Introduction to ISO/IEC 18013-5

5 October 2021 | W3C Credential Community Group

Arjan Geluk

Presenter

Arjan Geluk, CISA

Lead Principal Advisor, Identity Management & Security, UL

Leiden, The Netherlands

ISO Mobile Driving License Task Force leader

Special technical advisor to AAMVA's Joint mDL WG

arjan.geluk@ul.com

ICS › 35 › 35.240 › 35.240.15

ISO/IEC 18013-5:2021

Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application

ABSTRACT PREVIEW

This document establishes interface specifications for the implementation of a driving licence in association with a mobile device. This document specifies the interface between the mDL and mDL reader and the interface between the mDL reader and the issuing authority infrastructure. This document also enables parties other than the issuing authority (e.g. other issuing authorities, or mDL verifiers in other countries) to:

— use a machine to obtain the mDL data;

— tie the mDL to the mDL holder;

— authenticate the origin of the mDL data;

— verify the integrity of the mDL data.

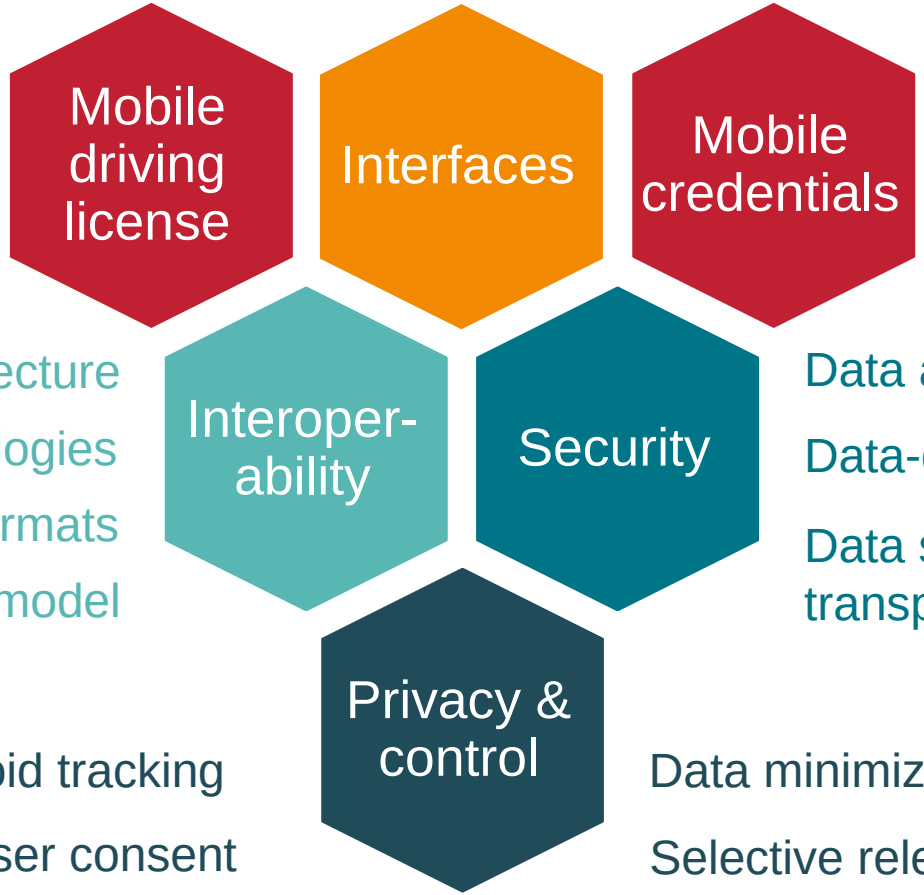
The following items are out of scope for this document:

— how mDL holder consent to share data is obtained;

— requirements on storage of mDL data and mDL private keys.

