MASKTECH

MTCOS®
eHEALTH

PKI features and data privacy

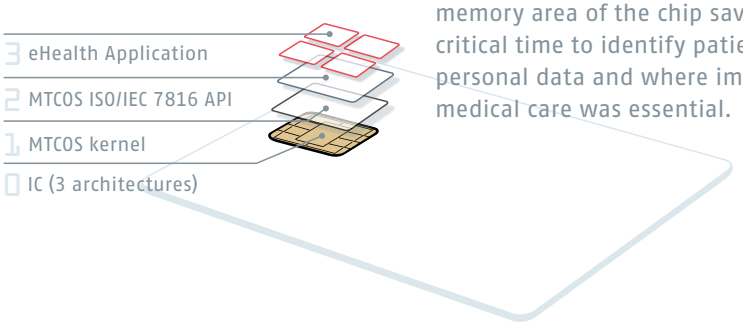
Chip solutions for secure patient data cards and health professional cards.

MTCOS®
eHEALTH

High security system on chip solutions for electronic health 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® & eHealth

MTCOS® eHealth is used in one of the largest microprocessor based health card projects in Central Europe as well as several closed clinic networks worldwide. The smartcard chip and related automated processes significantly reduced administration costs and those caused by misuse. Emergency data stored in the secure memory area of the chip saved critical time to identify patients personal data and where immediate medical care was essential.

The incidence of fraud in health benefit claims is a significant issue for governments and healthcare enterprises today. Paper-based manual processes greatly increase the risk of human error which results in extensive avoidable costs to insurers, national health agencies, and healthcare providers. Too often, these processes result in substantial delays in referral, treatment, and reimbursement for insured patients. Modern smart card technology can help to reduce fraud and provide clean data for eligibility verification and claims processing.

MTCOS® & ID Data

patients personal data are securely stored in the chips memory. The data can be protected with an electronic signature guaranteeing integrity and authenticity.

MTCOS® & Admin Data

administration data are used by the issuing authority and contain information about the insurance, status, expiry date, etc.

MTCOS® & Emergency Data

accessible by authorized doctors only, the emergency data set contains immediately required informations such as blood group, allergies, immunization data, current medication, etc. The number of entries is only limited by the smart card IC available secure memory.

MTCOS® & Copy Protection

public key authentication makes copying of the health card impossible.

MTCOS® & Card2Card

the public key based Card2Card authentication mechanism ensures that only trusted entities can access the sensitive data on the card.

MTCOS® & Trusted Medic

simplifies the access to patient data information for certain trusted doctors (no PIN entry) selected by the patient.

MTCOS® & Privacy

the patient decides which data are accessible by the doctor. Individual access rights for all data on the chip can be easily configured.

MTCOS® & Signature

signature functions are used to authenticate card holders for web portal services.

TECHNOLOGICAL COMPETENCE AND RELIABILITY

Highest security by modern cryptographic encryption.

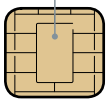
Maximum flexibility in semiconductor support.

Large functional range.

Many years of experience.

Standard solutions and customer specific development.

Independent.



MTCOS®
eHealth
Chip

- Holder data
- Administration data
- Emergency data

- 3DES & AES Cryptography
- RSA Cryptography
- Elliptic Curve Cryptography

- Card2Card authentication
- Trusted medic
- Copy protection

- Certificates
- Digital signature

1 **Flexibility**
Individual configuration of the patients personal data, administrative data, emergency data and related access rights.

2 **Project specific customization**
Possibility to add new commands, cryptographic algorithms and new security mechanisms.

3 **Extensibility**
Possibility to add additional applications. Post-issuance personalization may be used to securely add or update patient information or update card services.

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 21549. Open design free of third party rights and license costs.

INDIVIDUAL CONFIGURATION

Our core expertise covers high security 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 health card personalization and manufacturing infrastructure.

MTCOS® & standards:

- ISO / IEC 7816 – 3,4,6,8,9,15
- CEN 14890, CEN 15480, PKCS#15
- SHA-1 and – 2 support
- ISO / IEC 21549
- ISO / IEC 14443 Type A or B

MTCOS® & personalization:

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

MTCOS® & latest eHealth masks:

- 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**

3 **VARIETY OF CRYPTOGRAPHIC PROCEDURES AND SECURITY LEVELS**

4 **MULTIPLE REQUIREMENTS**

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 at the 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 comprehensively security tested and certified. On request we also develop project specific masks.

MTCOS® supports a variety of cryptographic methods such as Elliptic Curves, RSA, 3DES and AES with key lengths meeting present and future security demands. Further customer specific cryptographic procedures can be loaded securely in initialization phase.

MTCOS® is available with predefined or customized setups for patient data cards as well as health professional cards both with built-in signature and PKI authentication features.

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

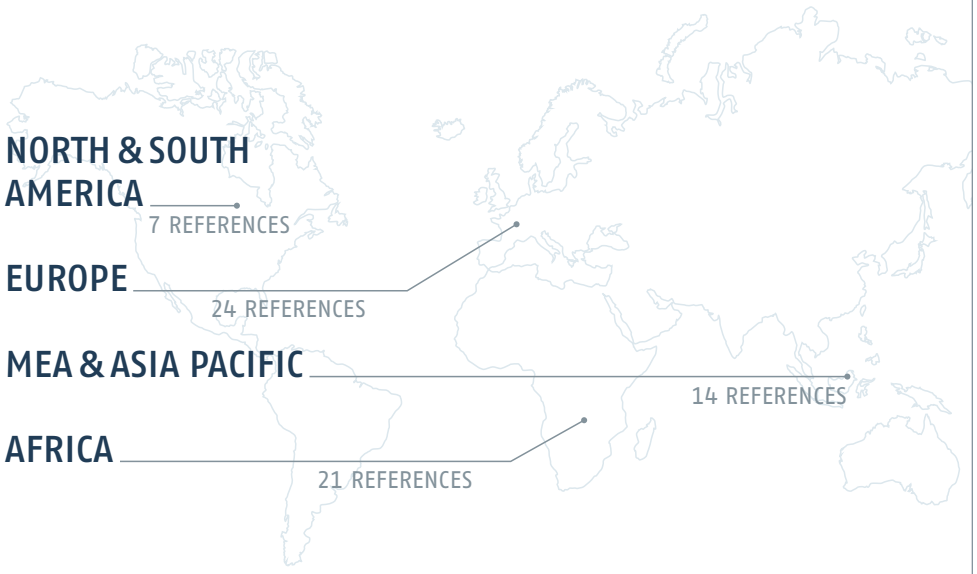
MTCOS® eRESIDENCE PERMIT

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