The webinar will begin shortly

1

The Mobile Driver's License and Ecosystem

Identity Council Webinar
April 30, 2020

Introductions

- Randy Vanderhoof, Secure Technology Alliance

Who We Are

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions.

We provide, in a collaborative, member-driven environment, education and information on how smart cards, embedded chip technology, and related hardware and software can be adopted across all markets in the United States.

Our Focus
- Access Control
- Authentication
- Healthcare
- Identity Management
- Internet of Things
- Mobile
- Payments
- Transportation

What We Do

- ❖ Bring together stakeholders to effectively collaborate on promoting secure solutions technology and addressing industry challenges
- ❖ Publish white papers, webinars, workshops, newsletters, position papers and web content
- ❖ Create conferences and events that focus on specific markets and technology
- ❖ Offer education programs, training and industry certifications
- ❖ Provide networking opportunities for professionals to share ideas and knowledge
- ❖ Produce strong industry communications through public relations, web resources and social media

Identity Council

"…Serves as a focal point for Alliance's identity and identity related efforts leveraging embedded chip technology and privacy- and security-enhancing software… Supports a spectrum of physical and logical use cases and applications, form factors, attributes, and authentication and authorization methods."

COUNCIL RESOURCES
- Assurance Levels Overview and Recommendations
- FICAM in Brief: A Smart Card Alliance Summary of the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance
- Identifiers and Authentication – Smart Credential Choices to Protect Digital Identity
- Identity Management in Healthcare
- Identity Management Systems, Smart Cards and Privacy
- Interoperable Identity Credentials for the Air Transport Industry
- Identity on a Mobile Device: Mobile Driver's License and Derived Credential Use Cases
- The Mobile Driver's License and Ecosystem
- Smart Card Technology and the FIDO Protocols

mDL - A Secure Technology Alliance Member Initiative

- Industry driven
- Education focused
- White papers, FAQs
- Online resources
  - Knowledge Center
  - mDL Uses
  - Implementation Map
- How to get involved
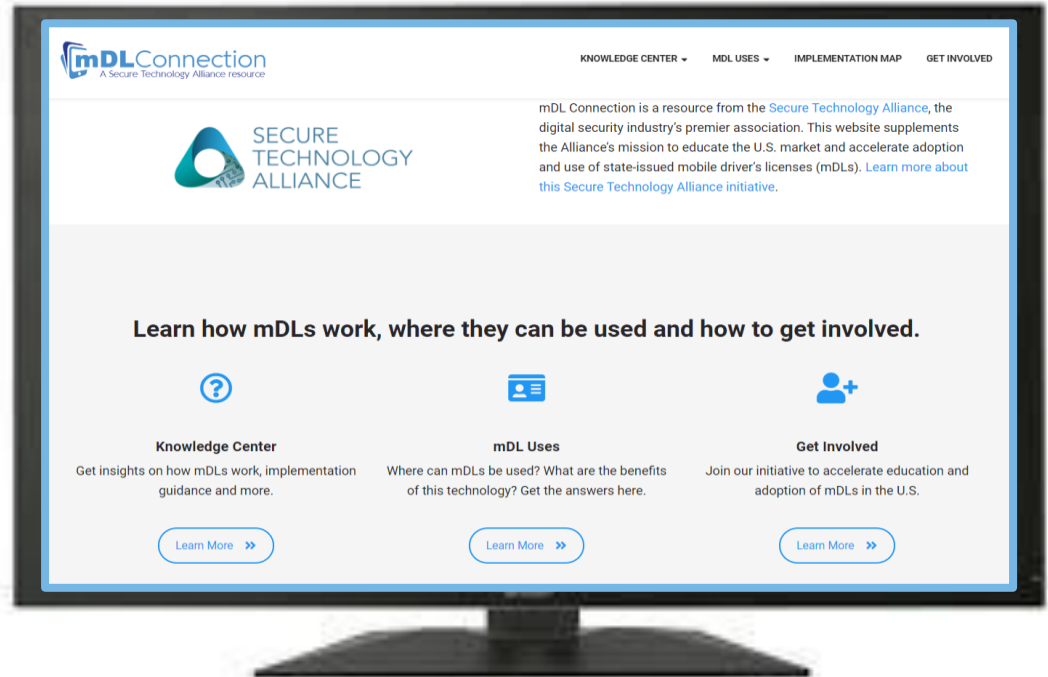
www.mdlconnection.com

Polling Question

What is the stakeholder category or business interest that best describes your interest in mobile driver's licenses (mDLs)?

