



American Association of
Motor Vehicle Administrators

Treading the Delicate mDL Ecosystem

*Lori Daigle, Program Specialist
Identity Management Team
February 26, 2025*

OUR VISION

*Safe drivers
Safe vehicles
Secure identities
Saving lives!*

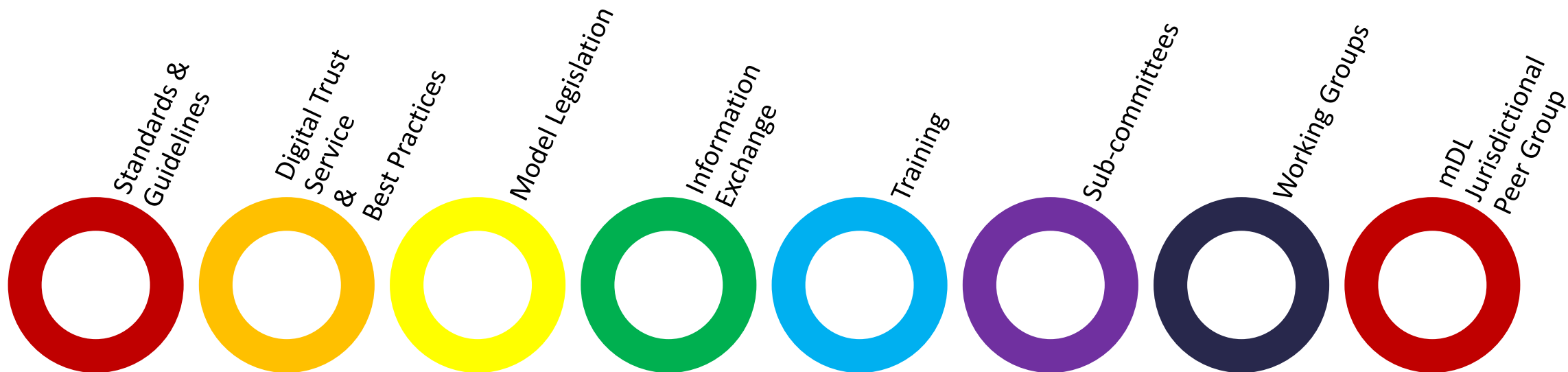
What is AAMVA's Role in the mDL Ecosystem?





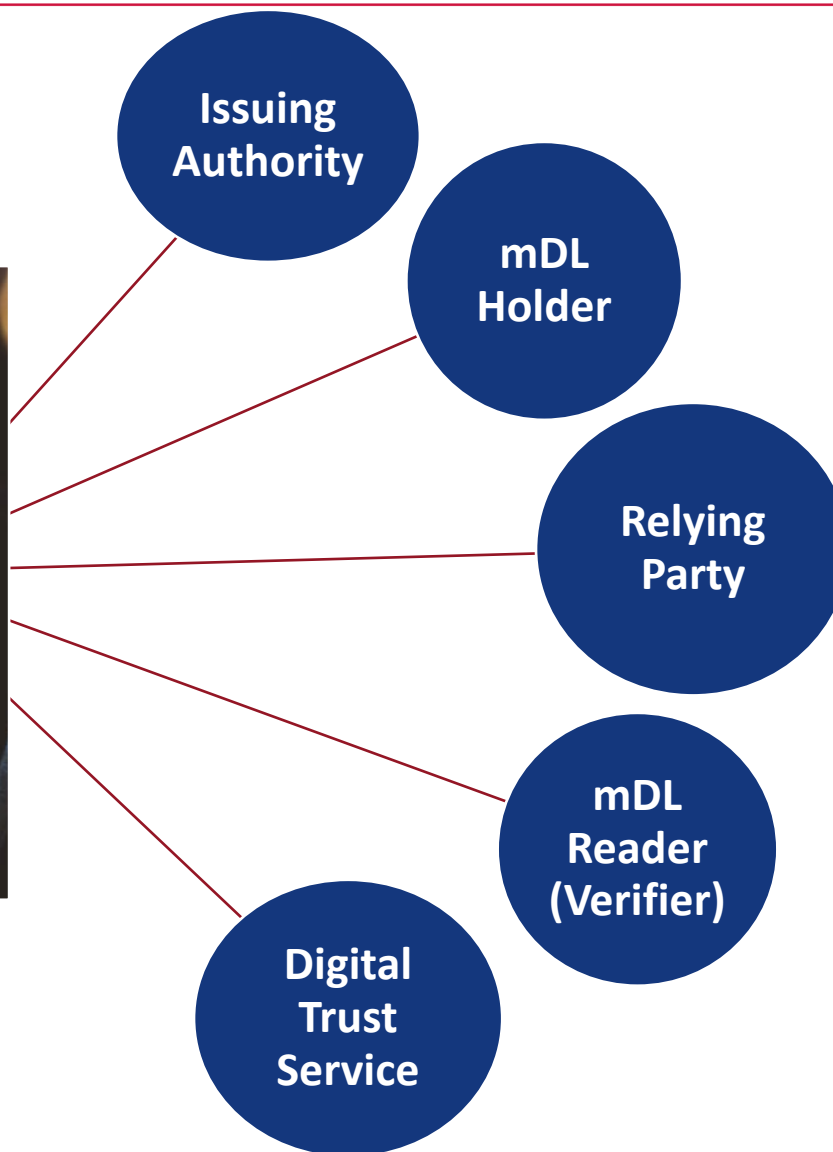
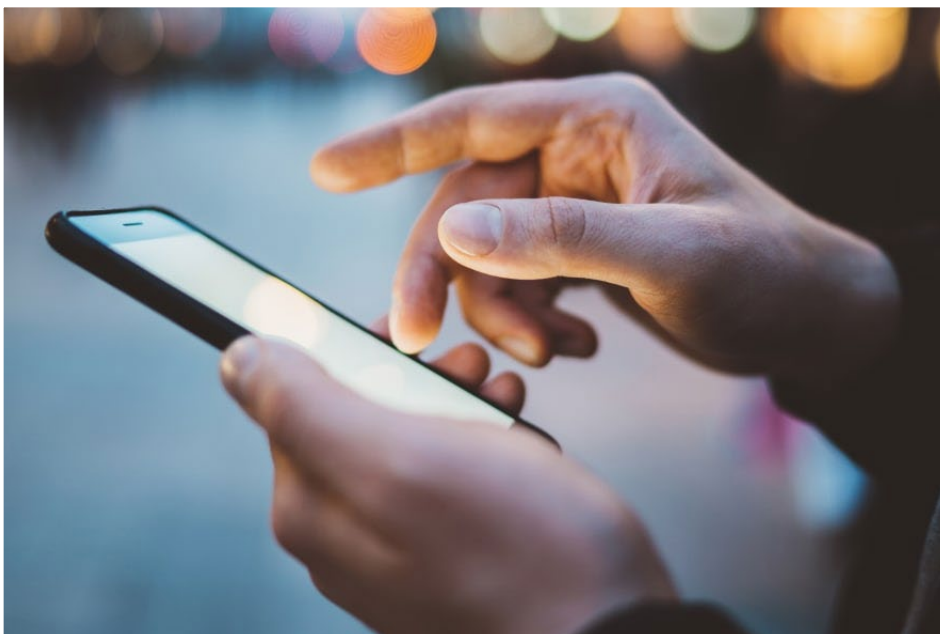
American Association of
Motor Vehicle Administrators

