity and authenticity while strong public key authentication (AA) prevents cloning and illegal copying of the eID card.

MTCOS® & BSI Tr03110

Access to sensitive biometric data such as fingerprints may be protected with the EAC feature which is available through all MTCOS® PRO versions. The EAC protocol may also be used for copy protection of the eID card.

MTCOS® & Client / Server Authentication

Support of client / server authentication mechanisms such as the transport layer security and socket security layer (TLS / SSL) network protocols may be used to release access to user specific web content and services.

MTCOS® & Electronic Signature

The electronic signature ensures a person adopts to a specific message and that the content of this message is the one that has been created by that person. MTCOS® supports the secure signature creation device (SSCD) feature set fully evaluated and certified according to the German signature law.

MTCOS® & PIN / PUK

MTCOS® supports knowledge based user authentication as defined in ISO / IEC 7816.

MTCOS® & Identification

The unique ID number of the card holder can be protected by customized access rights.

MTCOS® & Privacy

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

TECHNOLOGICAL COMPETENCE AND RELIABILITY

Highest security by modern cryptographic encryption.

Maximum flexibility in semiconductor support.

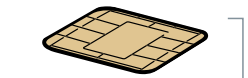
Large functional range.

Many years of experience.

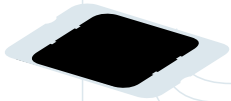
Standard solutions and customer specific development.

Independent.

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



Contact



Contactless

Dual Interface

Passive Authentication	3DES Cryptography	Electronic signature	Anti-skimming software
Basic Access Control	AES Cryptography	Knowledge based user auth.	Supplemental Access Control
Active Authentication	RSA Cryptography	Identification services	
Extended Access Control	Elliptic Curve Cryptography	Client / Server authentication	

1 **Flexibility**
Individual configuration of the security features and protocols for each application and data file. Cryptographic protocols are available for all installed applications on the chip.

2 **Adding Applications**
A powerful ISO/IEC multiapplication file system is included in MTCOS®. Applications are activated or added by creating new application directories. Installing new applications may be protected by administration keys.

3 **Pre- and post issuance loading**
Additional applications and plug-ins can be installed using our Common Criteria certified application loading mechanism, in any card life cycle and if permitted by the issuer.

4 **External Plug-ins**
Third party plug-ins such as match on card algorithms from different vendors or cryptographic features can be added securely. The code execution of all third party "Plug In's" is protected by the chip's hardware MMU.

BEYOND THE MERE OPERATING SYSTEM...
Flexible procurement, no additional dependencies

5 **Availability**
Hardware ports to chip platforms and memory configuration with the best price–performance ratio.

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

INDIVIDUAL CONFIGURATION

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

Our specialists assist to integrate MTCOS® in any eID personalization and manufacturing infrastructure.

MTCOS® & standards:

- ISO/IEC 7816 – 3,4,6,8,9,15
- ICAO DOC 9303
- BSI TR-03110
- ISO/IEC 14443 Type A or B
- CEN 14890, CEN 15480, PKCS#15

MTCOS® & eID applications

- Travel document (ICAO)
- Electronic signature
- Match on Card (MoC)
- Web logon, Client/Server authentication
- User authentication

MTCOS® & supported eID smart card ICs

- INFINEON SLE78 series (MTCOS PRO V2.2)
- INFINEON SLE77 series (MTCOS FlexID V2.2)
- NXP P5 & P60 series (MTCOS PRO V2.2)
- STM ST23 series (MTCOS PRO V2.1)

SECURITY
IN EVERY PHASE

Challenges to be met – 4 examples:

1 PARTICULAR PERSONALIZATION INFRASTRUCTURES

2 EXTENSIONS AND CUSTOMER SPECIFIC FEATURES BY MASKTECH

3 VARIETY OF CRYPTOGRAPHIC ALGORITHMS, CRYPTO MIGRATION

4 MULTIPLE APPLICATIONS

OUR APPROACH

MTCOS® supports the life cycle model specified by Common Criteria for the production process of modern electronic documents. All data communication is completely encrypted. Unauthorized access is prevented by transport keys. Global Platform secure messaging and key handling is available for customers using related equipment and functions.

MTCOS® can be upgraded flexibly on customer's request without changing the ROM-mask. The changes are loaded completely encrypted during the OS-setup using the loading mechanism that is Common Criteria certified. The resulting product configuration is completely security tested and certified. On request we also develop project specific masks.

MTCOS® supports a variety of cryptographic protocols, such as Elliptic Curves, RSA, 3DES and AES with key lengths meeting present and future security demands. Crypto migration allows the upgrade of cryptographic methods and keys in already issued ID documents in order to protect them from future potential risks and weaknesses.

MTCOS® built-in applications can be activated and used at any time in the document life cycle. All applications and features can be used stand alone or in any conceivable combination. Some examples of our pre-insatalled applications include ICAO, e-signature, user and device authentication, certificates and many more.

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

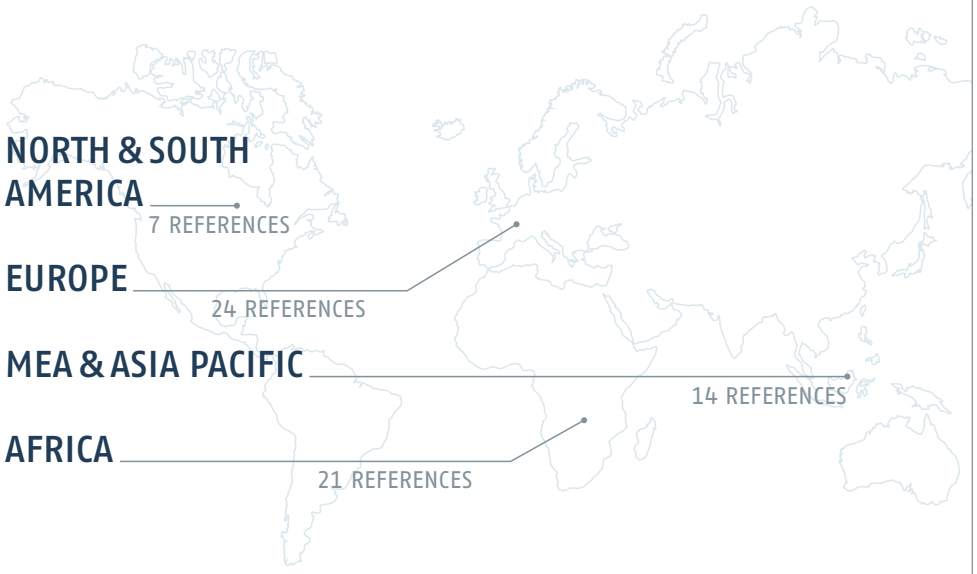
MTCOS® eRESIDENCE PERMIT

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