- Technology: Identity/security technology provider/integrator
- Issuance: Government/other entity issuing ID documents
- Relying Party: Entity using ID credentials in its business
- Standards: Regulator/standards setting body for digital ID
- Other: None of the above

Webinar Panelists

- Randy Vanderhoof, Secure Technology Alliance

- Geoff Slagle, AAMVA

- Mike McCaskill, Florida Highway Patrol

- David Kelts, GET Group NA

Geoff Slagle – Director of Identity Management AAMVA

Date   30 April 2020

Who is AAMVA?

- DMVs & State/Provincial LE agencies (U.S. and Canada)

- 150+ Associate members

- Federal government (DOT, DOJ, DHS, State, DoD, DOC, SSA)

- Coalitions/Associations (STA)

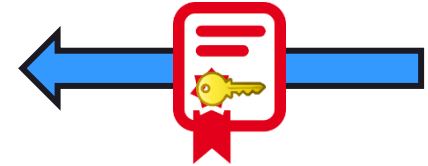- Standards Developing Organization (ANSI)

High-level overview of mDL

What is an mDL?

- Concept
- Common misconceptions
- Functional requirements
- International work

What is an mDL?

Concept

Utopia State

Hello Abu
Connection
Online

Settings Help

My Cards

010110
110011
101000
0001

mDL Reader

✓ Valid

[1,2] Name: Abu Tanaka
[3] DOB: 1980-01-01
[4b] Validity: 2022-03-22
[9] Code: A, BE
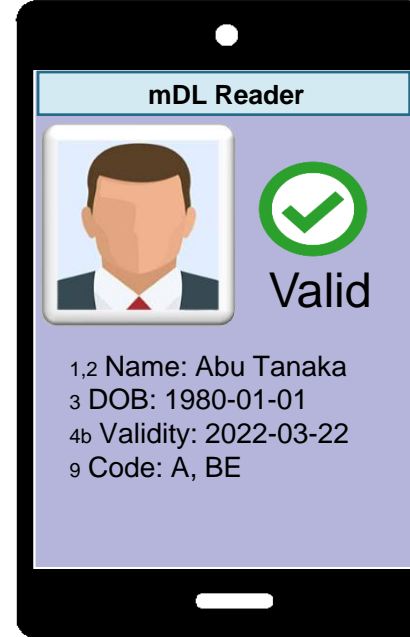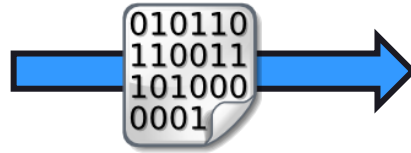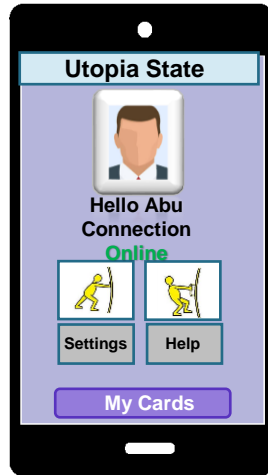
What is an mDL?

Common misconceptions

mDL is **NOT** a picture of the physical license on the device

What is an mDL?

