THALES
Building a future we can all trust

JAVA CARD Forum

Digital Identity Applications on Secure Elements/Java Cards

JCF Webinar

OPEN

Agenda

Introduction

High level overview

- What is Digital Identity?
- User Privacy and Personal Data Protection

Recent Developments in Standardization space

- Enhanced Holder authentication, user consent, full user control,...

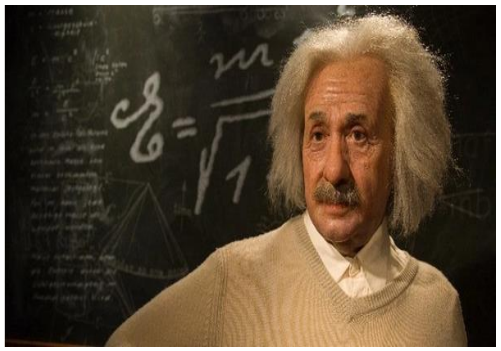
This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

What is identity?

Identity is what is left invariant, persists over time.







This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

What is Identity?

(photo cred: Individuality, The New Yorker June 2, 2014)

The qualities / characteristics that make them different from others.

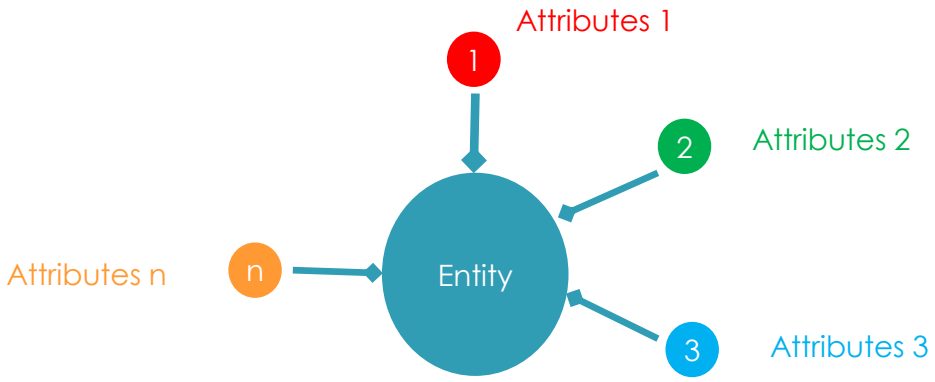
- Those characteristics can be born with, assigned, acquired overtime.

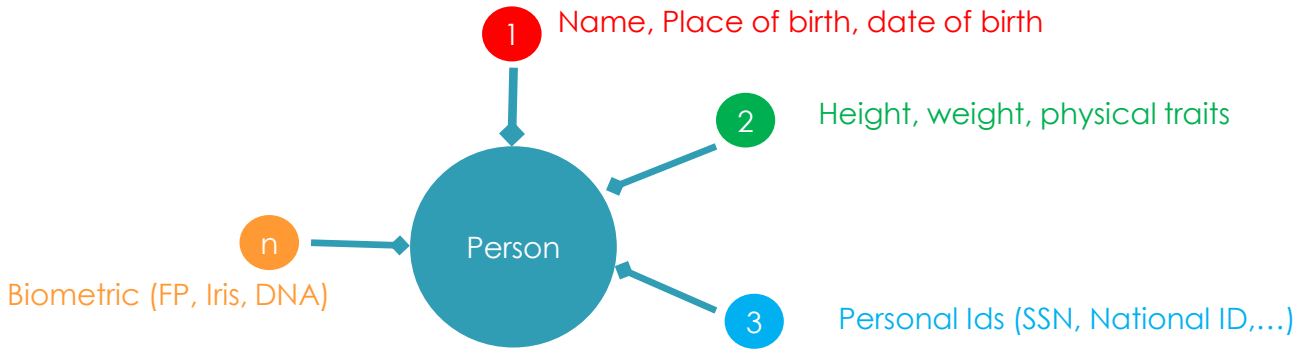
This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

What is Identity?

ITU definition

- A representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context.





OPEN

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

THALES
Building a future we can all trust

What is Digital identity?

The digital representation of an entity, detailed enough to make the individual distinguishable within the digital context.

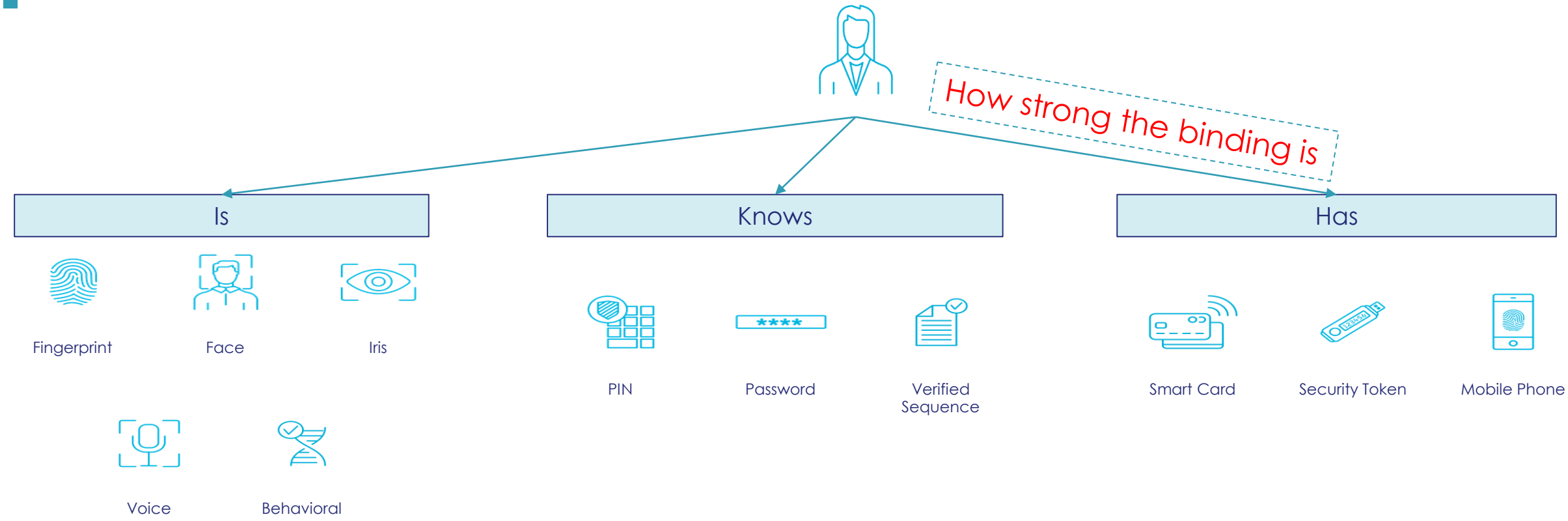
- Stored and exchanged with a remote entity electronically

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

What is Authentication?