ISO/IEC 18013-5

Scope and purpose



Data exchange architecture

Transmission technologies

Message formats

mDL data model

Data authenticity

Data-device binding

Data security during transport

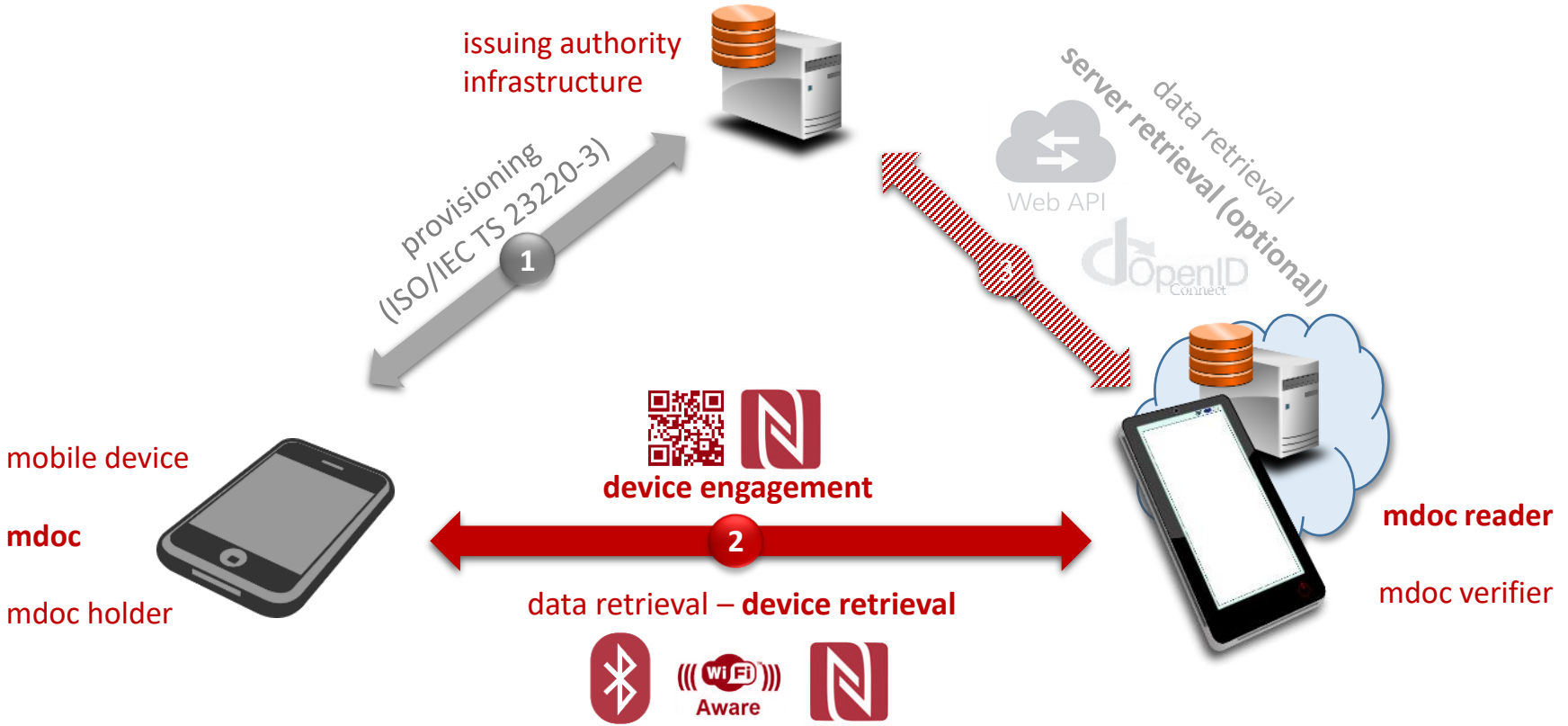
Avoid tracking

User consent

Data minimization

Selective release

Architecture and transmission technologies



Requests and responses

- Request and response messages are fully specified.
  - CBOR encoded for device engagement and device retrieval.
  - Request and response formats are independent of whether BLE, NFC or Wi-Fi Aware is used.
- Reader must request each data element individually.
- Holder can deny release of each data element individually.
- Data from multiple documents/namespaces can be retrieved with a single request + response.