Functional requirements

Security AND Privacy by design

Confirm Identity

Convey Driving Privileges

Trustable

Interoperable
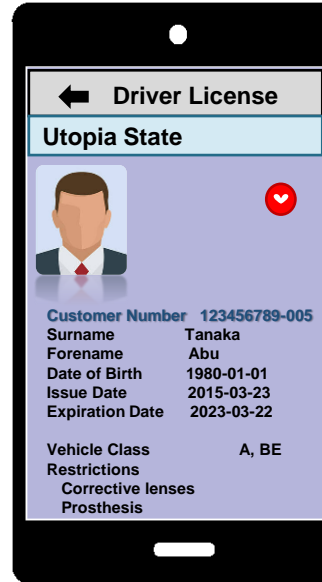
Selective Info Release

Attended and Unattended

Remote Management

Work Offline

Driver License

Utopia State

Customer Number   123456789-005
Surname   Tanaka
Forename   Abu
Date of Birth   1980-01-01
Issue Date   2015-03-23
Expiration Date   2023-03-22

Vehicle Class   A, BE
Restrictions
    Corrective lenses
    Prosthesis

mDL standardization

ISO
WG10 & WG4

International activity

Implementations
Pilots
Proof of Concepts
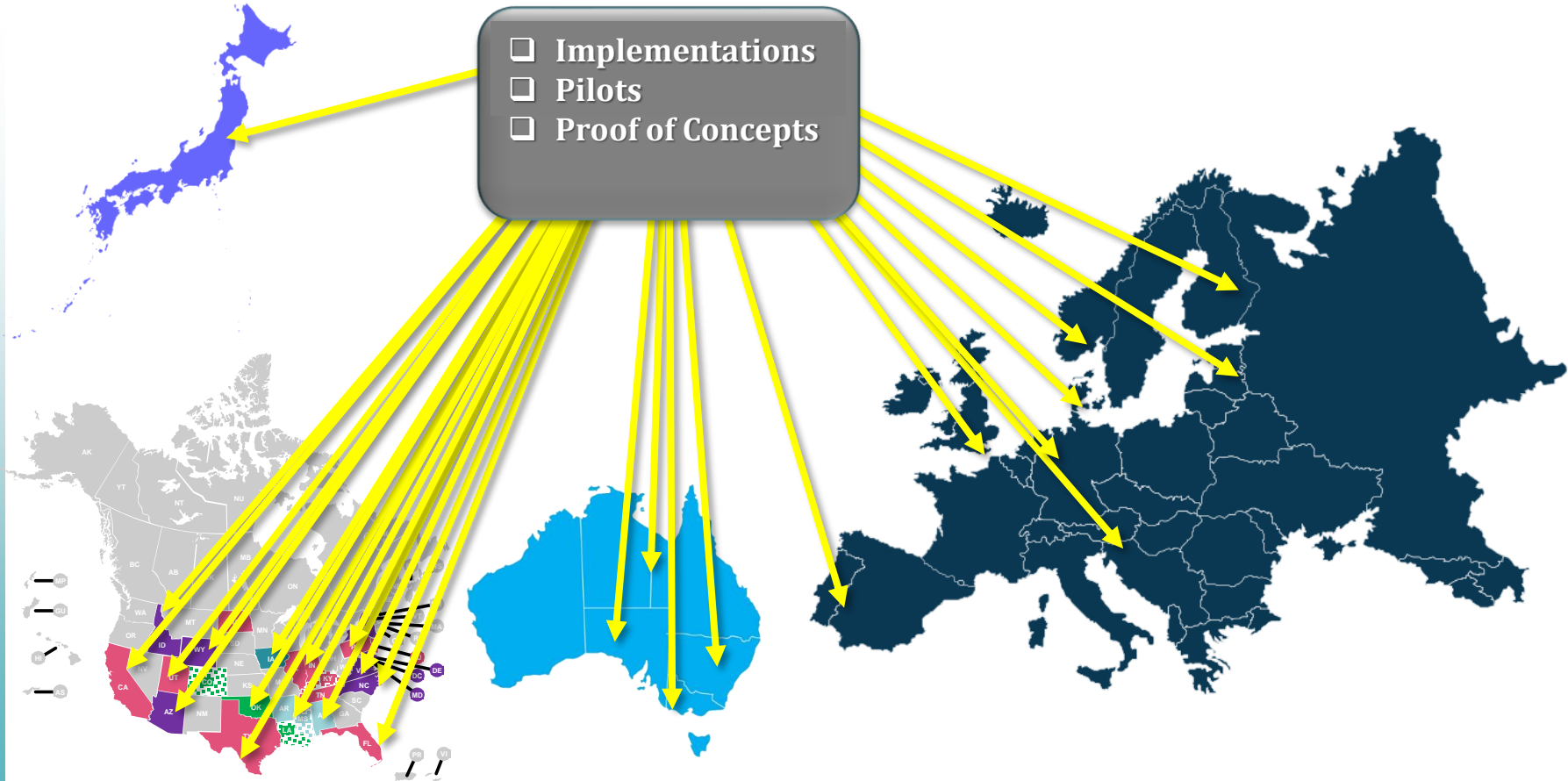
SECURE TECHNOLOGY ALLIANCE