Authentication: Is the process of proving that entity possesses and controls one or more registered authenticators

Common authentication factors are based on what someone …

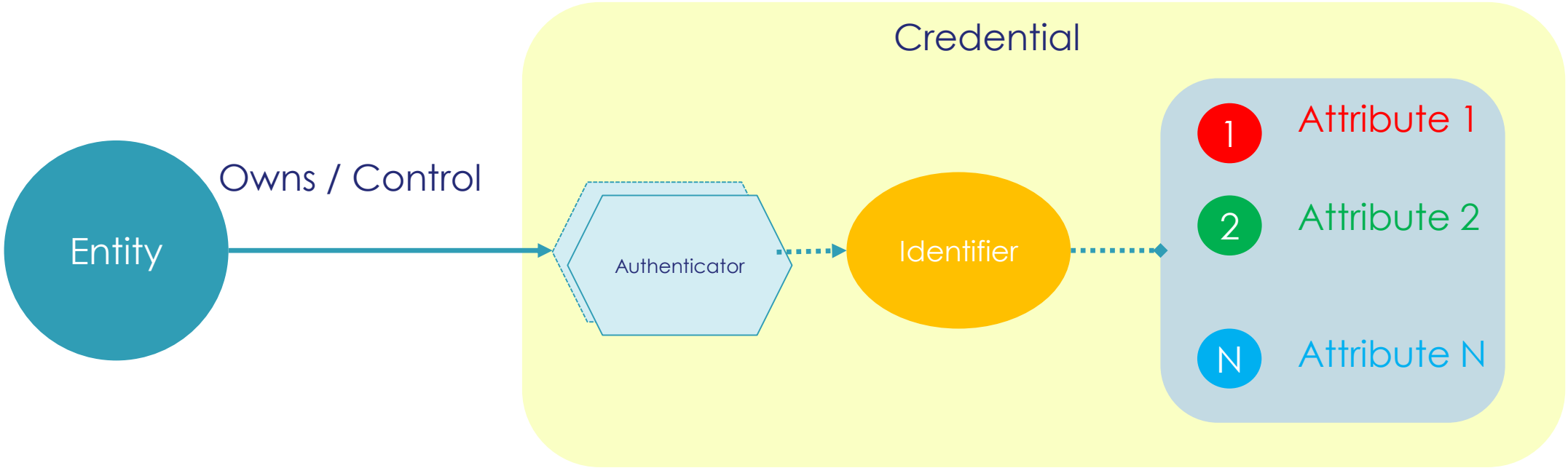


Source: McKinsey Global Institute analysis, these authentication factors are illustrative and not comprehensive

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

Credential: Binding of attributes to an entity

An object or data structure that authoritatively binds an identity—via an identifier or identifiers—and (optionally) additional attributes, to at least one authenticator possessed and controlled by a subscriber … NIST 800-63

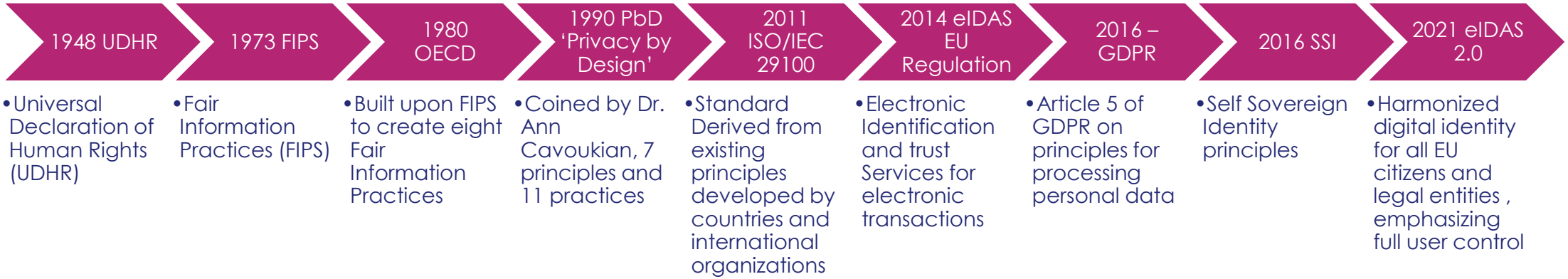


Credential can be used to assert identity by a person

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

User Privacy and Personal Data Protection

Privacy-and-security-by-design approach embodies a number of global standards and principles



Source: Privacy by Design, ISO/IEC 29100, and EU (2016).