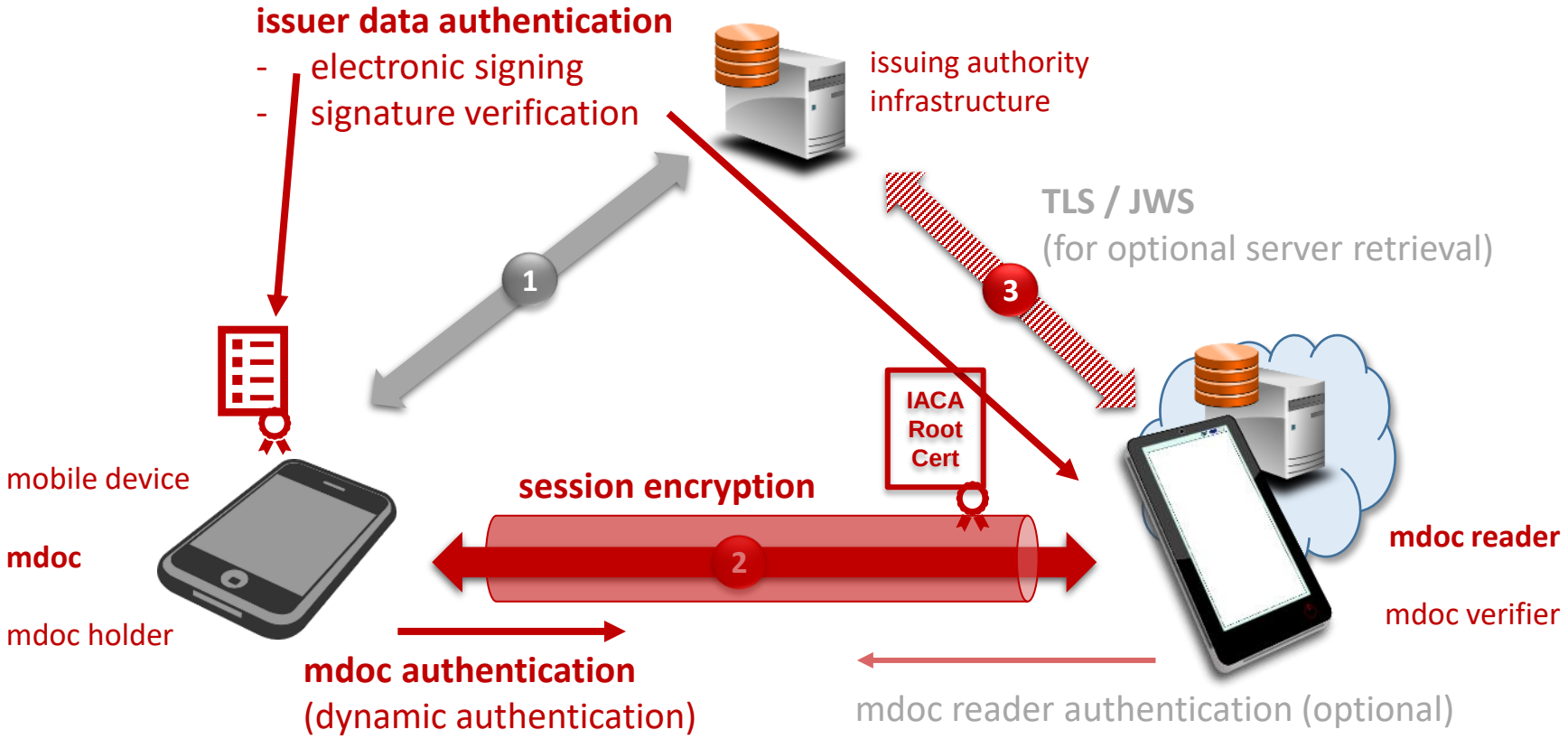
Document type and namespace

ISO/IEC 18013-5

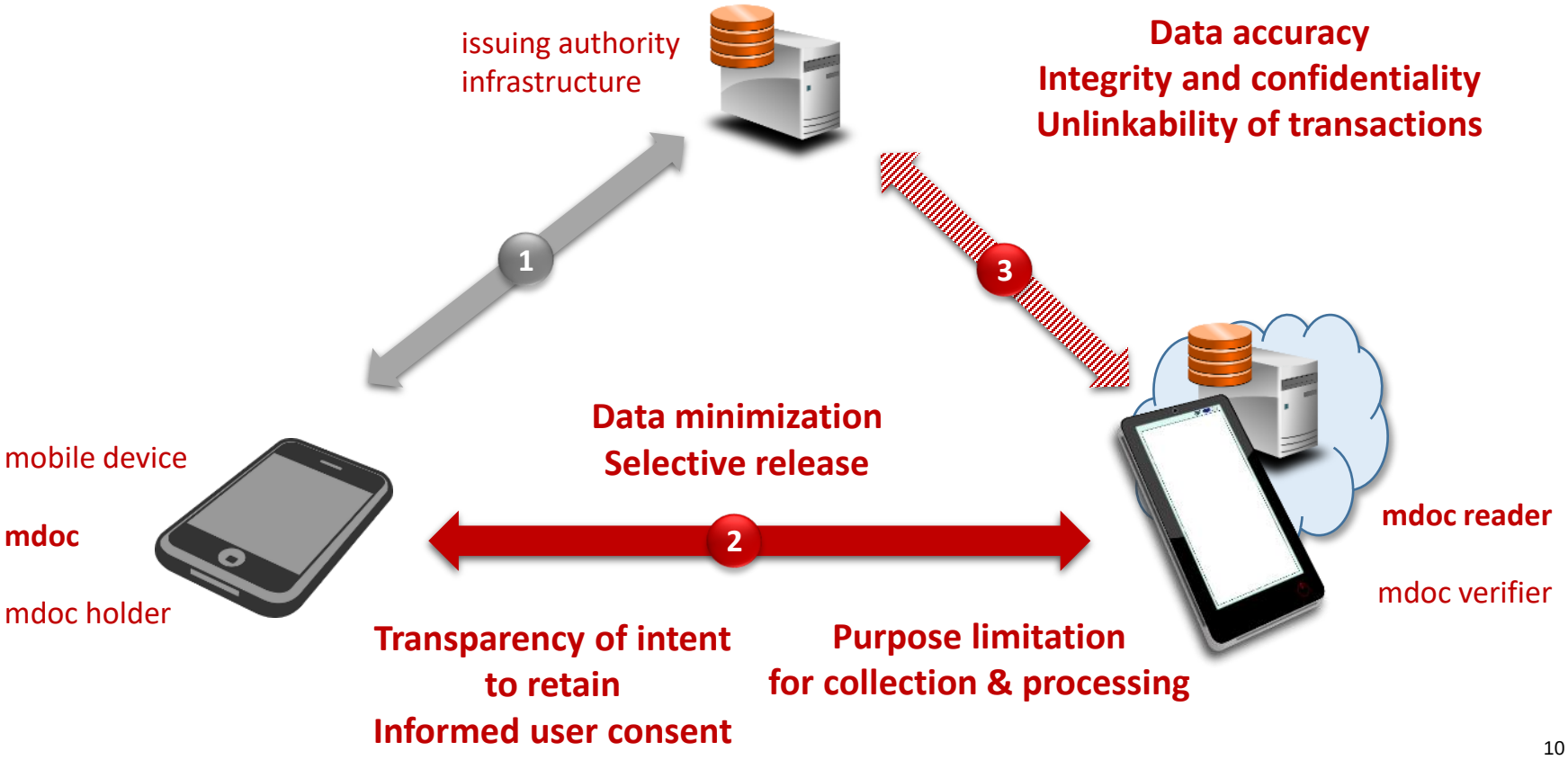
- Facilitates *international interoperability* by fully defining the mDL doctype and namespace.
- Supports *domestic needs* by allowing domestic namespaces.
- Supports *other document types* by allowing different doctypes.

Transmission technologies, request/response messages and security mechanisms can be used with any document type or namespace.