Provides Resources, Advocacy, & Participation Opportunities



Why Embrace the mDL Ecosystem?





Mobile Driver Licenses Benefit Everyone

Drive License Holders

- Safer than physical DLs
- Convenient
- Always up to date
- Aligned with “tap” payment processes
- Protect Privacy
- Consent-based workflows
- Protects holders in the digital domain in ways physical DLs cannot (in-person and online)

Businesses & Service Providers

- Enhanced trust in authenticity
- Easily authenticated
- Faster identity verifications
- Less keystrokes/errors
- Minimize exposure to unwanted PII
- Minimize fraudulent transaction risk
- Create a safer customer scenario
- Faster, easier, and safer age verifications

Value-Added Advantages



Relying Party Trust



The identity credential
being presented comes
from a legitimate
Issuing Authority.

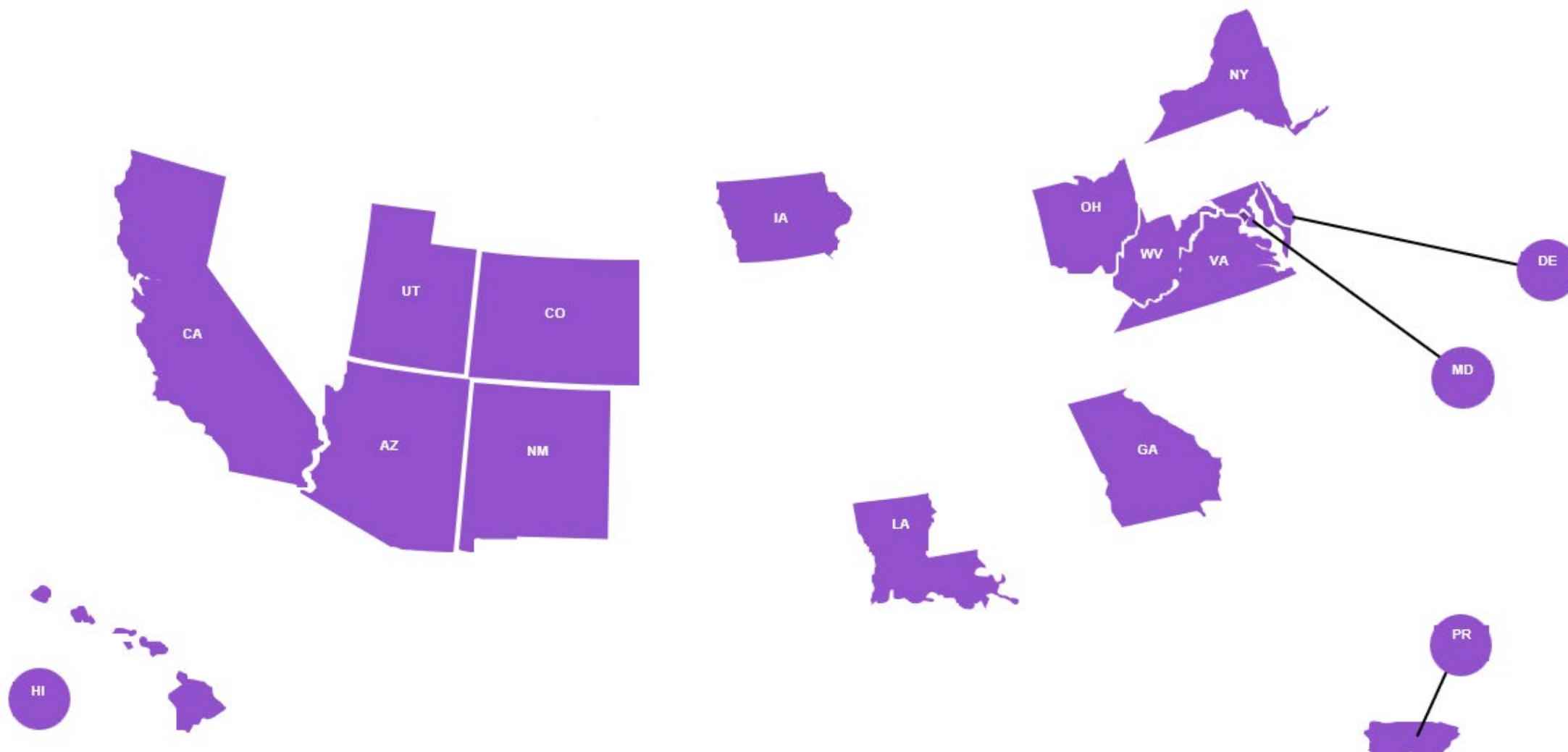
The credential contains
both accurate and
current data.

The credential was
issued to the person
presenting it.

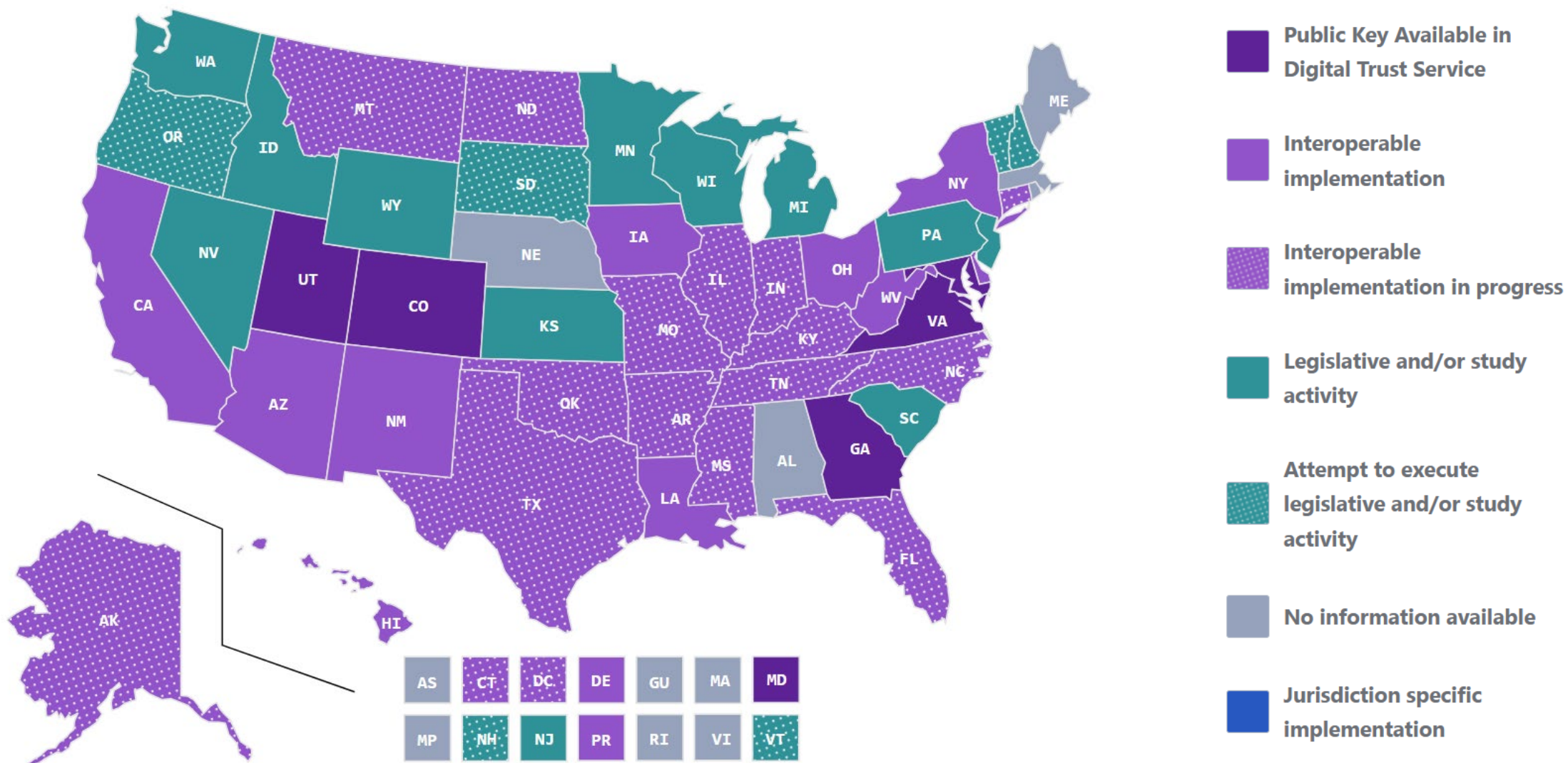
Who has an mDL in North America?