In light of the recent pandemic, the need for standardized mDL implementations is even greater than originally envisioned. With an overnight reality thrust upon the world that has turned into an online/virtual workforce and workplace with a super strong aversion to having to physically interact with something if it's not 100% necessary.

- Geoff Slagle

Mike McCaskill – Chief Administrative Officer, Florida Highway Patrol, Chair of Joint mDL Working Group

Date   30 April 2020

Jurisdictional Needs

- Confirm Identity
- Convey Driving Privilege
  - Revoked, Cancelled, Suspended
- Privacy
  - No tracking
  - Selective information release
- Security
  - Data secured on the device
  - Device engagement Encrypted

Jurisdictional Needs Cont.

- Interoperable
  - Across jurisdictional lines
  - globally
- Trustable
  - Data authentic
  - Data source validation
- Work Offline
  - Areas without cellular service
- Ability to manage remotely
  - Remove mDL from device

SECURE
TECHNOLOGY
ALLIANCE

The mDL will be the single biggest change ever seen in the identity landscape. It will allow for process improvements in banking, travel, driving privilege management, and safety improvements for law enforcement.

- Mike McCaskill

Mobile Drivers License (mDL) is **not** an image of a Driver's License

Photoshop, Screenshots, Barcode generators, Image sharing, & the lack of Trusted Screen Environment make this an expensive mistake someone will make

ISO 18013-5

Enter ISO 18013-5, a collaboration of over 50 Companies, Issuers, Associations and Platform OEMs

- Citizens should have control over their personal data
- Issuers eSign the identity attributes to demonstrate they have been proven
- Relying Parties should obtain just the data they need for compliance of their use case and not store data
- Relying Parties verify the data to trust the interaction – *in person or online*