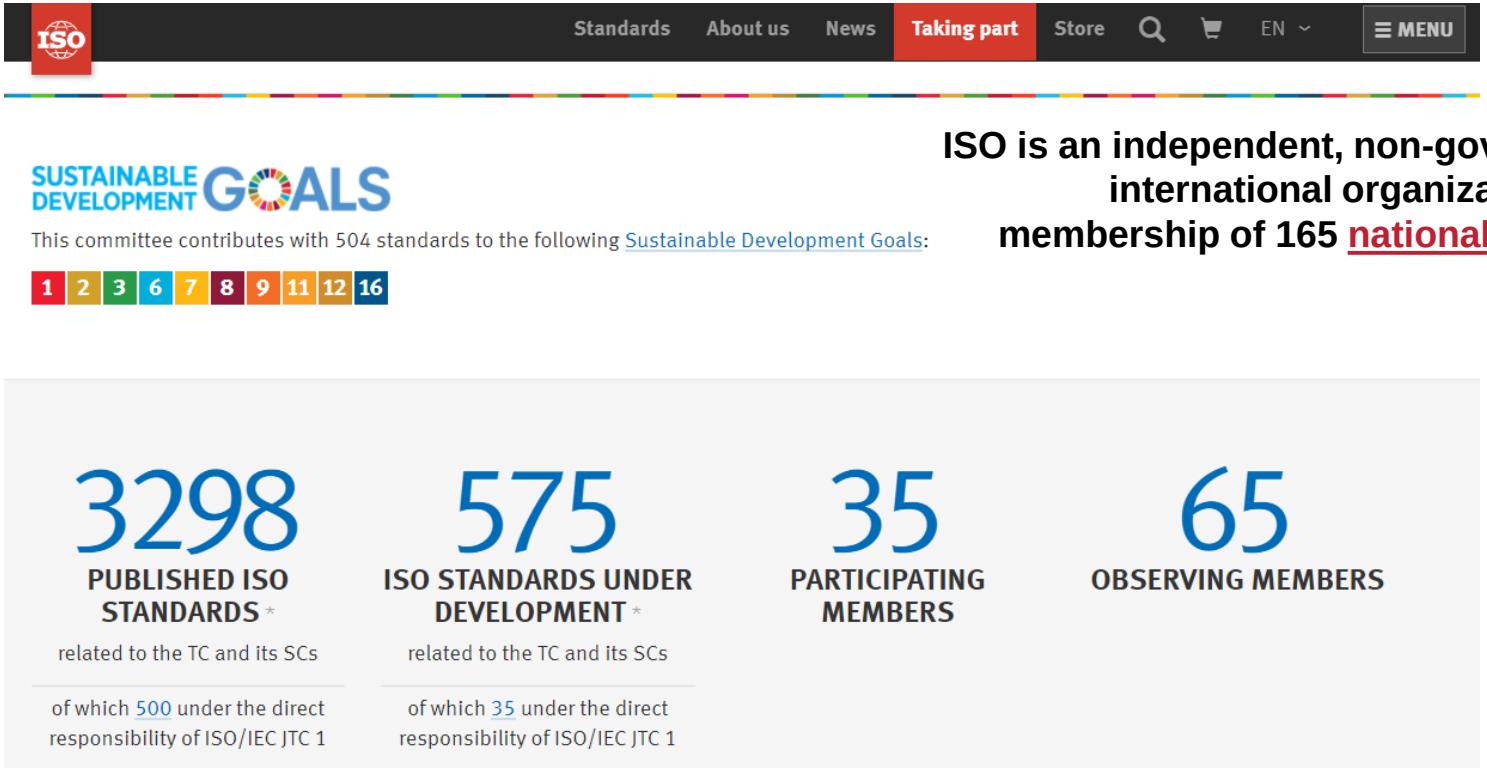
Security mechanisms



Privacy enabling features

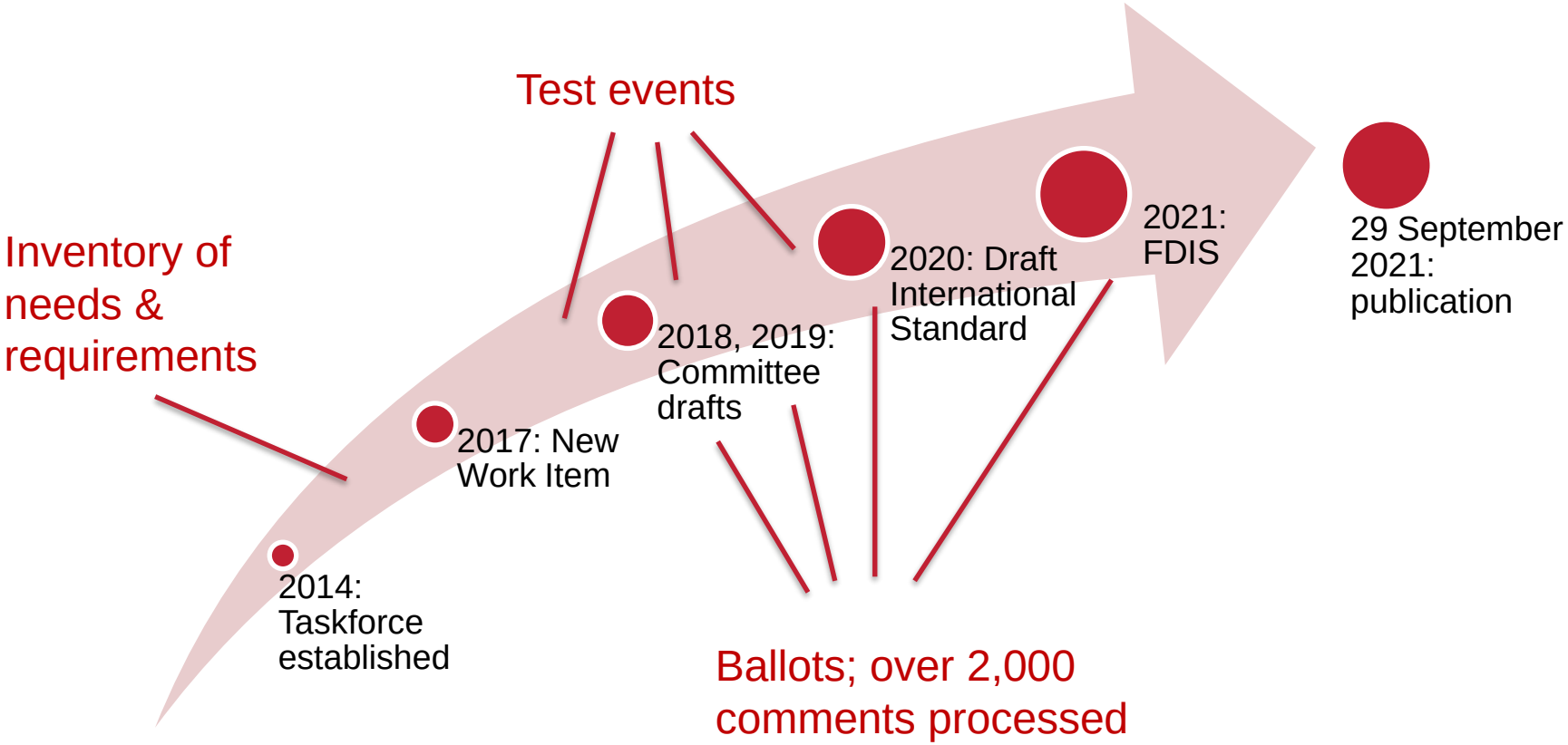


ISO/IEC JTC1 – Information Technology



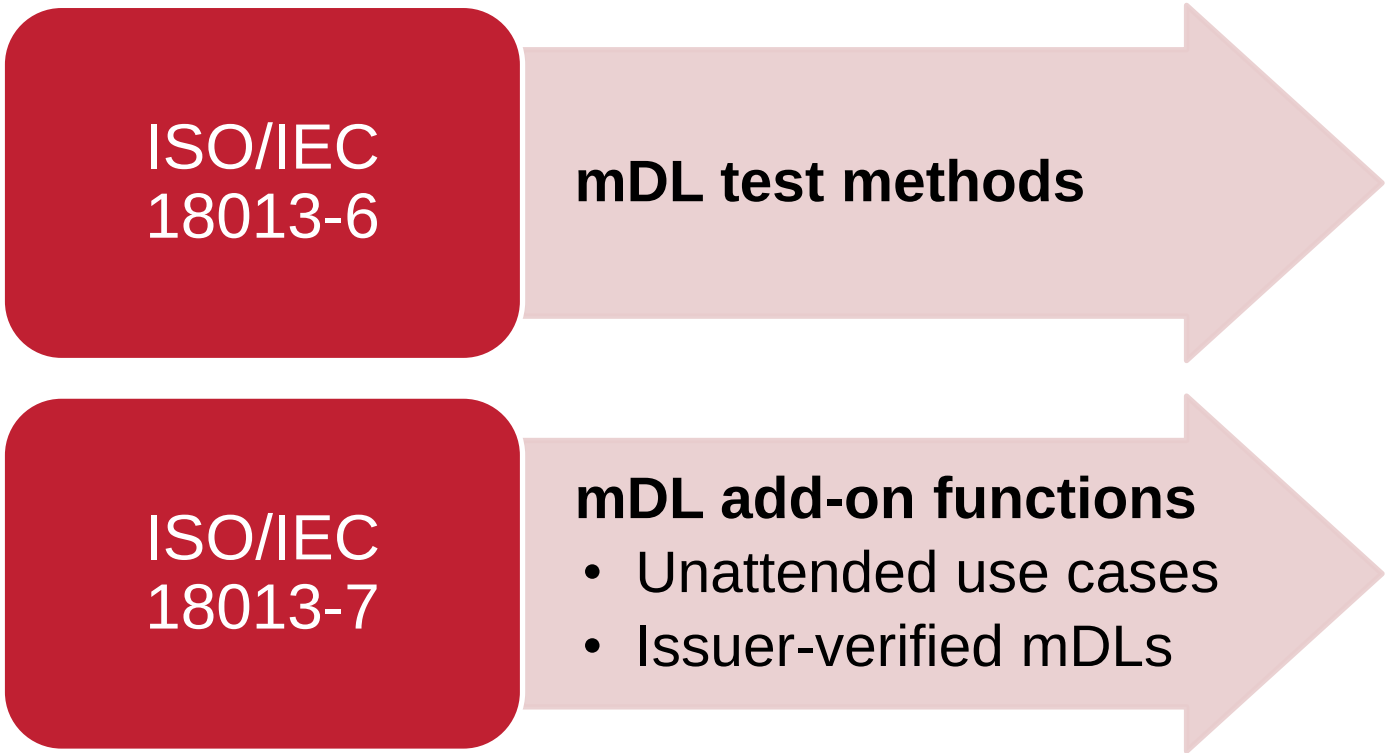
ISO is an independent, non-governmental international organization with a membership of 165 national standards bodies

