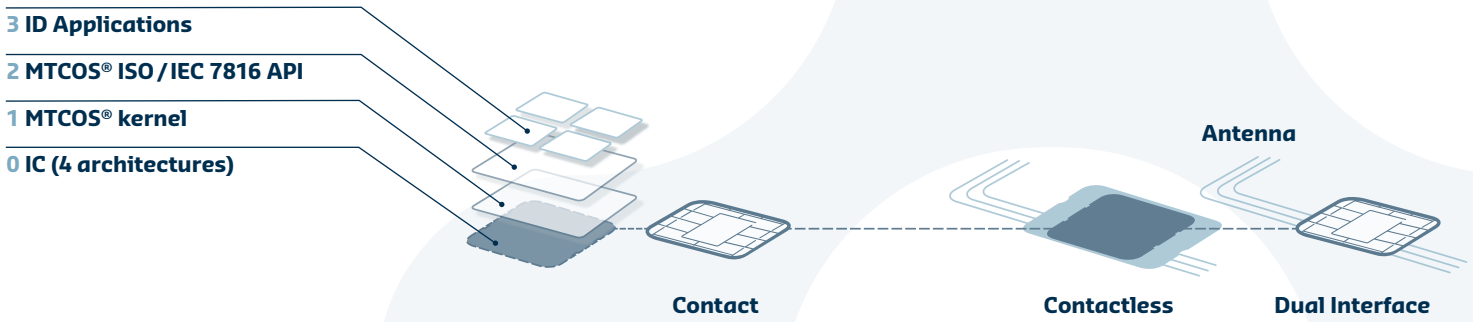
MASKTECH
DNA for ID solutions

MTCOS®
national ID

**Cryptographic-contact &
contactless-biometric ID**

High security/Common Criteria-certified
application for national ID cards.



MTCOS® **eID**

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

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 lifecycle features are available for new applications that may be added securely during or after issuance. The eID can act as interoperable travel document and enables access to eGovernment services.

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 attached 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.

To guarantee an ultra-fast and simultaneously ultra-secure procurement at (automated) border control stations, MaskTech offers a platform-/chip-independent and globally prove eID application which stores, secures and manages the data saved on the chip of an electronic ID document.

Security & Support in every phase

Challenges to be met – 4 key points

1 Particular personalization infrastructures
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.

2 Customer-specific features certified by Common Criteria
MTCOS® can be upgraded at customer's request during the eID 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 applications
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-installed applications include ICAO, e-signature, user and device authentication, certificates and many more.

Individual **Configuration**

MTCOS® and latest eID 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 eID personalization and manufacturing infrastructure.

MTCOS® PRO

- **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+)

MTCOS® FLEX ID

- **IFX SLC36** (MTCOS® FlexID V2.5)
- **STM ST31P450** (MTCOS® FlexID V2.5)

MTCOS® Flex ID
is our choice for cost efficient projec ts with adequate memory and data processing needs.

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.

Adding applications
A powerful ISO/IEC multi-application 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.

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.

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-ins is protected by the chip's hardware MMU.

Beyond the mere eID 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 can be activated at a later point in time.

4 **Our experience is your benefit:** We suggest or jointly develop the best suitable eID 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® ePassport

MTCOS® eResidence Permit

MTCOS® eDriving License

MTCOS® eHealth

MTCOS® ePayment

MTCOS® Customised

Checklist for **eID projects**

Contact | Contactless | Dual Interface

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

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

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.

MTCOS® & Standards:

- ISO/IEC 7816 - 3, 4, 6, 8, 9, 15, eIDAS
- 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® & Cryptographic protocols:

- Passive Authentication
- Basic Access Protection
- Active Authentication
- Extended Access Control
- 3DES cryptography
- AES cryptography
- RSA cryptography
- Elliptic-curve cryptography
- Anti-skimming features
- Electronic signature
- Knowledge based user authentication
- Identification services
- Client/Server authentication
- Supplemental Access Control

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 eID 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