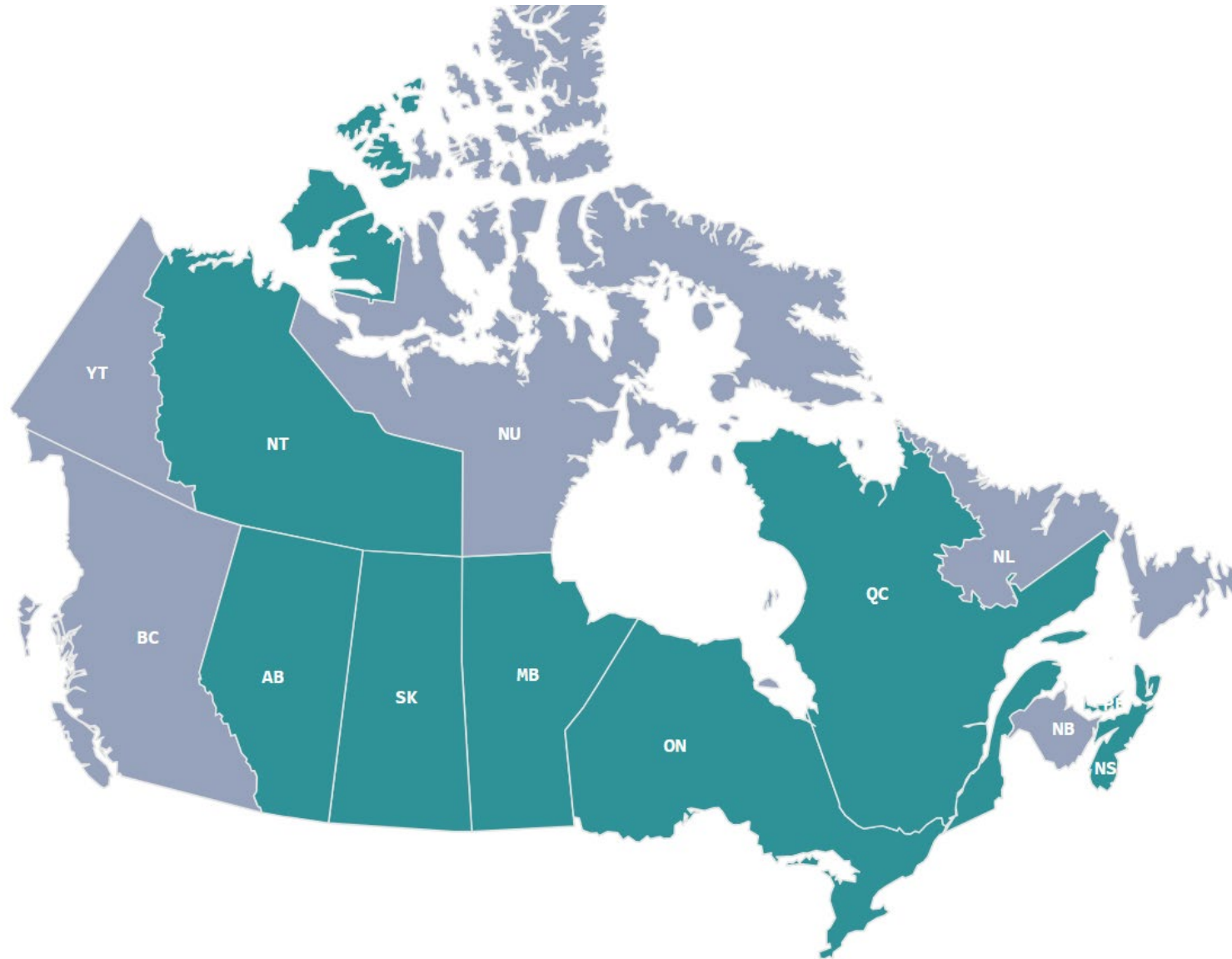
Jurisdictions with mDL Programs



mDL Ecosystem – United States and Territories

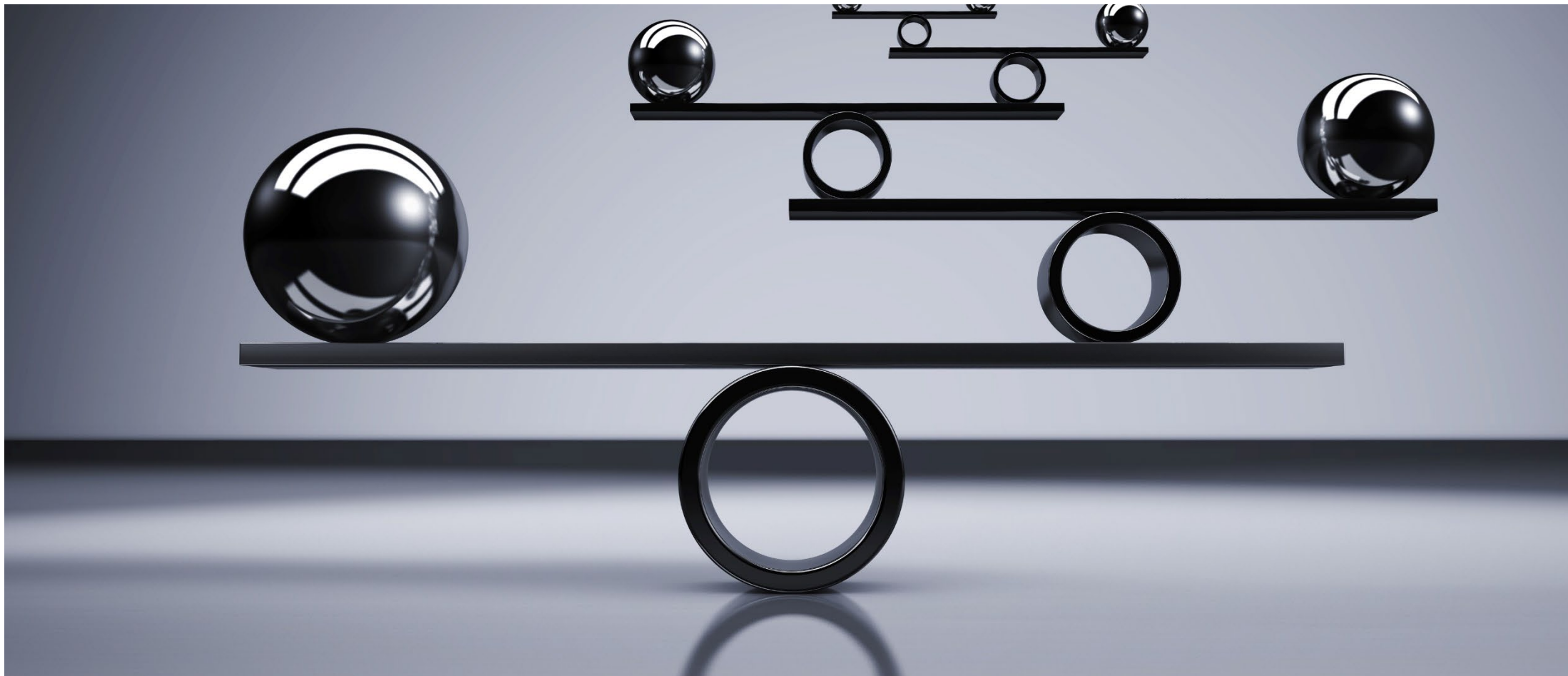


mDL Ecosystem - Canadian Provinces



-  Public Key Available in Digital Trust Service
-  Interoperable implementation
-  Interoperable implementation in progress
-  Legislative and/or study activity
-  Attempt to execute legislative and/or study activity
-  No information available
-  Jurisdiction specific implementation

