MASKTECH

MTCOS®
ePASSPORT

secure system on chip solutions for travel documents

MRTD according to ICAO/DOC.9303
and BSI TR03110 (EAC&SAC/PACE)

MTCOS®
ePASSPORT

Contactless and high security identification application built for electronic passports.

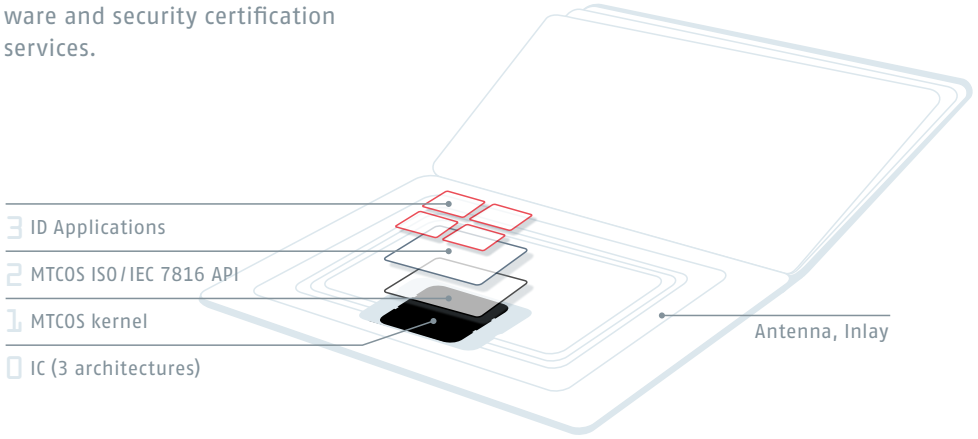
MaskTech is the leading developer of high security system on chip solutions (SoC) used in smart cards and contactless identification applications such as electronic passports, residence permits, national IDs, driving licenses and health cards.

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® & ePassport

In 2004 MTCOS® ePassport was introduced as the worldwide first fully ICAO compliant operating system. Today MTCOS® is the most popular embedded solution for electronic travel documents.



Because of growing international terrorism and increasing illegal migration, many governments have decided to introduce electronic passports. So the paper document finally becomes an electronic high-tech product. The ICAO advises the storage of biometric data, usually a digital facial image and two or more fingerprint images, in the contactless high security chip embedded in the passport.

MTCOS® & Passive Authentication

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

MTCOS® & BAC

The Basic Access Protocol protects personal passport holder data against unauthorized reading.

MTCOS® & AA

Active Authentication (AA) makes copying of an electronic passport impossible.

MTCOS® & EAC

Second generation biometric passports store the fingerprints of the passport holder. The Extended Access Control procedure (EAC) protects these sensitive data against unauthorized reading and copying in addition to the up to now existing security mechanisms.

MTCOS® & SAC / PACE

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

MTCOS® & Security

MTCOS® Anti-Skimming procedure prevents the unauthorized reading of the ePassport by brute-force attacks.

MTCOS® & Privacy

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

TECHNOLOGICAL COMPETENCE AND RELIABILITY

Highest security by modern cryptographic algorithms.

Maximum flexibility in semiconductor support.

Large functional range.

Many years of experience.

Standard solutions and customer specific development.

Independent.

- Passive Authentication
- Basic Access Control
- Active Authentication
- Extended Access Control
- Supplemental Access Control
- Support of all ICAO – DG's
- 3DES Cryptography
- AES Cryptography
- RSA Cryptography
- Elliptic Curve Cryptography
- Anti-skimming features

INDIVIDUAL CONFIGURATION

1 **Flexibility**
Individual configuration of the security protocols like PA+BAC, PA+BAC+AA, PA+BAC+AA+EAC. All proven protocols may be extended by SAC / PACE or PACE may be used independently.

2 **Project specific extensions**
Possibility to add and adjust data-group 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...

Flexible procurement, no additional dependencies

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.

Our core expertise and products cover embedded software development and corresponding Common Criteria certification – 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
- ICAO DOC 9303
- BSI TR-03110
- ISO / IEC 14443 Type A or B
- ISO / IEC 15408 / Common Criteria EAL4+

MTCOS® & personalization:

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

MTCOS® & latest ePassport masks:

- IFX SLE78CLX series (MTCOS PRO V2.2, 160k/80k/36k, EAL4+)
- NXP P5 & P60 series (MTCOS PRO V2.2, 80k/40k, EAL4+)
- ST23YR80 (MTCOS PRO V2.1, 80k, EAL4+)

SECURITY
IN EVERY PHASE

Challenges to be met – 4 examples:

1 INDIVIDUAL AND GENERIC PERSONALIZATION INFRASTRUCTURES

2 CUSTOMER SPECIFIC FEATURES COMMON CRITERIA CERTIFIED

3 VARIETY OF CRYPTOGRAPHIC ALGORITHMS, CRYPTO MIGRATION

4 MULTIPLE CONFIGURATIONS

OUR APPROACH

MTCOS® supports the life cycle model specified by Common Criteria for the production process of modern electronic passports. 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 certified.

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 travel and ID documents in order to protect them from future potential risks and weaknesses.

MTCOS® can be configured to meet every ICAO/EU requirement: Just Passive Authentication and Basic Access Control compliance with or without Extended Access Control and, furthermore, with or without Active Authentication in both cases. Supplemental Access Control 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

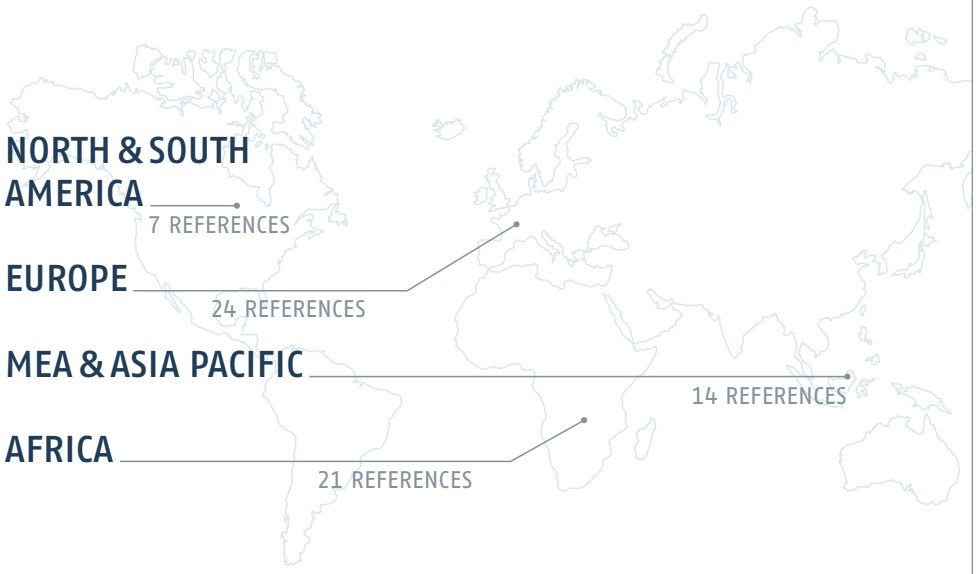
MTCOS® eRESIDENCE PERMIT

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