Development of ISO/IEC 18013-5



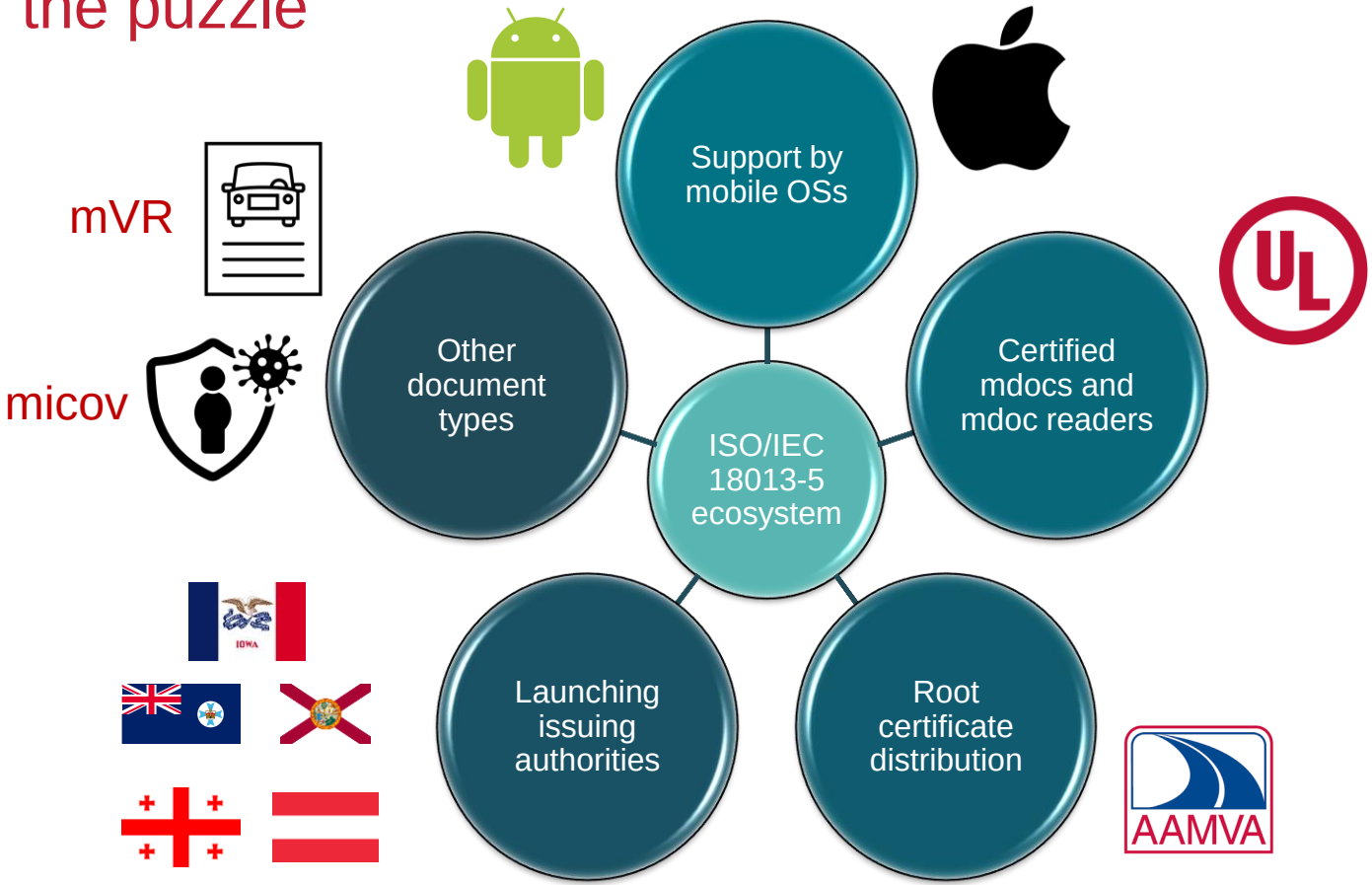
Ongoing standardization efforts

1



Building an ecosystem

Parts of the puzzle



ISO/IEC 18013-5 & Verifiable Credentials

A standards-based implementation of Verifiable Credentials?

I think that ISO 18013-5 and VCs should not be seen as competitors, but as complements.

That's nice. But what do you mean, complements?

Well. My impression is that without further specification, different implementations of the VC Data Model may not be interoperable…

You mean because we have no common communication protocols, requests/responses and security mechanisms?

