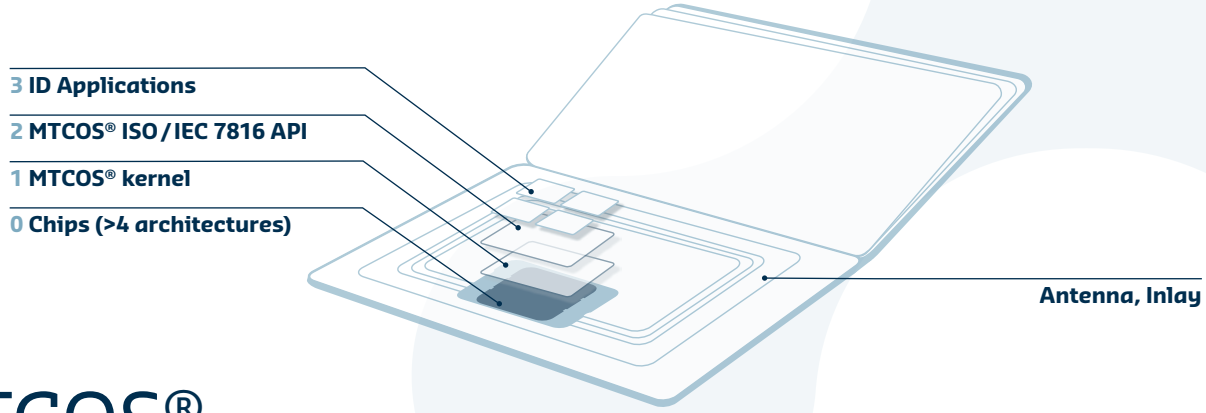
MASKTECH
DNA for ID solutions

MTCOS®
ePassport

Secure and platform-independent application 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.

Globalisation, economic growth in the Global South and the rise of migration are all drivers for increasing air transport passenger numbers. Yet, responsible and safe travel in times of pandemics is a precondition before going back to normal. This new normal includes an even faster and unequivocal identification of travel document holders through (automated) border control systems and the attached management systems.

To guarantee an ultra-fast and simultaneously ultra-secure procurement at (automated) border control stations, MaskTech offers a platform-/chip-independent and globally proven ePassport application which stores, secures and manages the data saved on the chip of an electronic ID document. Like the coding system of DNA, MTCOS® secures the personal data of the document holder for an encrypted, wireless transmission and guarantees a unique and swift identification at border control stations. In only a few seconds, MTCOS® verifies whether the (automated) border control system is allowed to have access to the personal and/or biometric data of the document holder. If so, MTCOS® encrypts this data with strong session keys for messaging and then sends it to the system.

Security & Support in every phase

Challenges to be met – 4 key points

1 Individual and generic personalization infrastructures
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.

2 Customer-specific features certified by Common Criteria
MTCOS® can be upgraded at customer's request during the passport production life cycle. Individual changes are loaded fully encrypted during the OS setup by using a Common Criteria-certified loading mechanism.

3 Variety of cryptographic algorithms, crypto migration
MTCOS® supports a variety of cryptographic protocols. 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.

4 Multiple configurations
MTCOS® can be configured to meet every ICAO/EU requirement, depending on our customers choice.

Individual **Configuration**

MTCOS® and latest ePassport masks

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.

MTCOS® is a chip-independent multi-application operating system – ready to be integrated into any ePassport personalization and manufacturing infrastructure.

MTCOS® PRO
MTCOS® & Latest MTCOS® PRO ePassport masks:

- **IFX SLE78 CLFX series** (MTCOS® PRO V2.5, EAL5+)
- **IFX SLE37 CLFX series** (MTCOS® PRO V2.5, EAL5+)
- **NXP P71D352** (MTCOS® PRO V2.5, EAL5+)
- **STM ST31G480** (MTCOS® PRO V2.5, EAL5+)

Flexibility
In an individual configuration, security protocols can be chosen from a list of proven protocols, in particular PA, BAC, SAC/PACE, AA and EAC.

Project-specific extensions
Possibility to add and adjust data group files with individual sizes, depending on national security standards.

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

Beyond the mere ePassport application

Flexible procurement, no additional dependencies

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

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

Our **Approach**

Technological competence & reliability
Full support for maximum security
in your individual project

We offer:

1 **Full independence** through triple sourcing – MTCOS® is EAL5+ certified on chips from three different hardware manufacturers.

2 We have been keeping up with ***all* interoperability and performance tests** in the industry to keep our products ahead of others.

3 **MTCOS® is an all-inclusive package:** Already included functionalities like LDS 2.0 can be activated at a later point in time.

4 **Our experience is your benefit:** We suggest or jointly develop the best suitable ePassport layout (data structure) for your individual project.

5 **Full flexibility and interoperability:** No matter which security chip, delivery form, design, antenna, inlay, data page, eBooklet... you choose, MTCOS® is ready for immediate integration (including already established personalization and manufacturing infrastructures).

MTCOS® applications **Overview**

MTCOS® eTachograph

MTCOS® eID

MTCOS® eResidence Permit

MTCOS® eDriving License

MTCOS® eHealth

MTCOS® ePayment

0011
1001

MTCOS® Customised

Checklist for **ePassport projects**

Apart from meeting internalional standards for electronic travel documents, MTCOS® supports a variety of cryptographic protocols with key lengths meeting present and future security demands.

MTCOS® & Passive Authentication
The data are protected with an electronic signature guaranteeing integrity and authenticity.

MTCOS® & Basic Access Control (BAC)
The Basic Access Protocol protects personal passport holder data against unauthorized reading.

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

MTCOS® & Extended Access Control (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 current security mechanisms.

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

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.

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 15480/Common Criteria EAL5+

MTCOS® & Personalization:

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

MTCOS® & Cryptographic protocols:

- 3DES cryptography
- AES cryptography
- RSA cryptography
- Elliptic-curve cryptography
- Anti-skimming features

About **MaskTech**

MaskTech is an independent company specialized in the development of high-security card operating systems. We provide MTCOS®, our MaskTech operating system, and various included applications for the electronic document and authentication market as license or as a chip and OS package.

Ever since our first ICAO-compliant application in 2004 to the implementation of the latest LDS 2.0 specification, we always work enthusiastically to provide our customers the safest and fastest electronic document solution on the market. Founded in 2002, MaskTech has gained an outstanding reputation for innovation and state-of-the-art technology in the electronic documents sector. Due to many years of experience and our excellent network in every step of the ePassport production and issuance chain, we can meet our clients' specifications, adding know-how to their portfolio if necessary.

Our product range includes generic and customized applications for chips of the leading security semiconductor manufacturers as well as security certification services. To date, MTCOS® protects more than 400 million eDocuments around the globe. The independent company has its headquarters in Nuernberg, Germany.

MaskTech **Testimonials**

MTCOS® is one of the most frequently used smartcard operating systems for eID documents. More than 65 countries worldwide have issued their ID and travel documents with MaskTech's secure OS.

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

Visit us on
masktech.de

MaskTech GmbH · Headquarters
Nordostpark 45
90411 Nuernberg · Germany
Phone +49 911 95 51 49-0
Fax +49 911 95 51 49-7
E-Mail info@masktech.de

MaskTech GmbH · Support
Bahnhofstrasse 13
87435 Kempten · Germany
Phone +49 911 95 51 49-0
Fax +49 831 51 21 077-1
E-Mail support@masktech.de

Rev. 3.0, November 2022