Secure ST solutions for identification

Focus MTCOS 2.5 roadmap

Agenda

1 MTCOS® Applications

2 Drivers for upgrading MTCOS®

3 MTCOS® Pro and Flex ID on ST chips

4 MTCOS® active features

5 Benefits of MTCOS® v 2.5

6 MTCOS® v 2.5 insight

7 About MASKTECH

8 MASKTECH in the value chain

9 Possible business models

10 MTCOS® JavaCard

MTCOS® Applications

- eHealth
- eTransport
- eVoting
- ePurse
- eVehicle Registration
- eDriving License

- ePassport
- eID
- eResidence Permit

- Customized/ other MTCOS applications on request

Drivers for upgrading MTCOS®

- Proactive/ongoing MASKTECH software development
- Compliance with ICAO, ISO and other evolving regulations
- Interaction with government customers (gov. personalization systems)
- Participation in international interoperability tests
- Interoperability with latest border control equipment, e.g. ABCs
- Participation in international working groups
- Feedback from chip manufacturers

MTCOS ® X

MTCOS® 2.5

MTCOS® 2.2

MTCOS® Pro and Flex ID on ST chips

MTCOS® v2.1 and v2.5: MTCOS® Flex ID is recommended for cost-efficient projects with limited memory and data processing needs

	MTCOS Pro	MTCOS Flex ID
MTCOS® 2.1	ST23YR80 ROM masked | MTCOS v2.1 | 75kB FS CC EAL 4+	
MTCOS® 2.5	ST31G480 FLASH | MTCOS v2.5 | 180 kB FS CC EAL 5+	NEW ST31P450 FLASH | MTCOS v2.5 | 150 kB FS

life.augmented

MASKTECH

MTCOS® active features 1/2

MTCOS® 2.5

MTCOS v2.2 +
PACE-ECDH-CAM | LDS2* |
VHBR (Very High Bit Rate) | Hidden Files

MTCOS® 2.2

MTCOS v2.1 +
PACE-ECDH-GM | AES up to 256 bit |
RSA up to 4096 bit

MTCOS® 2.1

MTCOS Base Features
BAC | Active Authentication | EAC-CA | EAC-TA |
Elliptic curves up to 512 Bit | RSA up to 3072 bit |
DH up to 2048 bit | SHA-1 up to -512

ICAO Standards

BAC	Basic Access Control
EAC	Extended Access Control
SAC	Supplemental Access Control
CA	Chip Authentication
TA	Terminal Authentication
PACE	Password Authenticated Connection Establishment
CAM	Chip Authentication Mapping

Cryptography

RSA	Rivest, Shamir and Adleman
DH	Diffie-Hellman
ECDH	Elliptic Curve Diffie-Hellman
AES	Advanced Encryption Standard
3DES	Triple Data Encryption Algorithm

(*) Prepared, awaiting final test specifications

MTCOS® active features 2/2

MTCOS v2.2

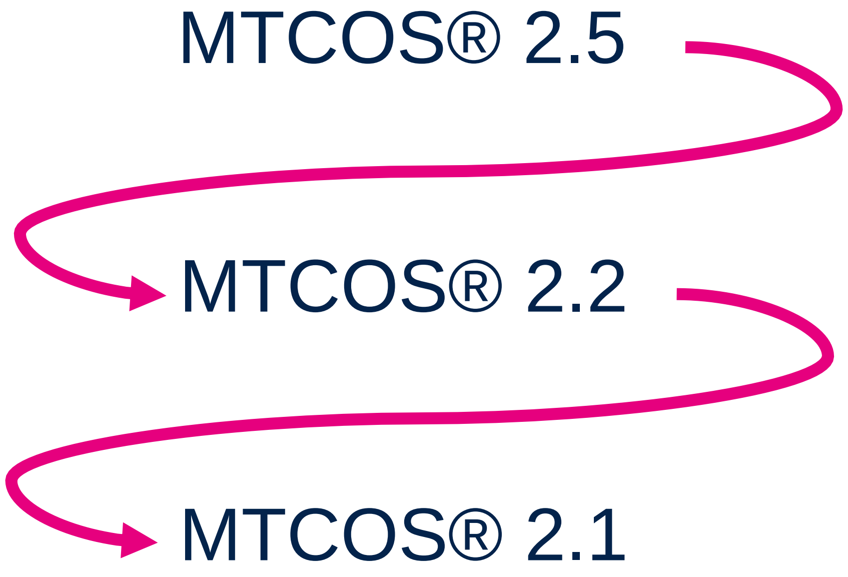
PACE-ECDH-CAM | LDS2* | VHBR (Very High Bit Rate) | Hidden Files