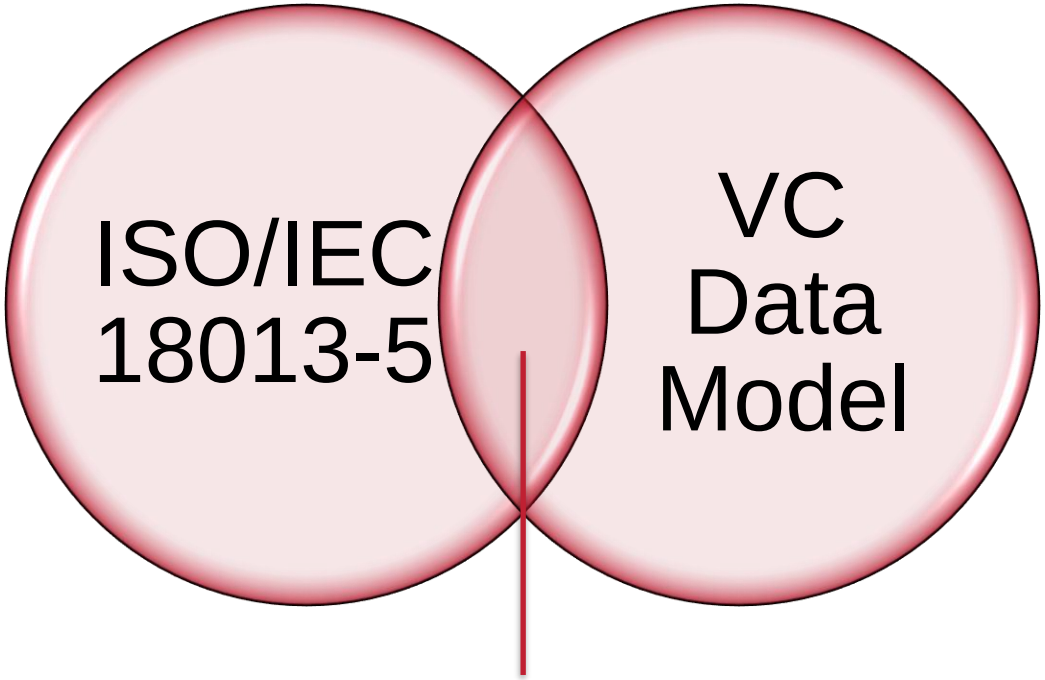
Exactly. But perhaps we can combine VCs with ISO 18013-5 to solve that.

OK, how?

I can think of four ways, actually.

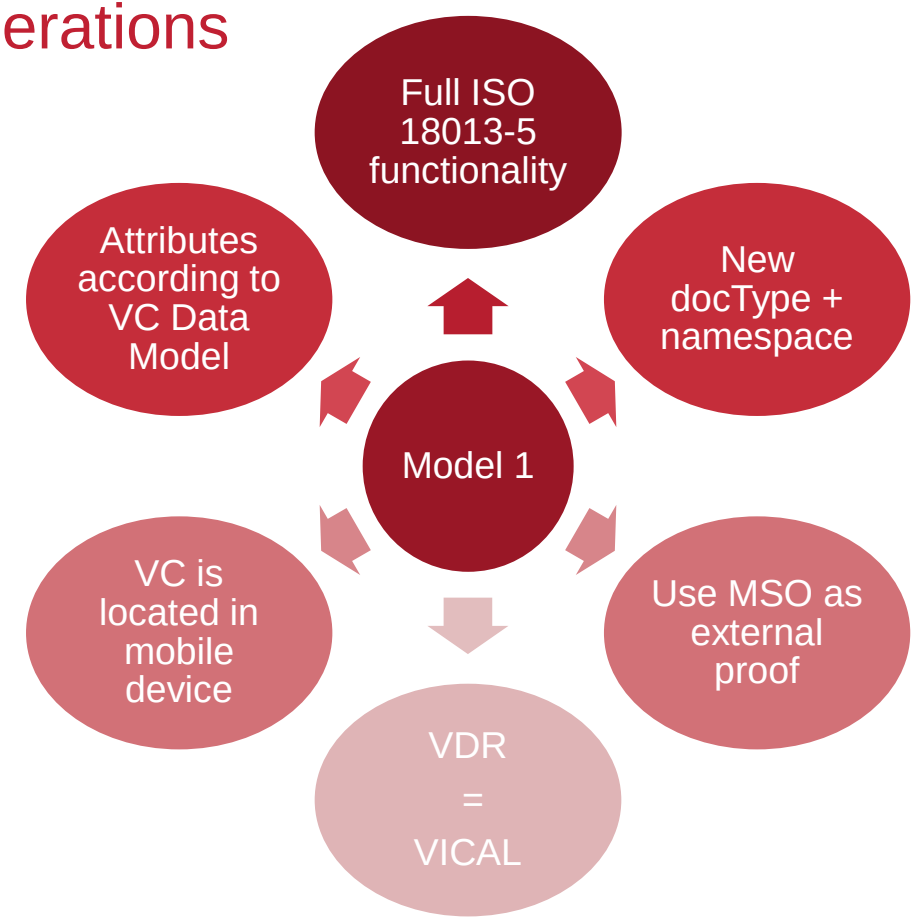
Let's check them out, then!