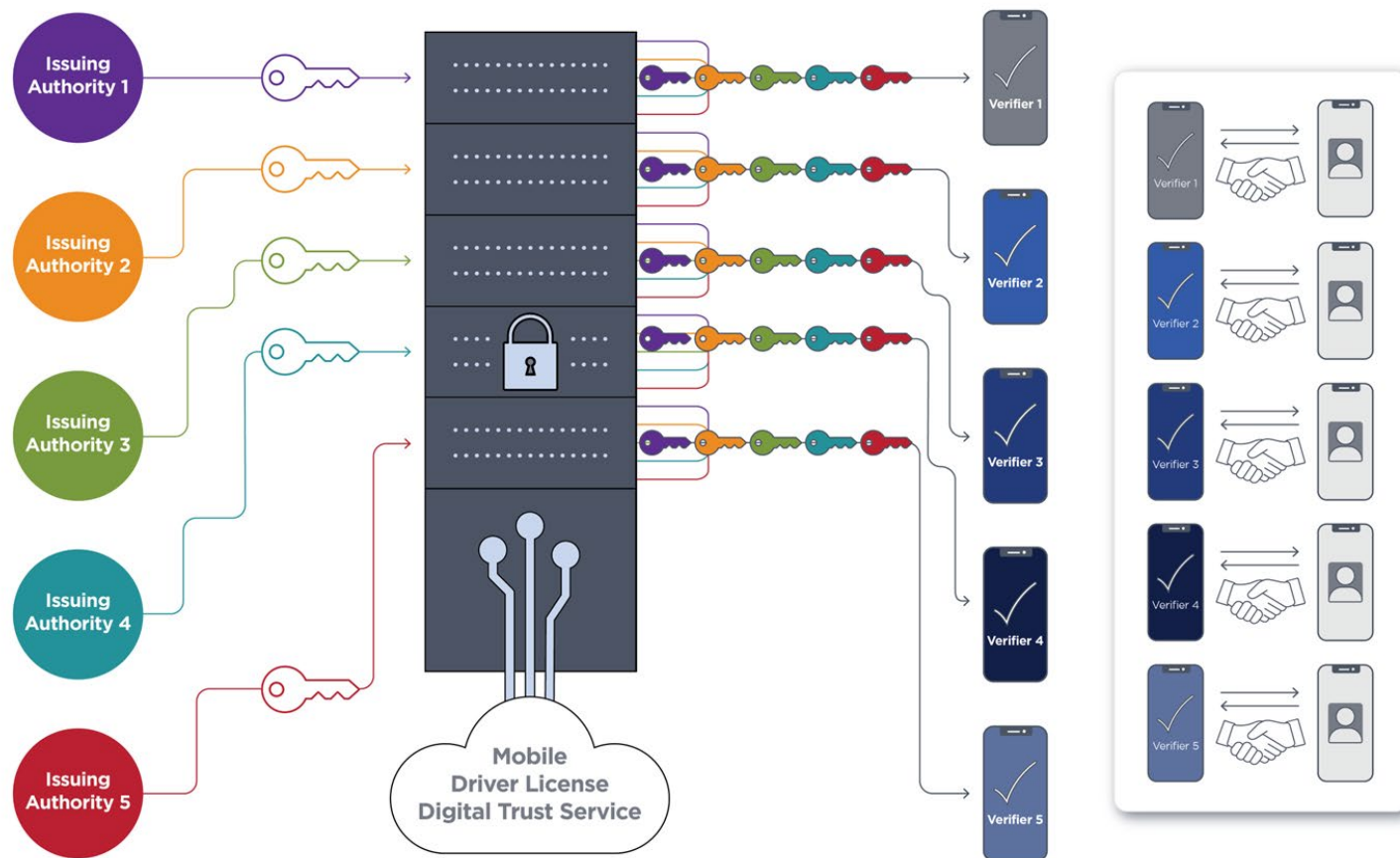
What is AAMVA's Digital Trust Service?



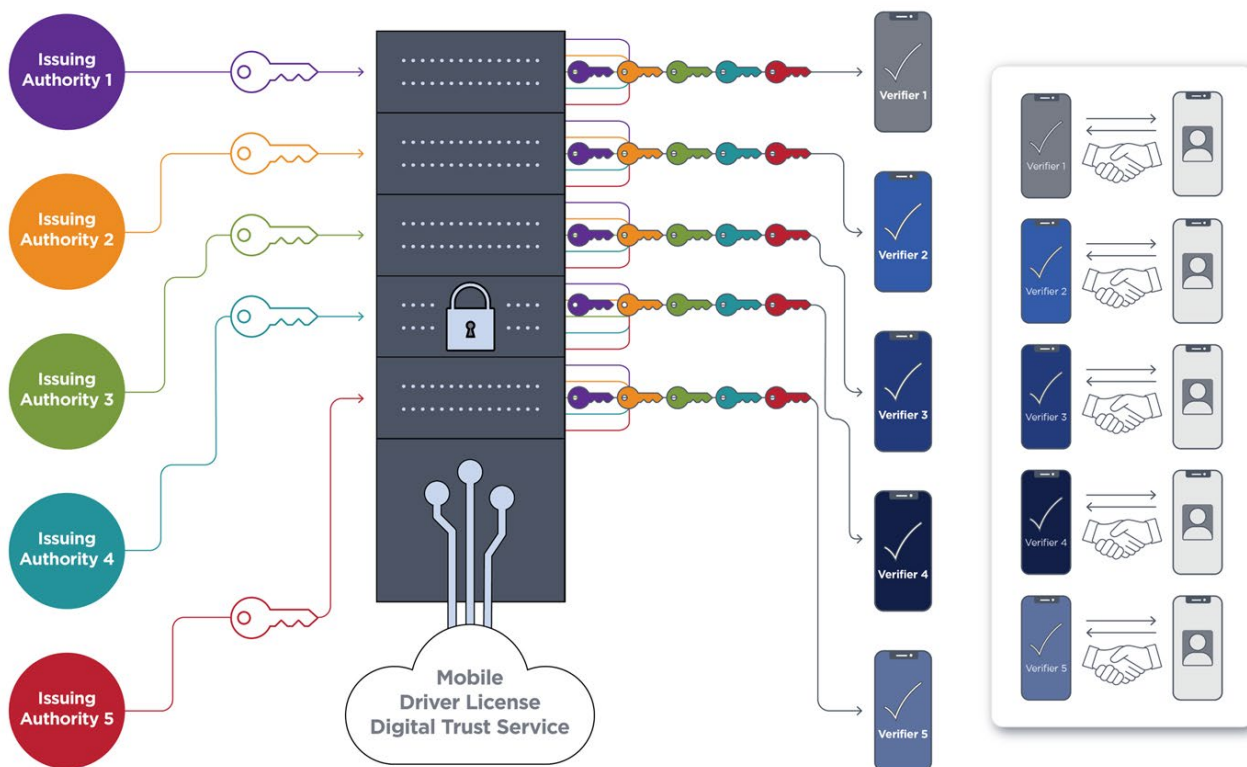
The AAMVA Digital Trust Service (DTS) was stood up to aid in adoption and maximize trust.