MTCOS v2.1

PACE-ECDH-GM | AES up to 256 bit | RSA up to 4096 bit

MTCOS Base Features

BAC | Active Authentication | EAC-CA | EAC-TA | Elliptic curves up to 512 bit | RSA up to 3072 bit | DH up to 2048 bit | SHA-1 up to -512



MTCOS® 2.5

MTCOS® 2.2

MTCOS® 2.1

All MTCOS® versions are backward-compatible

Benefits of MTCOS® v2.5

Features can be activated for all passports or specific classes of books (e.g. Diplomats & Officials vs. Tourist)

Added government-controlled functionality

- Invisible EAC, SAC, LDS2 and other data groups (without anybody knowing about these added functionalities)
- Hidden Files

Added government-controlled flexibility

- Any or all features can be turned on at any point in the future, e.g. change from BAC ePassport to EAC ePassport (only personalization has to be adjusted)
- No impact on book inventory

Testing

- Newly activated feature(s) can be tested with in-house ePassport covers in the standard production environment, e.g. for Interop Tests

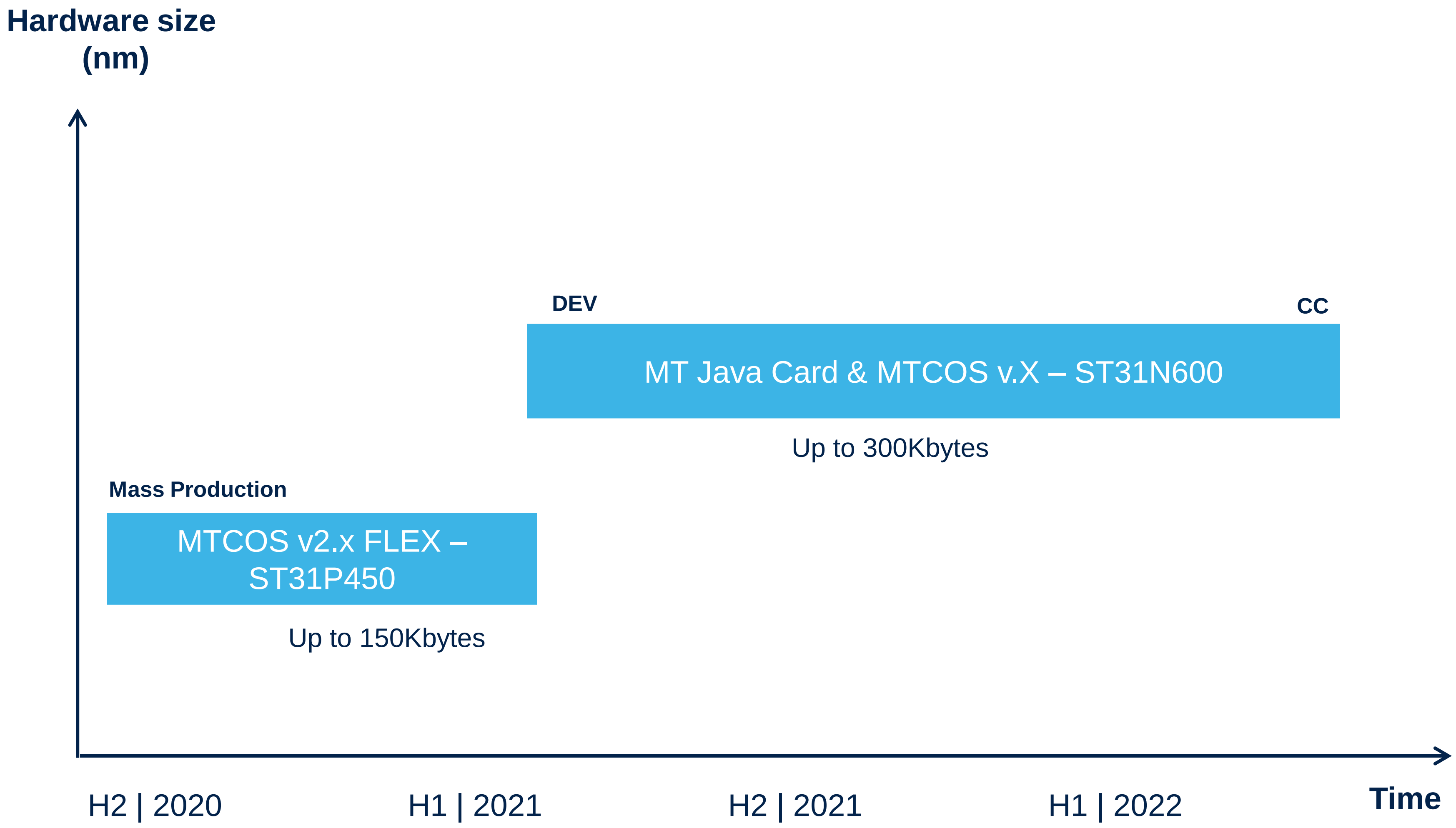
MTCOS® v2.5 insight

Recommended minimum chip size & performance data