Model 1: New implementation based on both specs

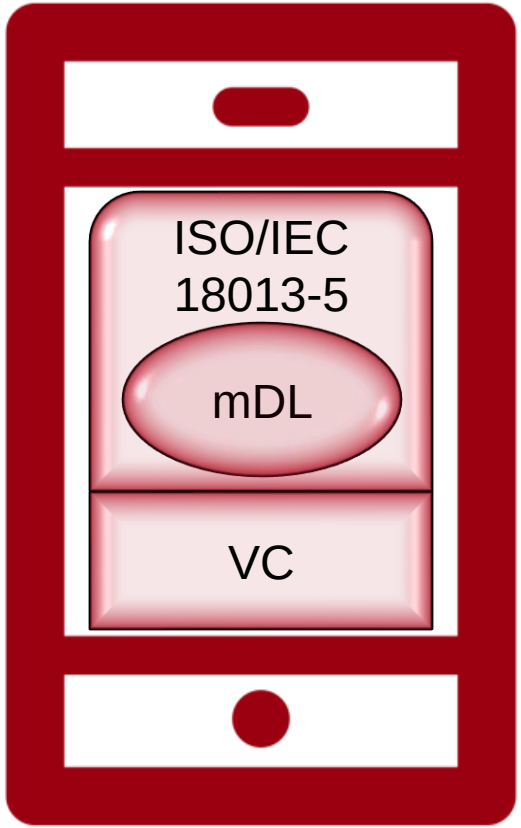


New implementation

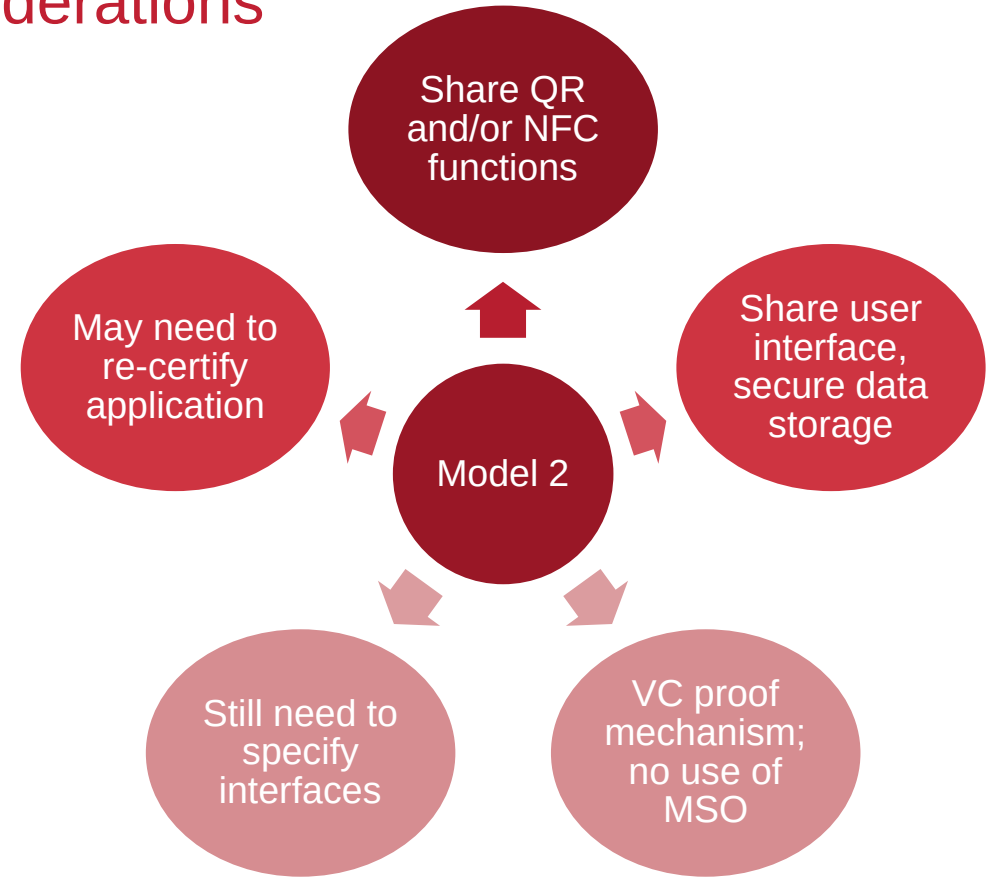
Model 1 considerations



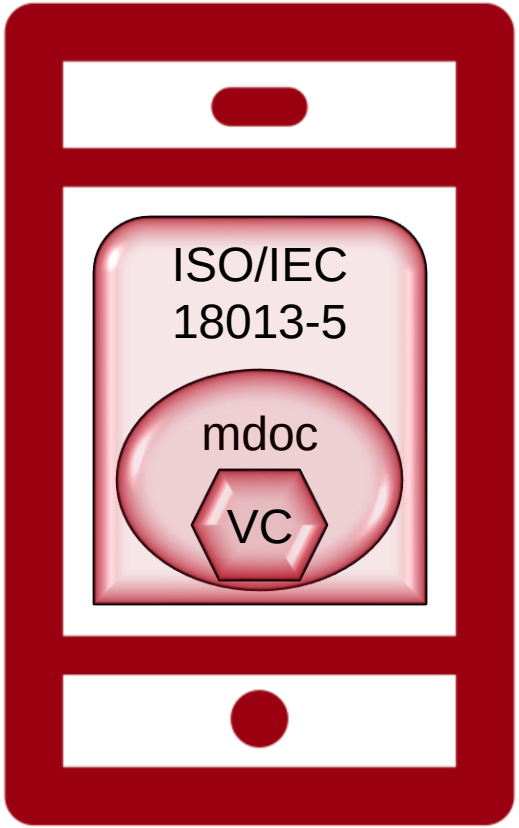
Model 2: ISO-compliant app as the repository for existing VC