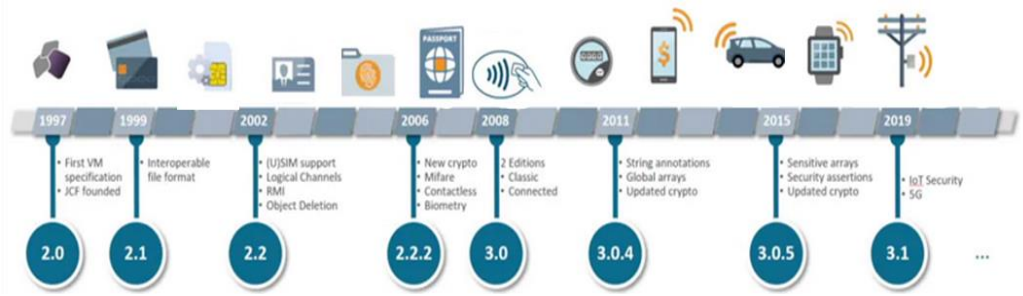
This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

Evolution of ID Documents

Paper -> Phot ID -> Plaststic -> Electronic ID -> Mobile / Biometric

Source : NYTimes , Charles de Saint-Mémin's United States passport, June 30, 1810

ISO/IEC JTC 7810 ID-1 card → ISO/IEC 7811 Magnetic Stripe → ISO/IEC 7501 ICAO Machine readable → ISO/IEC 7816 Integrated Chip Card – Smart Cards → ISO/IEC 14443 Contactless → ISO/IEC 18013-5 mDL → ISO/IEC FDIS 23220 mID