	BAC	BAC + SAC	BAC + SAC + EAC	BAC + SAC + EAC + bio data[1]
Minimum chip size	64 Kbytes (36 Kbytes needed)	64 Kbytes (40 Kbytes needed)	80 Kbytes	140 Kbytes
MTCOS® V2.5 performance data	Write < 2 seconds	Write < 2 seconds	Write < 6 seconds	Write < 10 seconds[2]
	Read < 1 second	Read < 1.5 seconds	Read < 6 seconds	Read < 10 seconds

(1) Large biometric data, e.g. iris or fingerprint data
(2) LDS2 written in field (no impact on personalization time)

MTCOS® continuing future development on 40nm HW



Hardware size (nm)

DEV

CC

MT Java Card & MTCOS v.X – ST31N600

Up to 300Kbytes

Mass Production

MTCOS v2.x FLEX – ST31P450

Up to 150Kbytes

H2 | 2020

H1 | 2021

H2 | 2021

H1 | 2022

Time

DEV: Development start

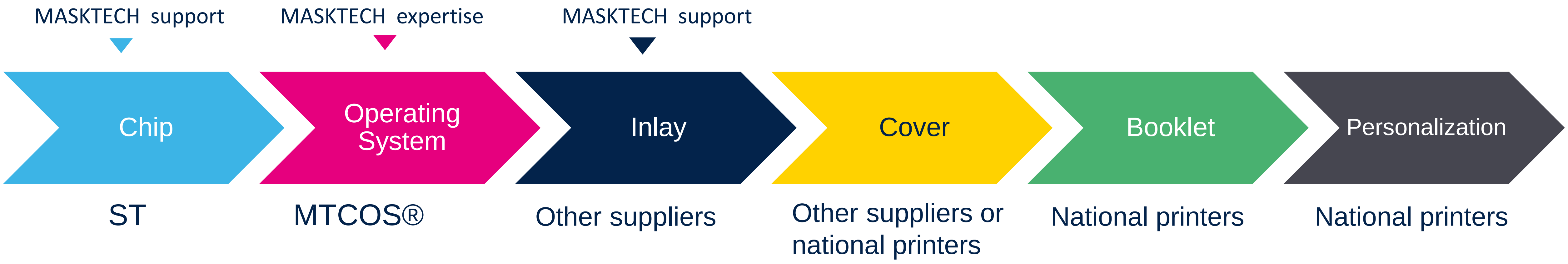
CC: CC certification expected

Under development

About MASKTECH

- Agile, responsive, proactive
- Independent, solely customer driven
- Guaranteed availability of OS for life of contract
- 50 government ePassport customers
  - > 250 million ePassports in use
- 350 million electronic MaskTech documents in circulation around the globe