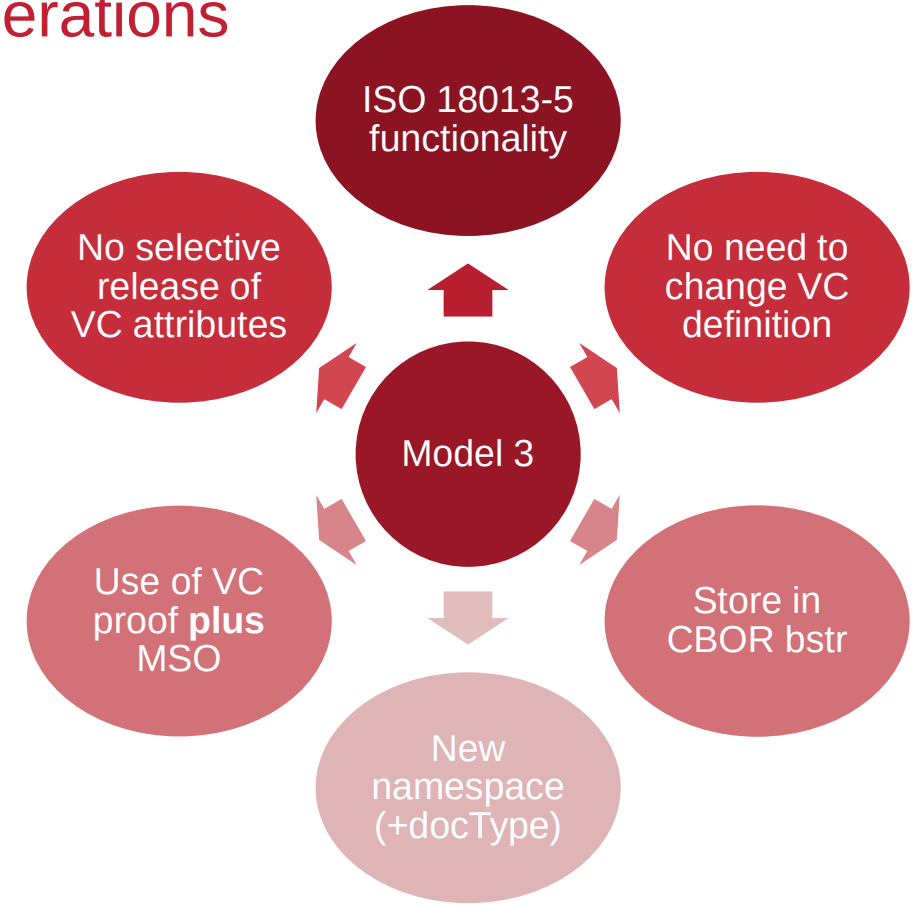
Model 2 considerations



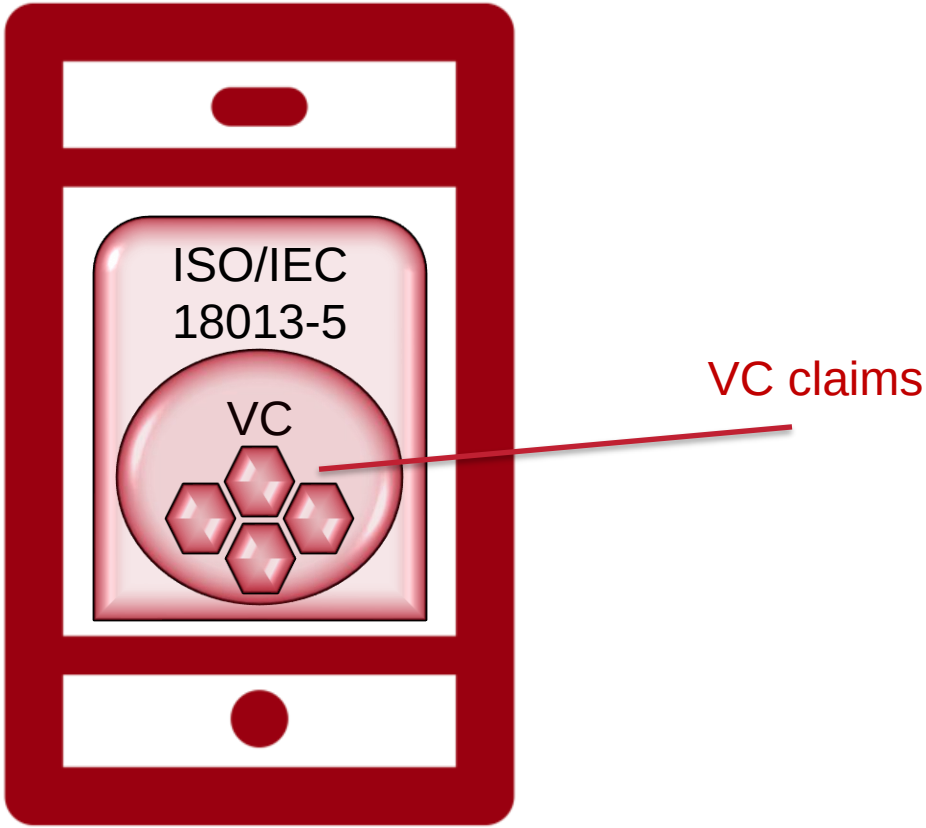
Model 3: Store existing VC as data element in an ISO mdoc



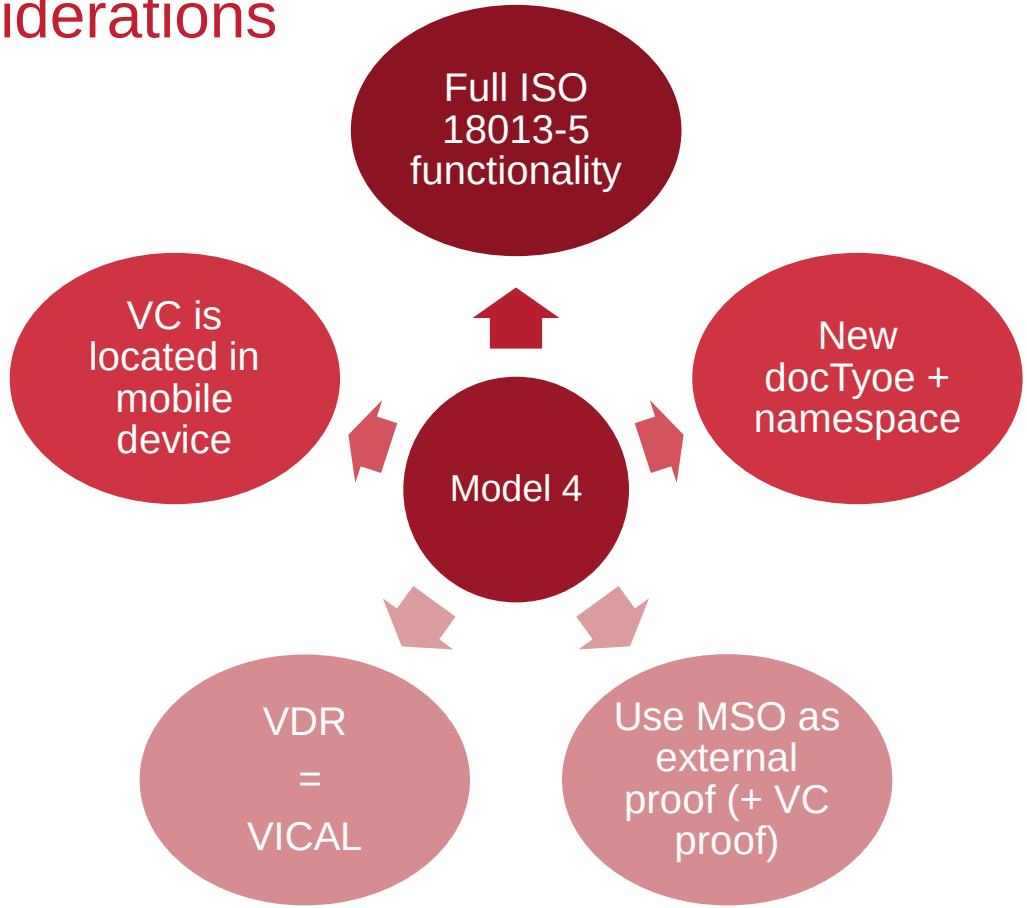
Model 3 considerations



Model 4: Store existing VC as ISO-compliant document



Model 4 considerations



Questions?
Comments?

Let’s discuss!

Arjan Geluk
identity management and security | UL
arjan.geluk@ul.com