Source: Java Card Forum 25 Years of Java Card Evolution

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

THALES
Building a future we can all trust

THALES
Building a future we can all trust

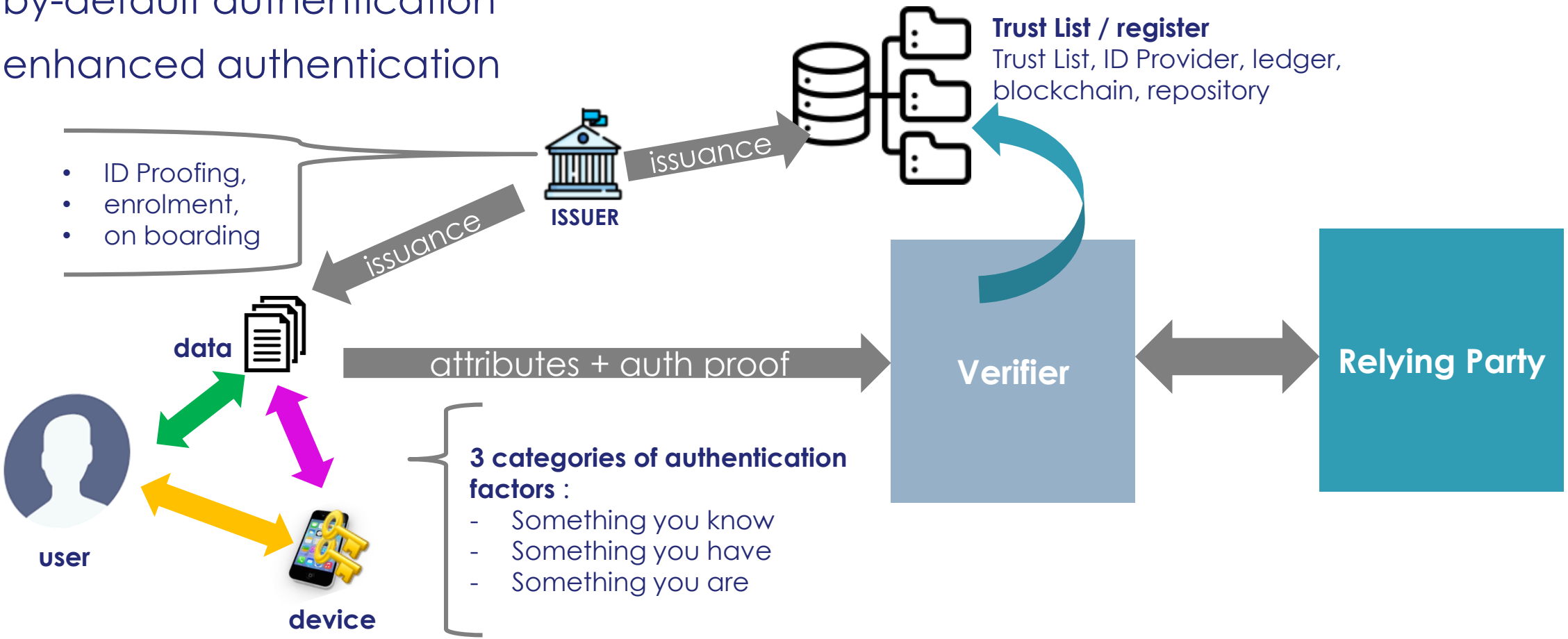
Recent Evolutions of Digital Identity

On-mobile holder authentication in eIDAS context

Identification & Authentication – Introduction : Landscape

multi-factor authentication

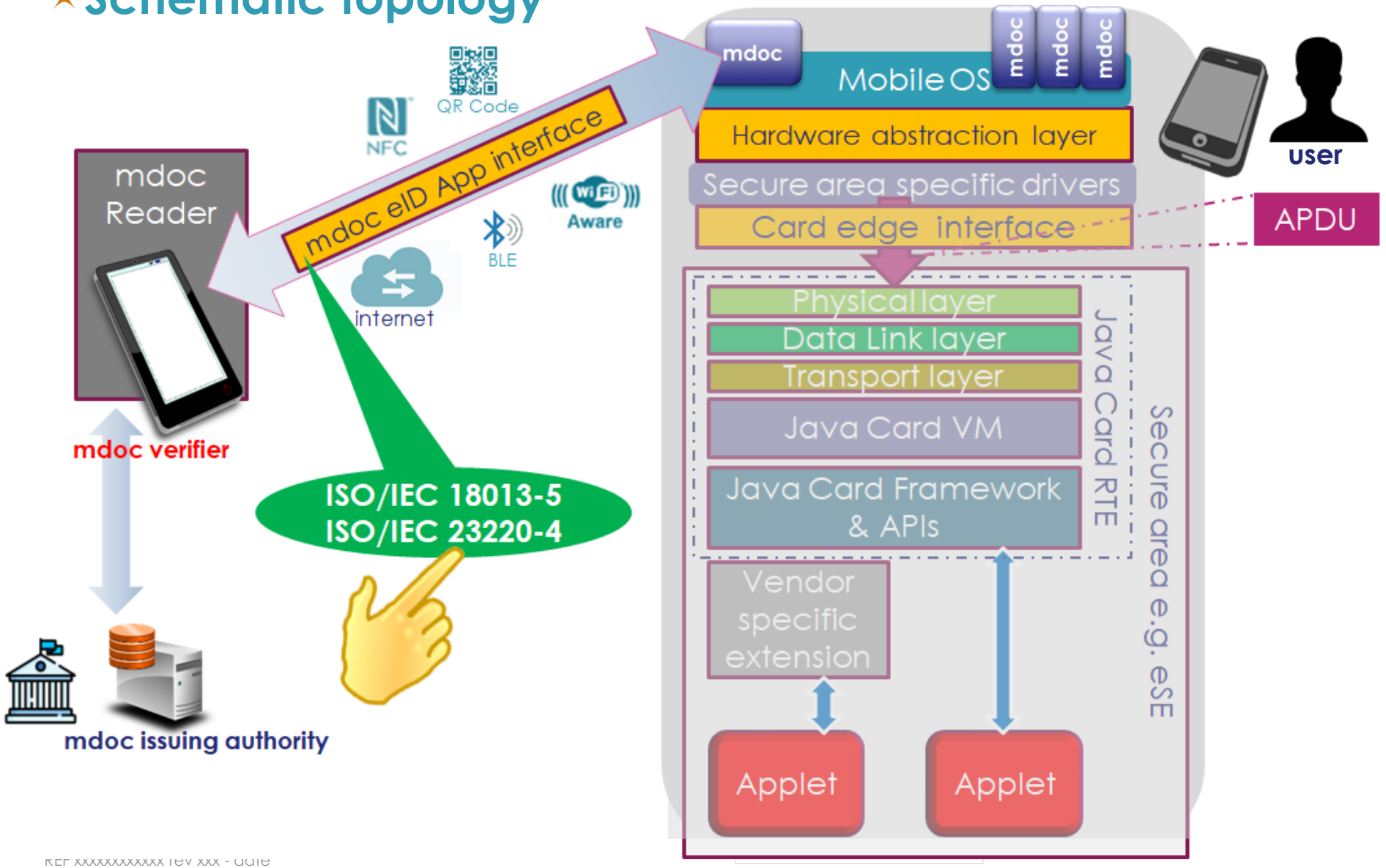
- by-default authentication
- enhanced authentication



This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

Main interfaces, with mdoc involvement

Schematic topology



This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

THALES
Building a future we can all trust

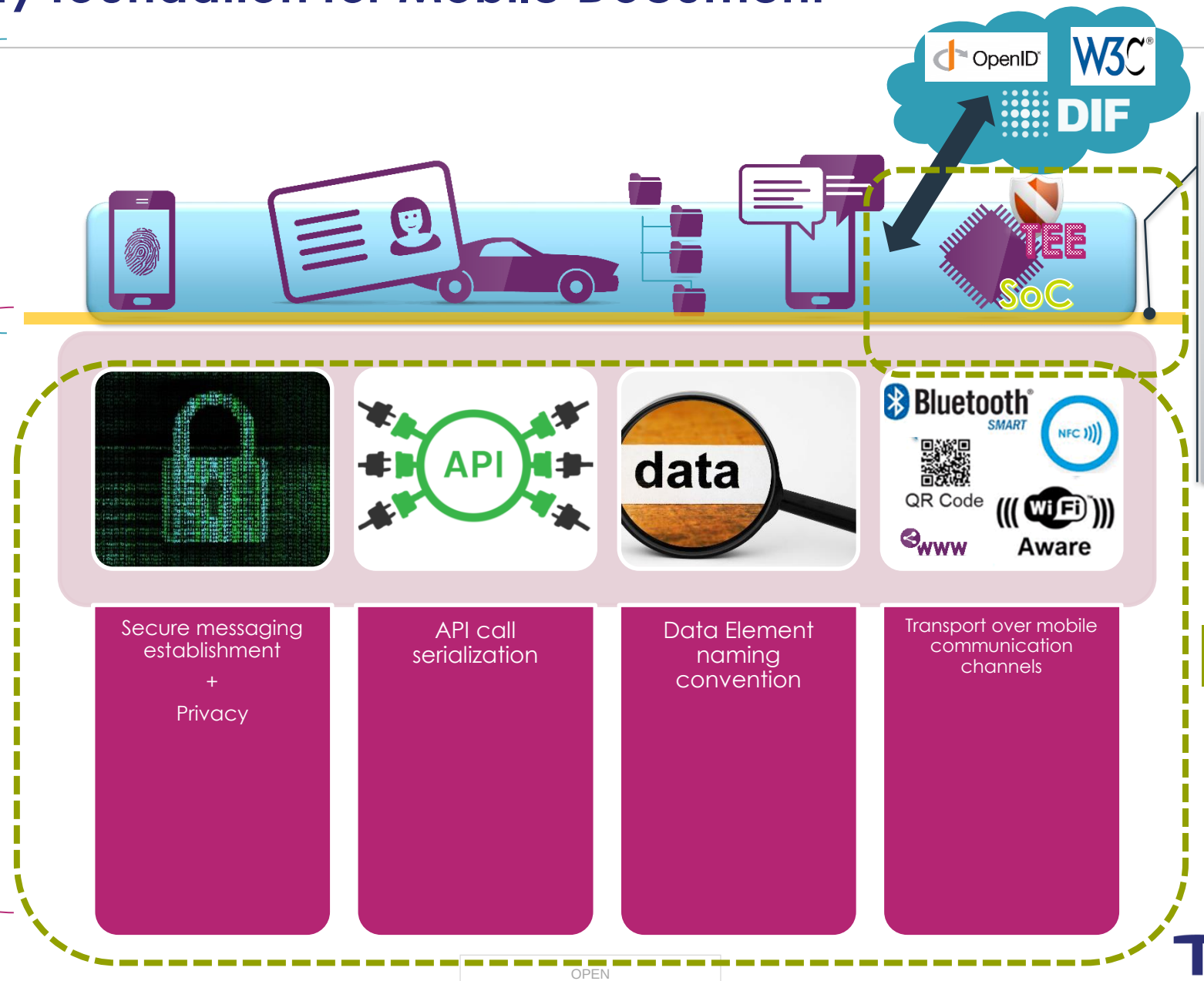
Interoperability foundation for Mobile Document