Single, secure, and convenient point of trust for mDL verification.

Issuing authorities and relying parties can obtain the public keys used to authenticate (mDLs) from a single location.



The DTS Ensures:

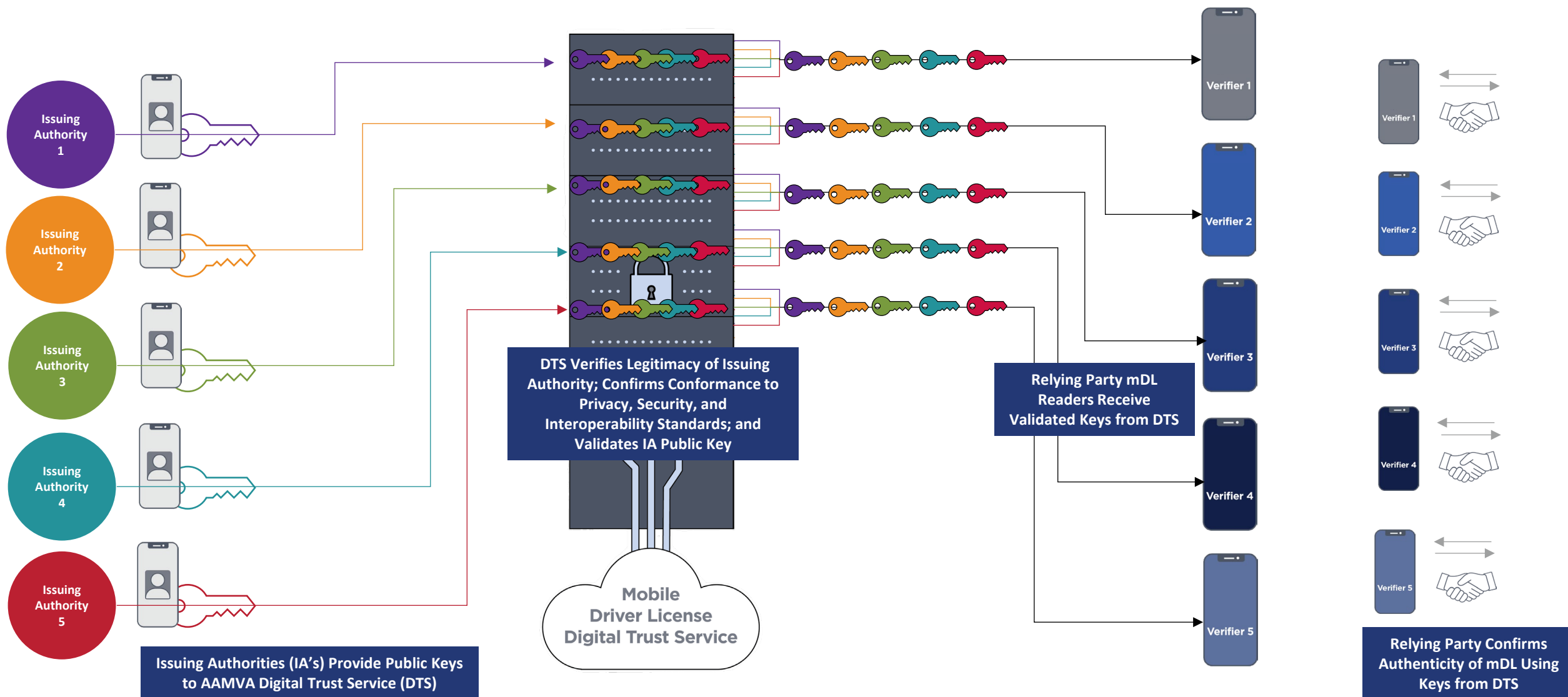


**The mDL was
issued by a bona
fide issuing
authority.**

**The mDL is safe,
secure, privacy
respecting, and
interoperable.**



The AAMVA Digital Trust Service



How Do We Work Together in the mDL Ecosystem?



