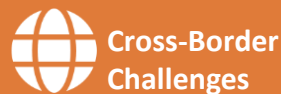


mDL Ecosystem

Security · Privacy · Interoperability

Presentation to ITU-T | June 2026



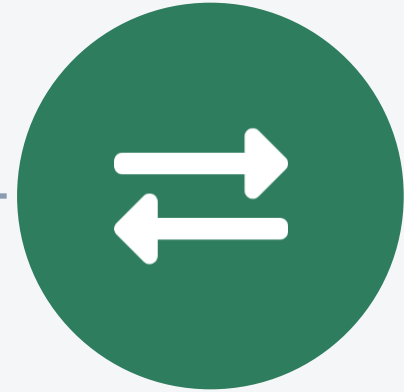
AAMVA's Goals for the mDL Ecosystem



Secure



**Privacy
Respecting**



Interoperable

Tools



**mDL Implementation
Guidelines**



Digital Trust Service (DTS)



Voluntary

Participation is not mandated. Issuing authorities choose to adopt the Guidelines — and choose to have their keys accepted into the DTS.



Guidance + Requirements

The Guidelines provide both general best-practice guidance and specific, enforceable requirements that contribute to interoperable, secure, and privacy-respecting mDL implementations.



By Issuers, For Issuers

The Guidelines were crafted and approved collectively by AAMVA members — the issuing authorities themselves. They reflect the consensus of the community that issues mDLs.



Compliance with the Guidelines is mandatory for an issuing authority's public key to be accepted into the DTS VICAL.



**Issuing
Authority**

Wants key in VICAL



**DTS
(AAMVA as
VICAL Provider)**

*Reviews & accepts compliant
IAs*



**Relying
Party**

Trusts keys in VICAL

What Relying Parties Know When a Key is in the VICAL:



The issuer is a valid, recognized
issuing authority



The issuer complies with all
security & privacy requirements in
the Guidelines



The issuer meets the
interoperability requirements in
the Guidelines

Cross-Jurisdictional Challenges



Assumes technical interoperability — the ability to exchange data — provided for mDL by ISO/IEC 18013-5



Relying Party



Holder



Does this credential come from a valid issuer?



Will the Relying Party respect my data?



Given it comes from a valid issuer — to what extent can I trust the information for my purposes?



Will I be surprised by what the RP does with my data?

A Pragmatic, Phased Approach

1



VICAL Sharing

AAMVA, Austroads, and EU VICALs mutually accept each other's certificates to identify valid issuers for relying parties.

In Progress

2



Issuer Practices Taxonomy

Describe issuer practices (PKI security, enrolment, provisioning) so RPs can assess fitness for purpose without mandating a single approach.

Under Discussion

3



Holder Data Rights

Scalable framework recognizing different jurisdictional approaches to holder consent, always allowing a successful path to transaction completion.

Pragmatic solution exists

The Challenge: Fitness for Purpose without Mandating Uniformity

✗ One Standard for All Issuers

Mandating identical PKI, enrolment, and provisioning practices across all jurisdictions

✗ Likely impedes sovereignty

✗ Not scalable globally

✓ Practices Taxonomy

A structured description of issuer practices enables relying parties to make informed trust decisions

✓ Preserves sovereignty

✓ Scalable globally

✓ Informed RP decisions

Taxonomy covers:

PKI Security

Enrolment

Provisioning

Privacy Practices

3 Holder Privacy — The Informed Guidance Approach



Two extremes

Decide for the holder (risks denial of service) — or let the holder decide alone (no guidance, same as a physical document)



A middle path

The wallet uses trust signals to apply a guidance model, and presents a clear recommendation to the holder



PEMC Certification (Kantara)

Provides the data point that enables wallets to craft that informed guidance



Works cross-border

Effective where local regulations are absent or do not apply — no dependency on home jurisdiction



Pragmatic approach

Can be combined with other wallet inputs — not the only solution, but holds considerable promise

Where We Are — And What Comes Next



Technical interoperability for mDL across jurisdictional boundaries already exists (ISO/IEC 18013-5)

The remaining challenges are operational acceptance by relying parties and privacy protection for holders

A phased, pragmatic approach makes sense — one step at a time

First-step solutions are being rolled out: VICAL trust lists for RP trust, and privacy-respecting certification (e.g. Kantara PEMC) for holder protection

Next up: Issuing authority practices taxonomy