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

mDL versatility

Specified by ISO/IEC **23220** series

Specified by the standard ISO/IEC **18013-5**



mdoc eID App interface

abstraction layer for:

* the secure area,
* the data structure,
* the data storage
* data security policy

Wallet kernel

OPEN

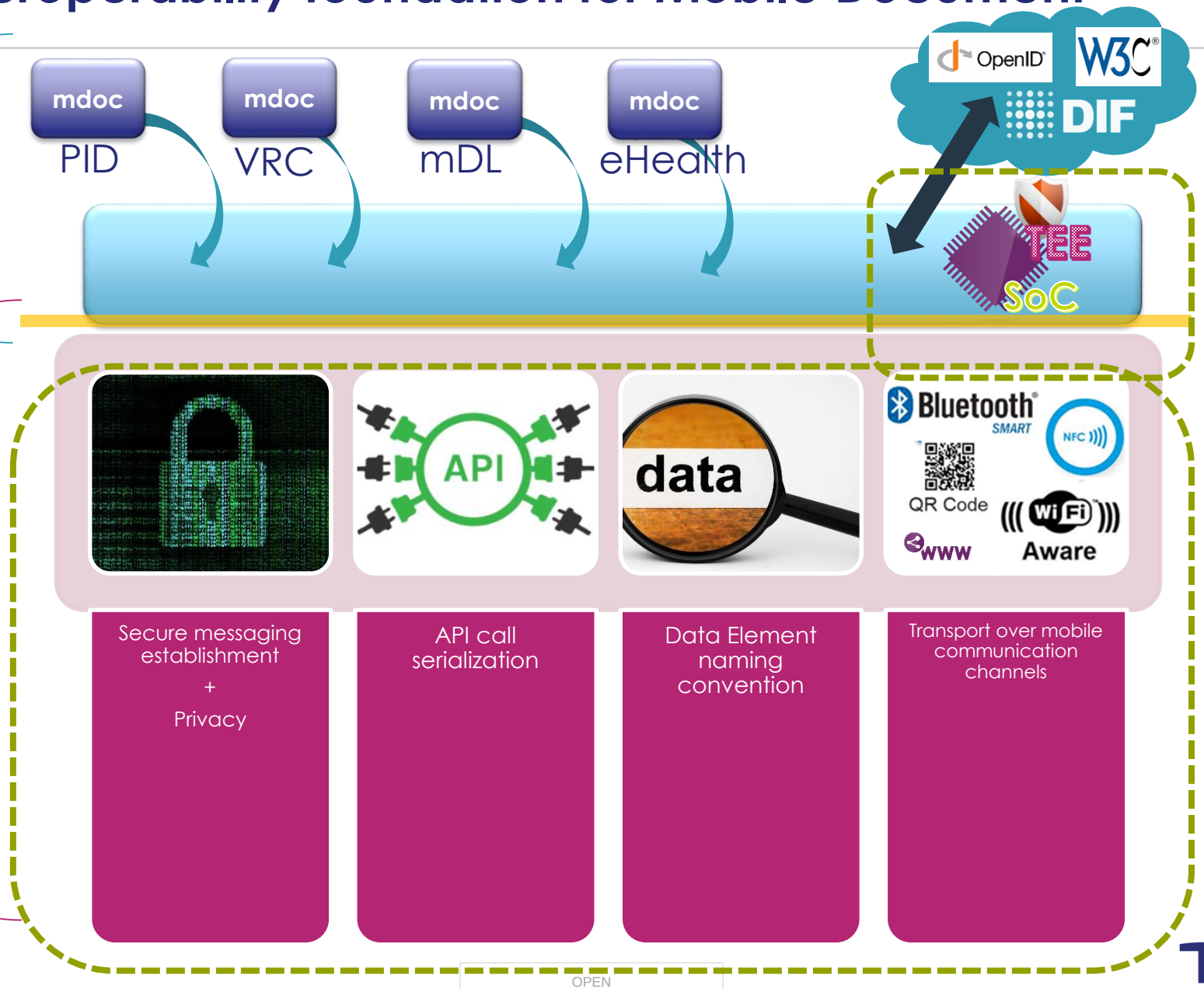
THALES
Building a future we can all trust