mDL Creates an Ecosystem

Issuing Authority

- Provision & Sign
- Manage Identity Accuracy
- {Optional} Identity Provider

Citizen

- mDL Holder / User
- Requests a Service with ID
  - in-person {or online}

Verifier

- Reads and Validates mDL
- Lowers Risk and Fulfills Compliance Regulations
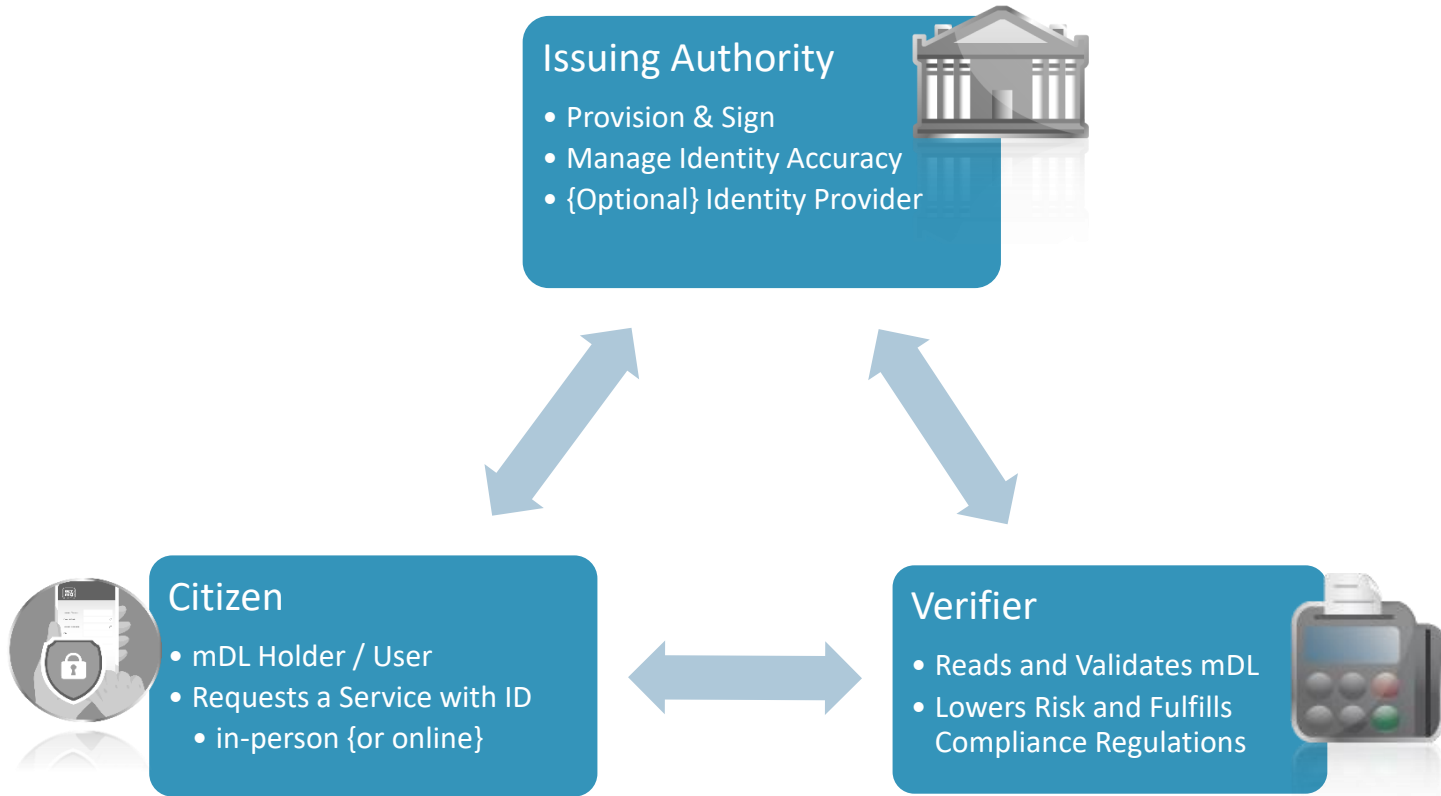
Trust Mechanisms - ISO 18013-5 mDL & mID

Issuing Authority
- Provision & Sign
- Manage Identity Accuracy
- {Optional} Identity Provider

PKI

Signer Certs

Master Lists

Citizen
- mDL Holder / User
- Requests a Service with ID
  - in-person {or online}

ISO 18013-5

Verifier
- Reads and Validates mDL
- Lowers Risk and Fulfills Compliance Regulations

