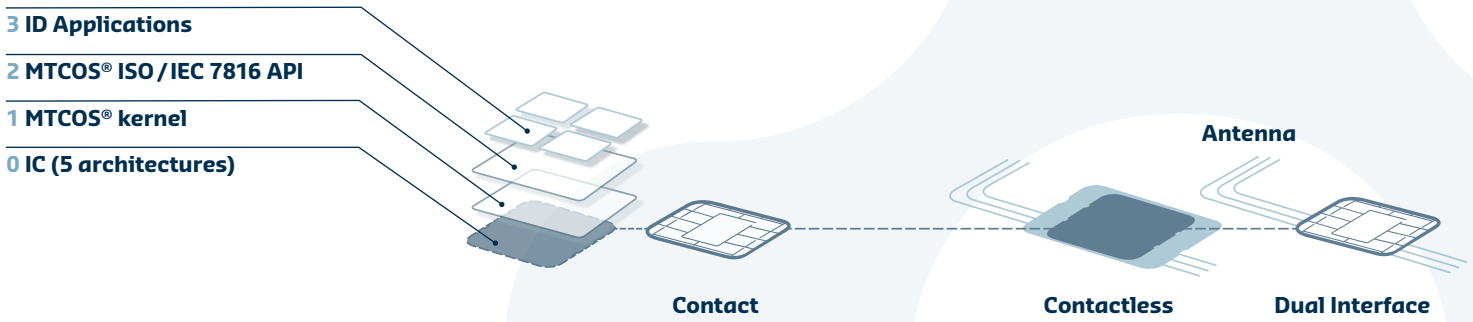
MASKTECH
DNA for ID solutions

# MTCOS®
# eDriving License

**The high performance application for eDriving Licenses**

ISO/IEC 18013
EU Commission Directive 383/2012




# MTCOS® eDriving License

## High security application for electronic driving licenses.

**MTCOS® with built-in eDriving License application has been rolled out in several large volume national projects and with several million documents in circulation. For a cost effective and flexible procurement process of all further system components, the documents are strictly designed according to the ISO/IEC 18013 standard.**

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. 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, MaskTech offers a platform-/chip-independent and globally proven eDriving License application which stores, secures and manages the data saved on the chip of an electronic driving license.

# 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 documents. All data communication is completely encrypted. Unauthorized access is prevented by transport keys.

**2 Customer-specific features**
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 procedures and security levels**
MTCOS® supports a variety of cryptographic protocols. Further customer specific crypto procedures can be loaded securely in initialization phase. On request we develop project-specific masks, if required with Common Criteria certification.

**4 Multiple configurations**
MTCOS® can be configured to meet ISO/IEC 18013 configuration, depending on our customers choice.

# Individual **Configuration**

## MTCOS® eDriving License 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 eDriving License 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 projects 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.

**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 eDriving License application

Product procurement, product dependancies

**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 eDriving License 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®** eID

**MTCOS®** eHealth

**MTCOS®** ePayment

**MTCOS®** Customised

# Checklist for **eDL 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 driving license 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® & BAP**
The Basic Access Protection mechanism (BAP) protects personal driving license holder data against unauthorized reading attempts and prevents skimming as well as eavesdropping by encrypting the communication between chip and terminal.

**MTCOS® & AA**
Active Authentication (AA) ensures that the driving license is not a copy of another driving license.

**MTCOS® & EAC/EAP**
Fingerprints and other sensitive data may be stored on the driving license's chip. The Extended Access Control and Extended Access Protection procedures strongly secure these data against unauthorized reading and copying in addition to the basic protection mechanisms. Compared to EAC, EAP allows protecting up to 24 data groups.

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

**MTCOS® & Security**
MTCOS® implements a unique Anti-Skimming procedure to prevent the unauthorized reading of the eDriving License by brute-force attacks.

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

**MTCOS® & Standards:**

- ISO/IEC 7816 - 3, 4, 6, 8, 9, 15
- ISO/IEC 18013 – 1-4
- ISO/IEC 18013 - BAP Config 1 ... 4
- ISO/IEC 14443 Type A or B

**MTCOS® & Personalization:**

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

**MTCOS® & Cryptographic protocols:**

- Passive Authentication
- Basic Access Protection
- Active Authentication
- Extended Access Control
- Anti-skimming software
- Extended Access Protection
- SAC/PACE
- 3DES cryptography
- AES cryptography
- Global Platform
- RSA cryptography
- Elliptic-curve cryptography
- Data Privacy
- Support of all DGs

# 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 eDriving License 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