Reminder: Interoperability foundation for Mobile Document

mDL versatility

Specified by ISO/IEC **23220** series

Specified by the standard ISO/IEC **18013-5**



Wallet kernel

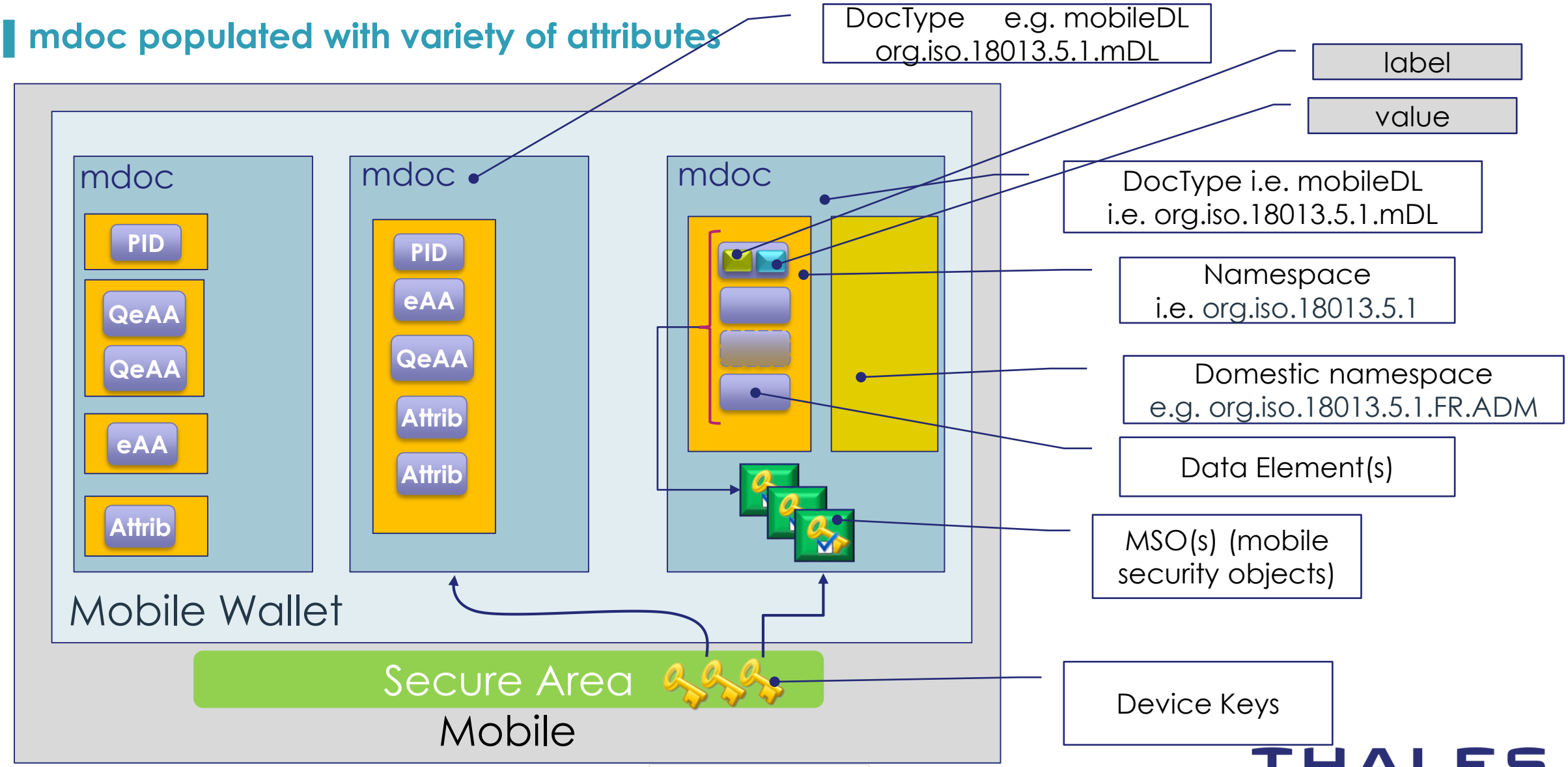
This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

OPEN

THALES
Building a future we can all trust

Focus on mdoc data structure : docType(s) + namespace(s)

mdoc populated with variety of attributes

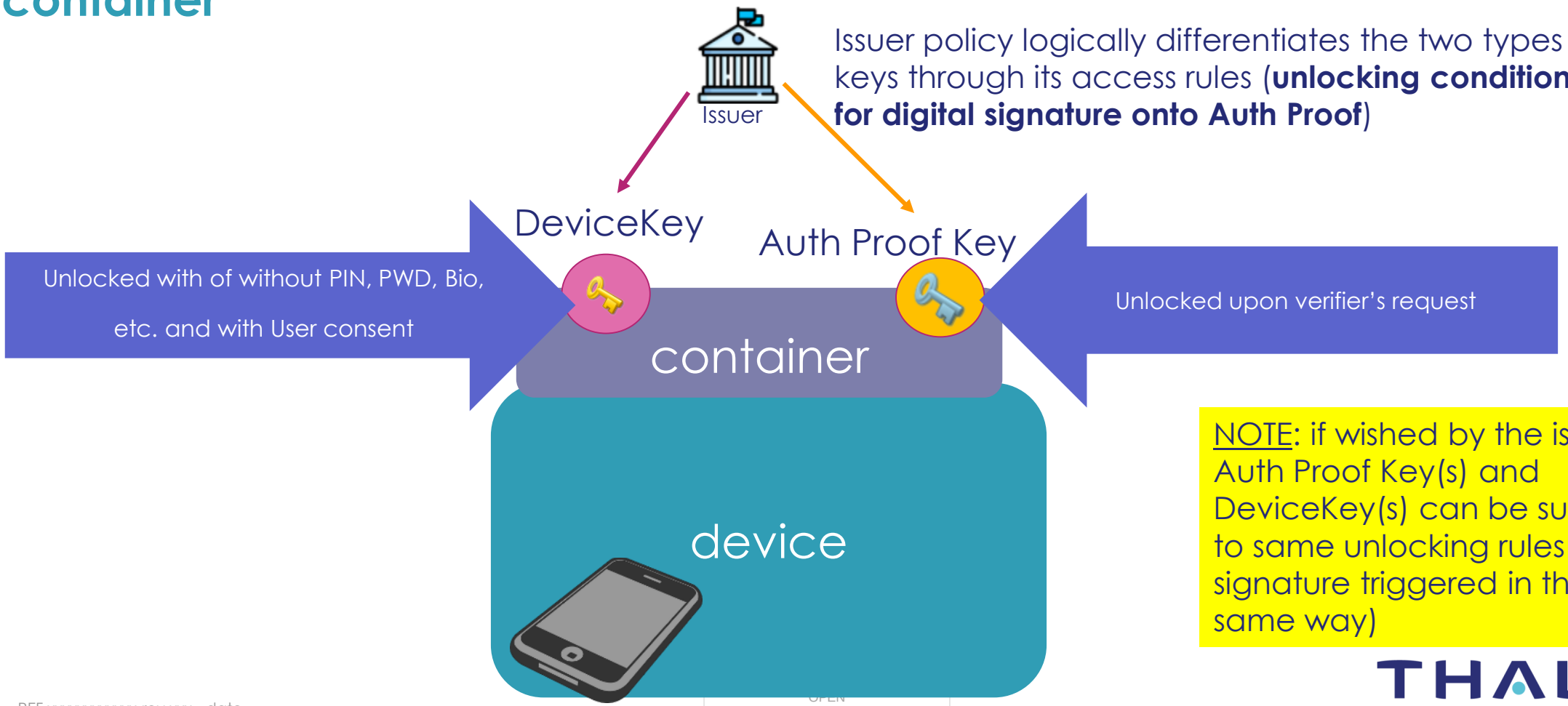


This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

Basic principles

Distinguishing DeviceKey from Authentication Proof Key

Authentication Proof Key and DeviceKey can be hosted in the same container



NOTE: if wished by the issuer, Auth Proof Key(s) and DeviceKey(s) can be subject to same unlocking rules (i.e. signature triggered in the same way)