Cryptographic Trust in the ID provided by ISO 18013-5
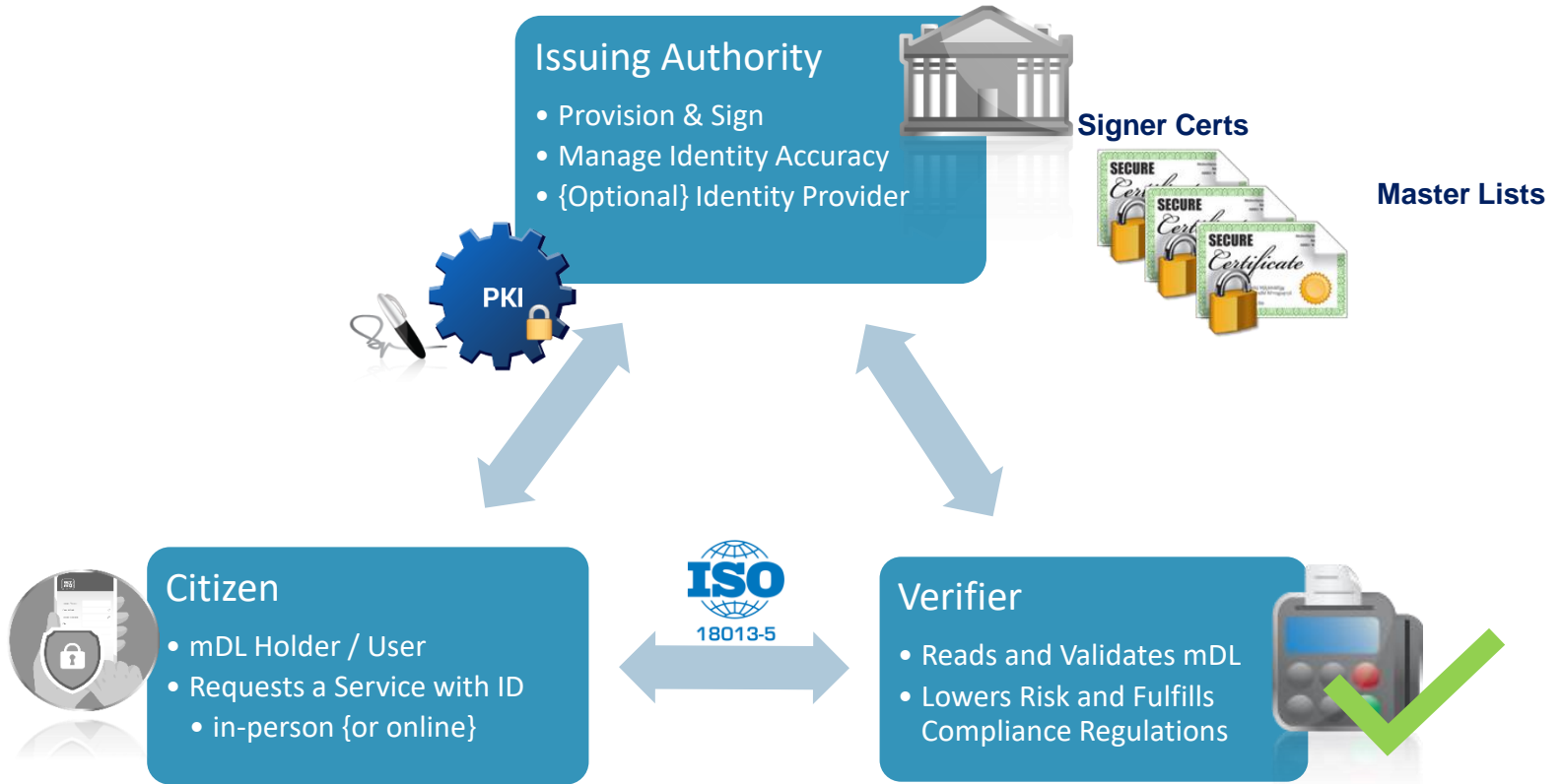
mDL Use Cases for ISO 18013-5

Drawn from *AAMVA mDL Functional Needs Whitepaper* and *known RFPs*

Unattended At-Distance

Gray = Not In Scope for 1st Version ISO 18013-5 (Day One)

Identity
- Cyber Identity
- Obtain Social Services ✓
- Vote or Register to Vote ✓
- Open Bank Accounts
- Peer to Peer Data Exchange

Contextual
- Rent a Car, Car Sharing ✓
- Check into Hotel
- Roadside Stop ✓
- Board a Plane, Security Check
- Federal Building Access ✓

Core
Provision, Delete, Update data or privileges
- Share Driving Privilege
- Enter a Bar, Club, or Restaurant ✓
- Purchase Age-Restricted Item ✓
- Show Driving Privilege (not trusted)