MASKTECH in the value chain



MASKTECH support

MASKTECH expertise

MASKTECH support

Chip

Operating System

Inlay

Cover

Booklet

Personalization

ST

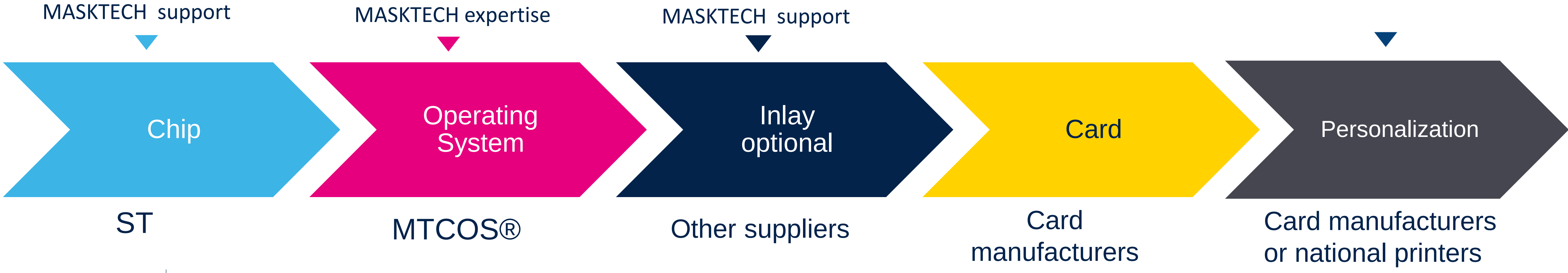
MTCOS®

Other suppliers

Other suppliers or national printers

National printers

National printers



MASKTECH support

MASKTECH expertise

MASKTECH support

Chip

Operating System

Inlay optional

Card

Personalization

ST

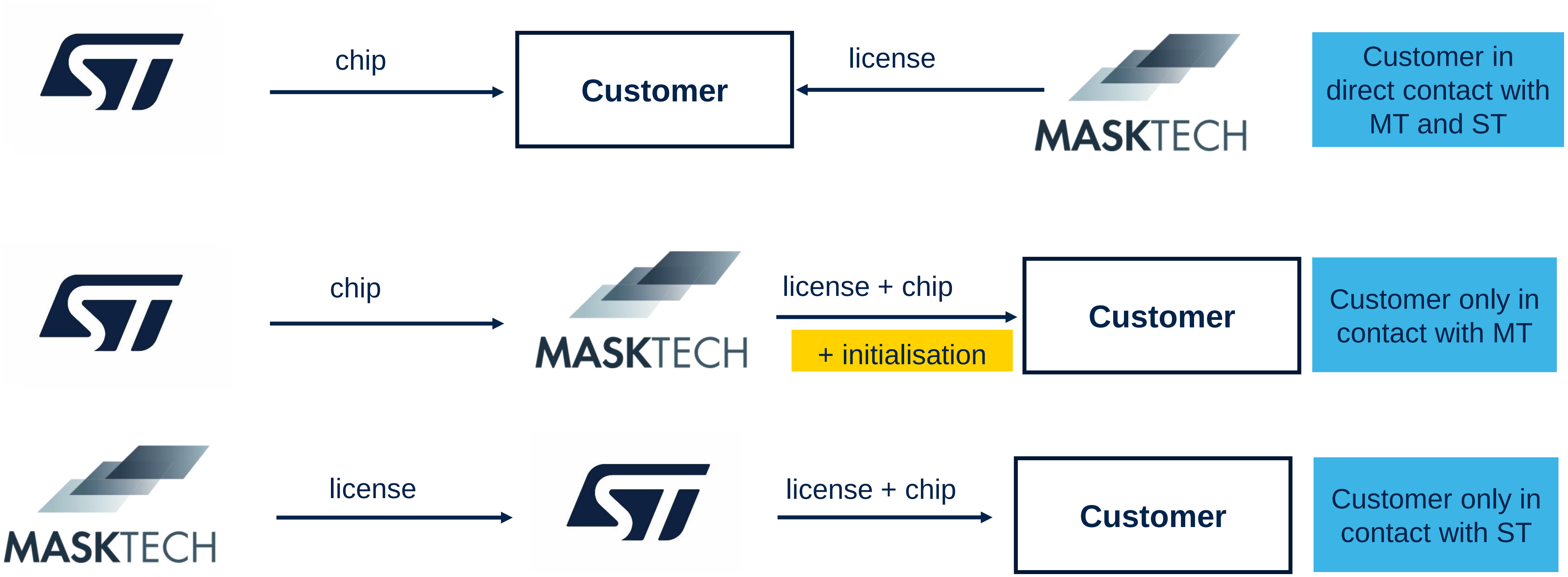
MTCOS®

Other suppliers

Card manufacturers

Card manufacturers or national printers