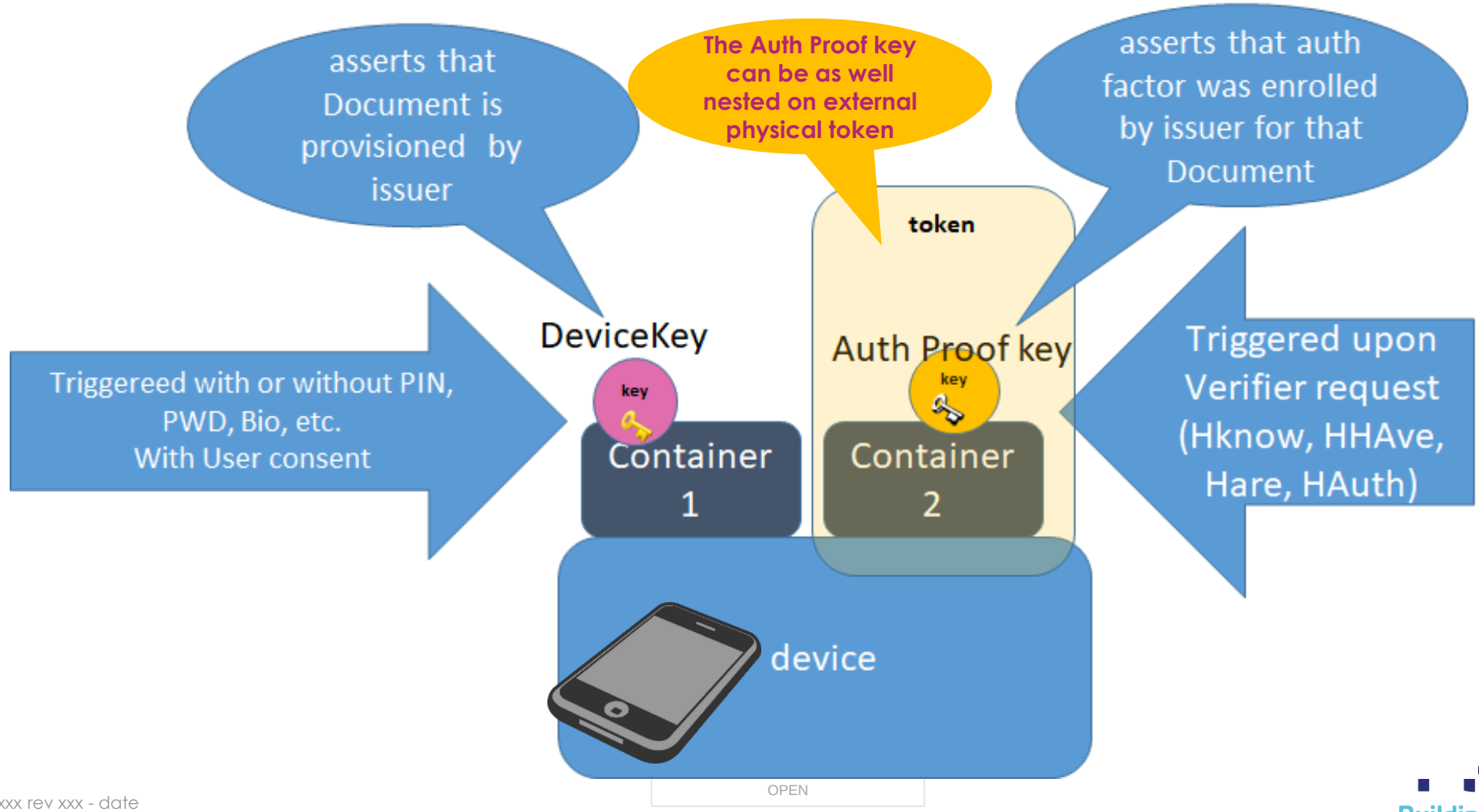
This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

THALES
Building a future we can all trust

Basic principles

Authentication Proof Key can as well be hosted in separate containers

- e.g. of containers: eID Card, SmartSD, eUICC, SIM, eSE , FIDO authenticator, PIV etc.



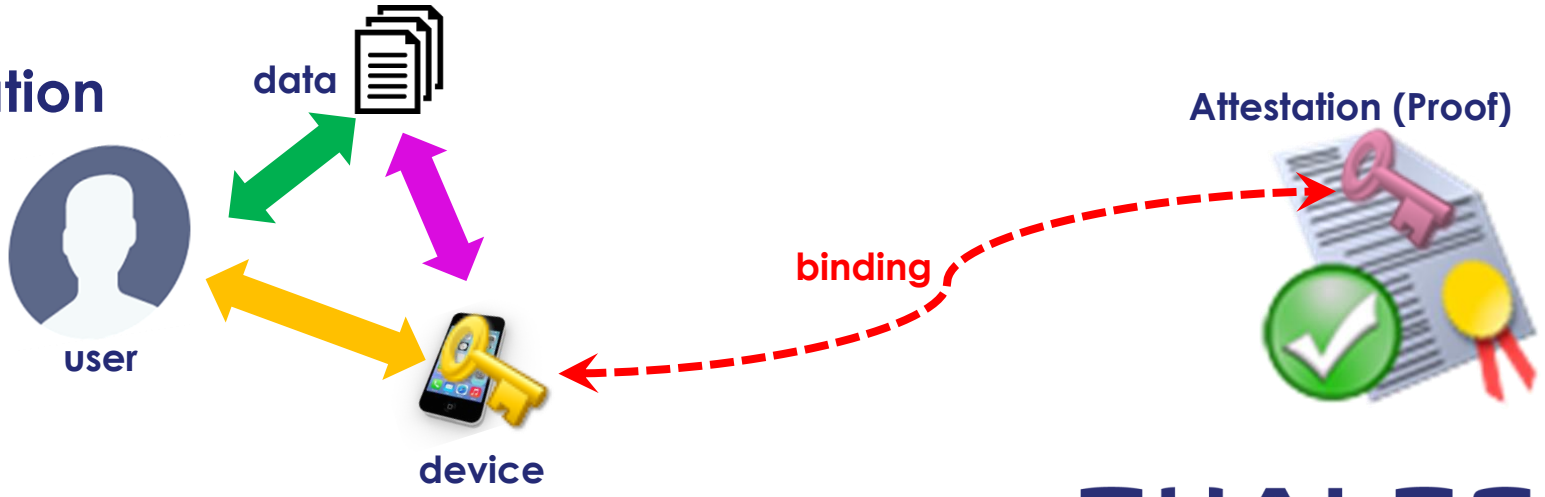
This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