Data Minimization is a requirement for all mDL Use Cases
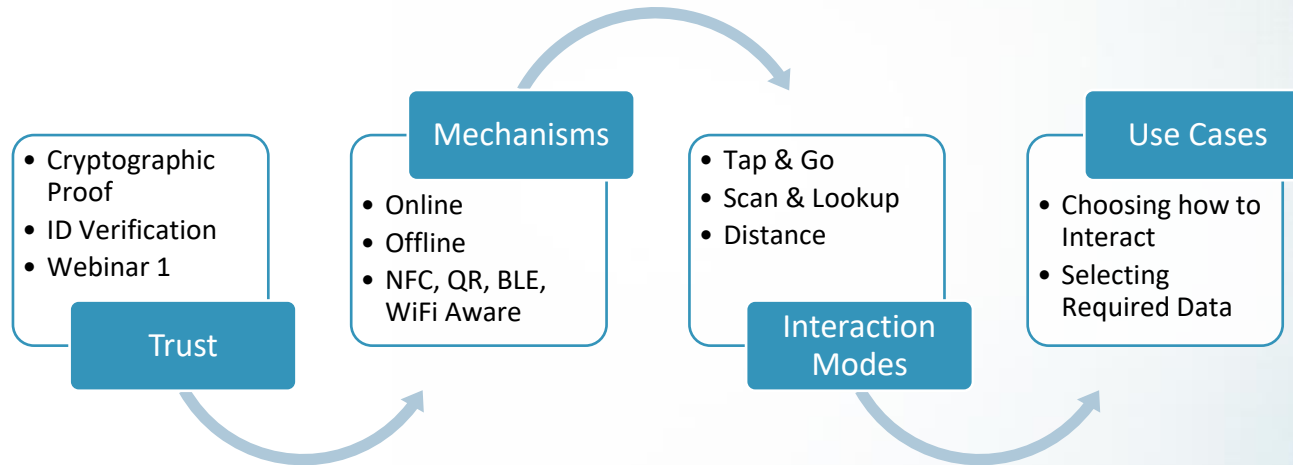
mDL promises a revolution in Customer Service delivery – we can now trust identity from distances, scenarios, and devices that we could not previously.

Will your company be ready to rely on Mobile ID and reap the benefits of mDL?

https://bit.ly/mDLWhitepaper

Webinar #2: Mobile Driver's License Uses

Trust
- Cryptographic Proof
- ID Verification
- Webinar 1

Mechanisms
- Online
- Offline
- NFC, QR, BLE, WiFi Aware

Interaction Modes
- Tap & Go
- Scan & Lookup
- Distance

Use Cases
- Choosing how to Interact
- Selecting Required Data

- Interaction Modes for an mDL
- Use Case Requirements
- How to Use the Secure Technology Alliance Use Case Template
- Example Use Case Interactions
- Alliance Resources Available Now

Register for the webinar at: https://attendee.gotowebinar.com/register/4477725226811143695

Q&A

Mobile Driver's License Webinar Series: Online Assessment

- Online knowledge assessment quiz available after each webinar in the series

- Participants in all four webinars and assessments receive a certificate and discounted registration to any future Alliance paid conference or educational event

- Assessment link:

  - https://www.surveymonkey.com/r/mDLQuiz1

Selected Resources

- **Mobile Driver's License and Ecosystem**, Secure Technology Alliance Identity Council white paper and FAQ https://www.securetechalliance.org/publications-the-mobile-drivers-license-mdl-and-ecosystem/

- **Secure Technology Alliance Knowledge Center** - https://www.securetechalliance.org/knowledge-center/

- **AAMVA Mobile Drivers License Resources** - https://www.aamva.org/mDL-Resources/

- **Draft International Standard ISO 18013-5, "Personal Identification — ISO-Compliant Driving Licence — Part 5: Mobile Driving Licence (mDL) application"** - https://isotc.iso.org/livelink/livelink?func=ll&objId=20919524&objAction=Open

Contact Information

- Randy Vanderhoof, rvanderhoof@securetechalliance.org

- Geoff Slagle, gslagle@aamva.org

- Mike McCaskill, MikeMcCaskill@flhsmv.gov

- David Kelts, dkelts@getgroupna.com

191 Clarksville Road
Princeton Junction, NJ 08550