An mDL is NOT
just a picture of
a driver license
on a phone
(flash pass).



Verifiably provisioned by an Issuing Authority to a mobile device

An identity credential that **Must** be read and validated by an electronic reader

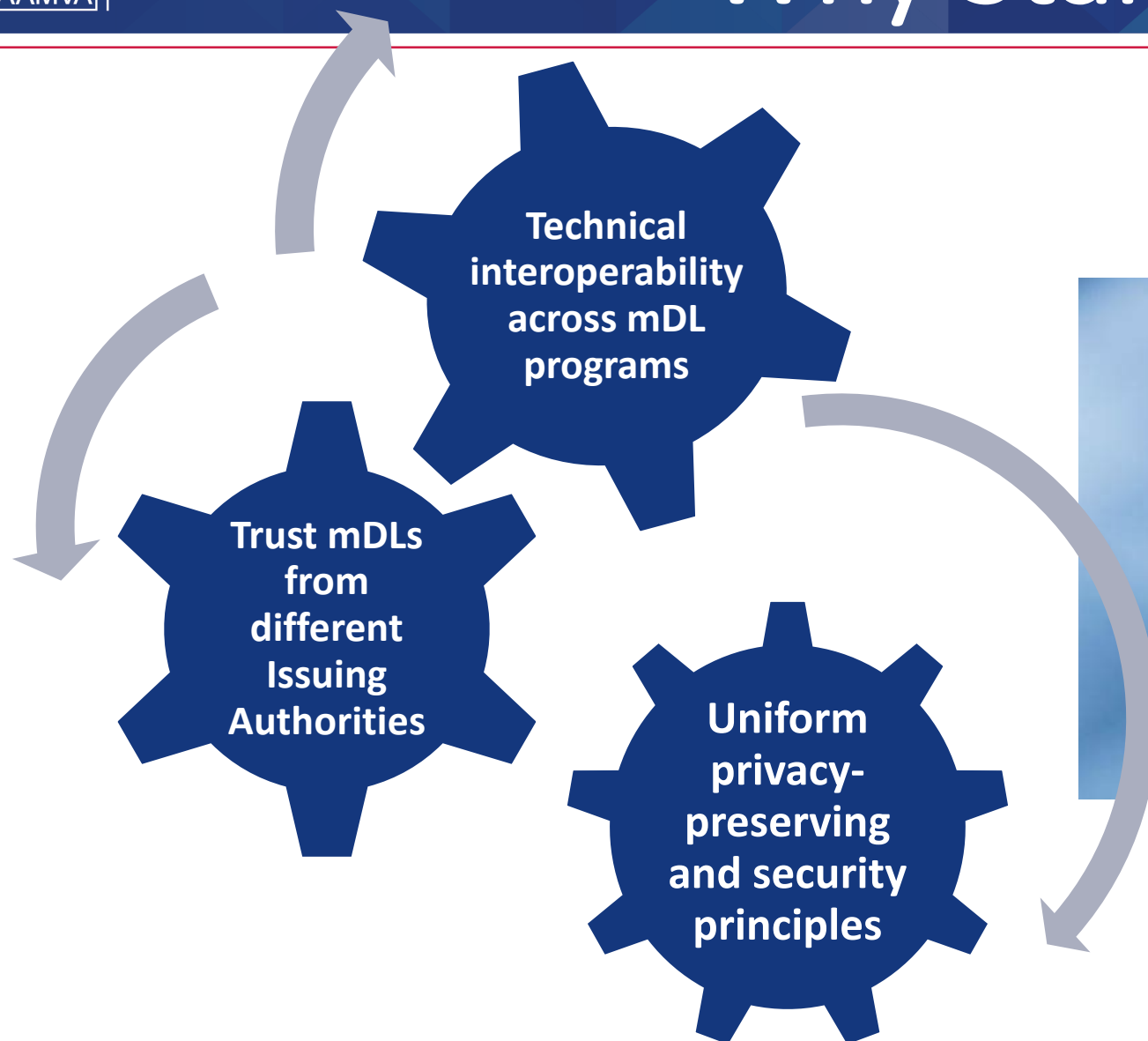
Compliant with the ISO/IEC 18013-5 standard

A carrier of the same data that is present on a physical ID Card or Driver License

An mDL IS:



Why Standardization Matters



How Can Relying Parties Know an mDL is authentic?

- The mDL reader device verifies the authenticity of the mDL by matching the Issuing Authority's previously-loaded public key to the privately signed certificate from the mDL.

Do Relying Parties need to physically touch the mDL holder's phone?

- NO! The mDL information will be displayed on Relying Parties' reader device once data has been transmitted. There is NO NEED for a Relying Party to touch an mDL holder's phone.

Is Internet Access Necessary to Read an mDL?

- mDL verification is device-to-device; the connection occurs locally using Wi-Fi, NFC, or Bluetooth.



TSA



**Know Your
Customer**



**Government
Services**



**Age
Verification**



**Online
Transactions**