Authentication at mdoc interface

looking at authentication with mdoc semantic

what are the requirements ?

- basically, verifier requests **data element(s)** from a dedicated **namespace** from within an **mdoc**
- a set of data elements to trigger **authentication**
  - « HAuth », « HAttest », « HAreAttest », « HHaveAttest », « HKnowAttest », ...
- authentication with either one of the 3 **authentication factors**, or a combination thereof
- possibly returning an **attestation**



This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

Authentication at mdoc interface

scenario examples

by-default authentication

Verifier Request

“HAuth”	Yes/No

mdoc Response

Attestation = Authentication proof

authentication with « something you are »

Verifier Request

“HAuth” + “HAreAttest”	Yes/No + Attestation

mdoc Response

authentication with « something you are » AND with « something you have »

Verifier Request

“HAuth” + “HAreAttest” + “HHAveAttest”	Yes/No + Attestation#1 + Attestation#2

mdoc Response

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

Authentication at mdoc interface

jurisdiction-dependent authentication

Verifier Request

"**specific attestation**"

e.g.
eIDAS attestation (QEAA),
NIST attestation,
Visa attestation,
GlobalPlatform attestation,
Country-specific attestation

Yes/No

+

attestation depending on jurisdiction

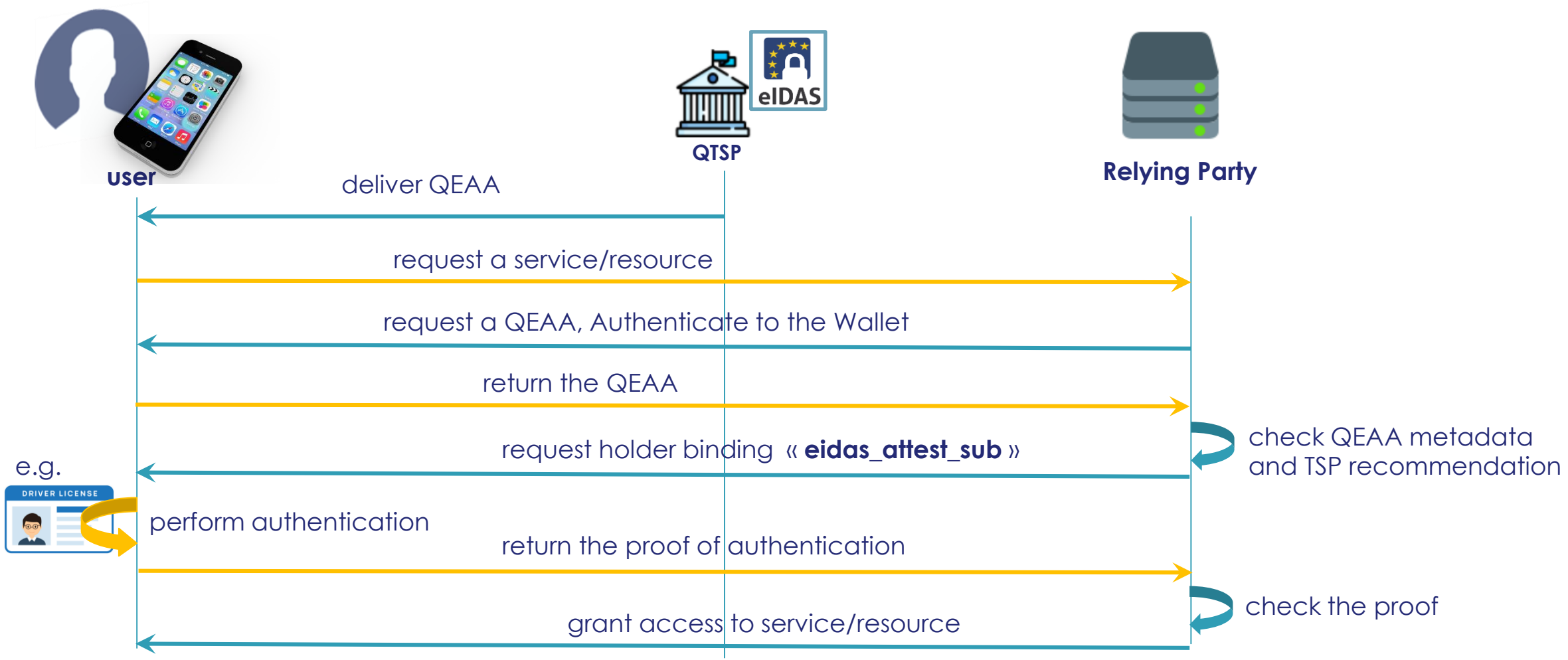
mdoc Response

"**eidas_attest_low**" or
"**eidas_attest_sub**" or
"**eidas_attest_high**"

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

Example of possible flow

may serve for QEAA and EAA



This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.

Thank You

END

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - © Thales 2020 All rights reserved.