Possible business models



chip

Customer

license

Customer in direct contact with MT and ST

chip

license + chip

+ initialisation

Customer

Customer only in contact with MT

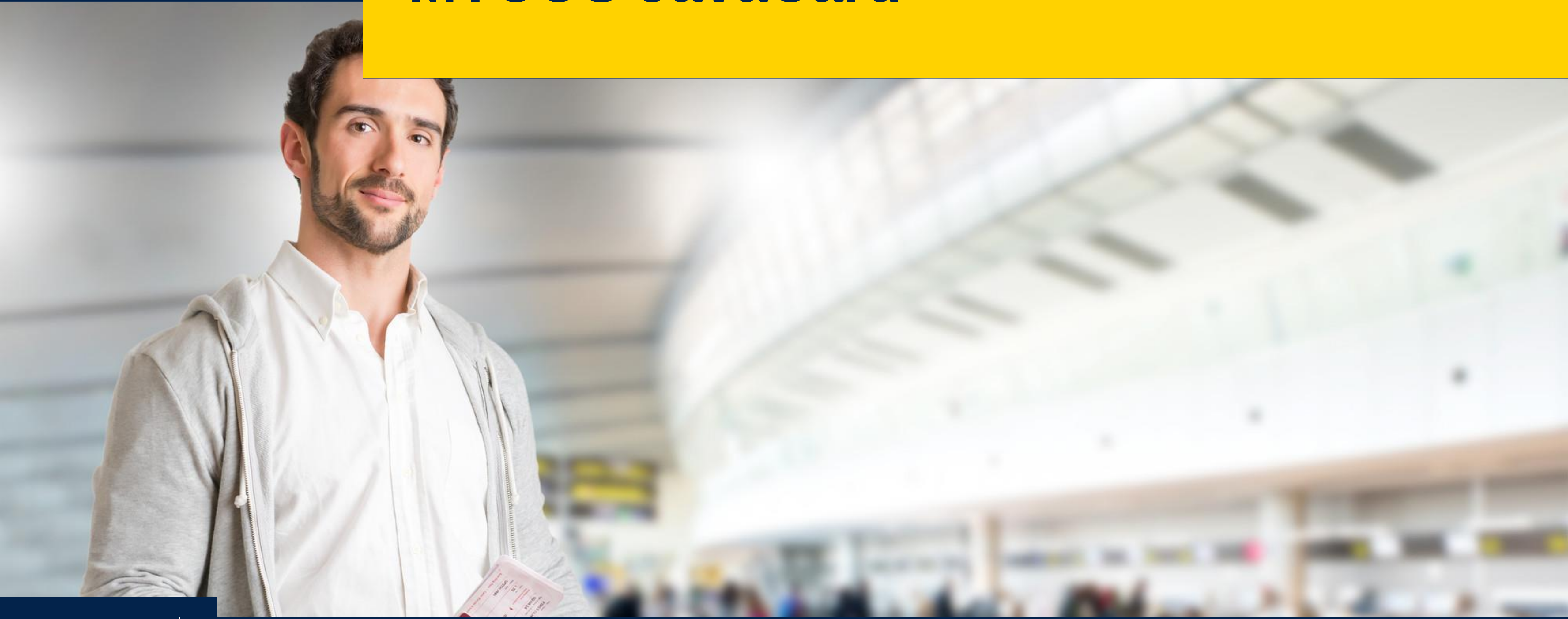
license

license + chip

Customer

Customer only in contact with ST

MTCOS JavaCard



life.augmented

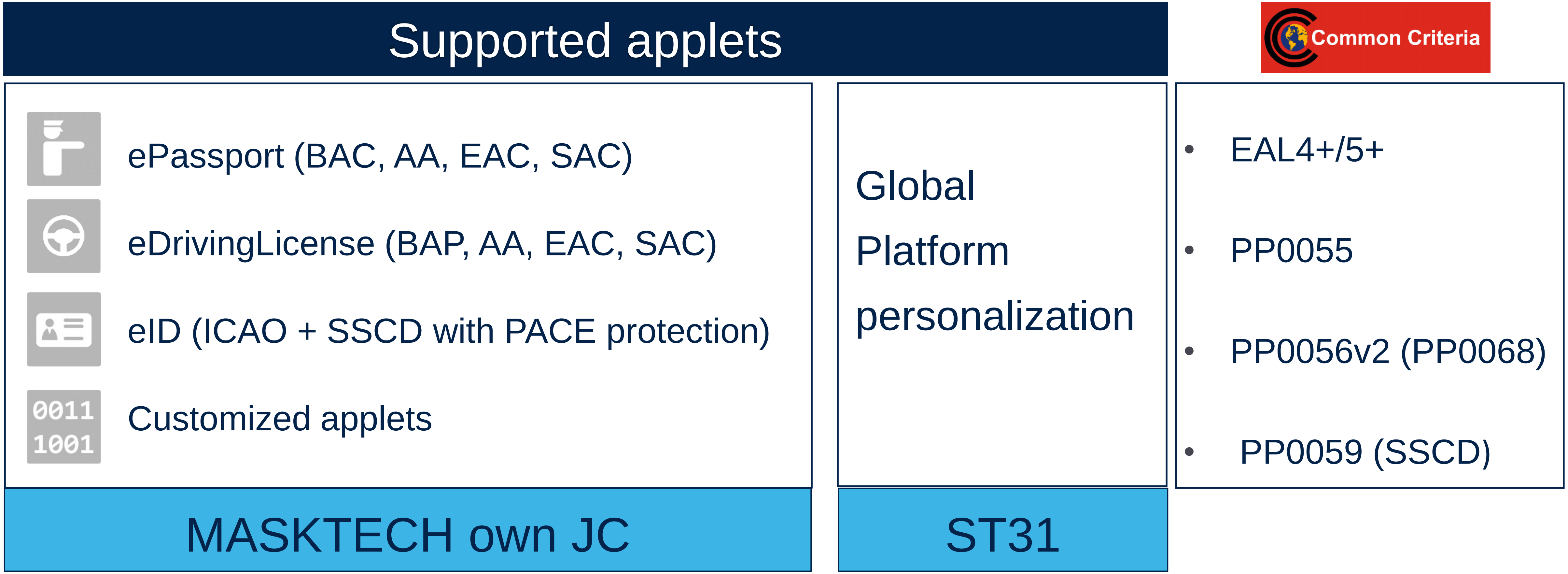
MASKTECH

ST Restricted

MASKTECH Java Card v 3.0.5

Platform & Feature Set
ST31N600 (ARM, 300kB Flash)
Java Card Classic Edition V3.0.5
MTCOS BIOS & Native API
Global Platform V 2.2.1 or higher (incl. eID extended packages)
Crypto Support for 3DES, AES, RSA, ECC
CC EAL5+
Applet Suite
ePassport (BAC, AA, EAC, SAC)
eDriving License (BAP, AA, EAC, SAC)
eID (eSign)
CC EAL4+/5+

MTCOS® Applet Suite



Supported applets

- ePassport (BAC, AA, EAC, SAC)
- eDrivingLicense (BAP, AA, EAC, SAC)
- eID (ICAO + SSCD with PACE protection)
- Customized applets

Global Platform personalization

MASKTECH own JC

ST31

Common Criteria

- EAL4+/5+
- PP0055
- PP0056v2 (PP0068)
- PP0059 (SSCD)

Thank you

life.augmented