SECURE TECHNOLOGY ALLIANCE

Privacy & Trust in the mDL Ecosystem

Identity Council Webinar

June 25, 2020

Introductions

- Randy Vanderhoof, Secure Technology Alliance

Who We Are

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."

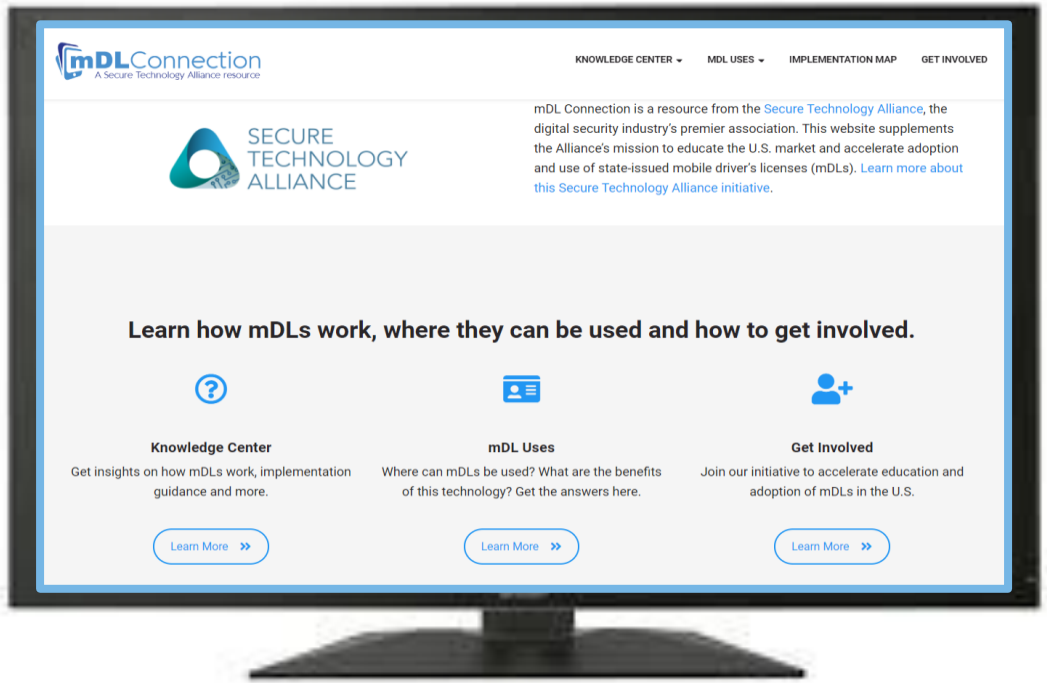
COUNCIL RESOURCES

- 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

SECURE TECHNOLOGY ALLIANCE

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



www.mdlconnection.com

Webinar Panelists

- Randy Vanderhoof, Secure Technology Alliance
- Matt Thompson, IDEMIA & Kantara Initiative
- John Wunderlich, Kantara Initiative
- Ted Sobel, DHS
- Dr. Christopher Williams, Exponent, Inc.
- Arjan Geluk, UL

SECURE TECHNOLOGY ALLIANCE

Privacy & Trust Model in the Federated Environment

Matt Thompson, IDEMIA

A CITIZEN & IDENTITY-DRIVEN FUTURE

Establish **citizen's identity** to access resources and preserve integrity

Enable **resource-sharing** while preserving **safety in a digital environment**

TRUST and CHOICE in a MODERN WORLD

Tailor context—from services to channels—and level of protection **to citizen preference**

Support **all interactions** across governments, businesses, citizens and 'things'

SECURE TECHNOLOGY ALLIANCE

SECURE TECHNOLOGY ALLIANCE

Privacy-Enhancing Features of ISO 18013-5 mDLs

John Wunderlich, Kantara Initiative

Privacy Life Cycle for mDL

Design Architecture for Privacy: User Choice

Privacy by Design

1. Proactive not Reactive
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality
5. End-to-End Security
6. Visibility and Transparency
7. User Centric

mDL Architecture

- ✓ Data Transfer Model presumes user involvement (#1, #3, #6) S 6.2
- ✓ Transactions initiated by the mDL Holder (#1, #2, #3, #7) S 6.3.2.1
- ✓ Data minimization enabled (#3)
- ✓ Biometric templates (#5)

SECURE TECHNOLOGY ALLIANCE

Fulfilling Design Goals: Implementation Challenges

Design Requirements

1. User Initiation
2. Minimum Data Transfers
3. Secure Transfers

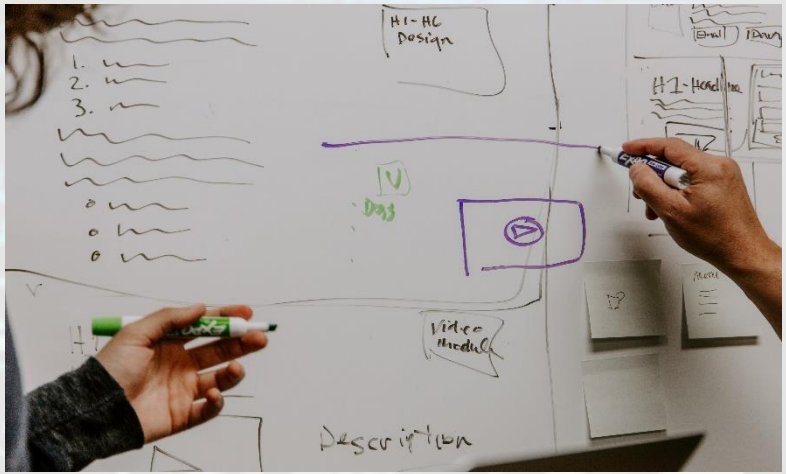


Photo by Kaleidico on Unsplash

Implementation Controls

- ✓ Training and Awareness for project staff
  - ✓ Importance of Non-Functional Requirements before Go-Live
- ✓ Assessments during Requirements or Design Processes:
  - ✓ Data Protection Impact Assessment
  - ✓ Privacy Impact Assessment
  - ✓ Threat/Risk Assessment
- ✓ Metrics and Reporting for
  - ✓ mDL Readers
  - ✓ mDL Holder
  - ✓ Regulators/Public

Closing the loop: Transparent Operation

What's the biggest lie on the Internet?
Yes, I have read and understood the Terms and Conditions, yada yada yada…

If you don't close the loop and show mDL holders why they should continue to trust you, your system will be at risk come the first adverse headline. **If a user is surprised when they discover how their data is being used, that is a privacy fail.**

Provide Transparency and Auditability:

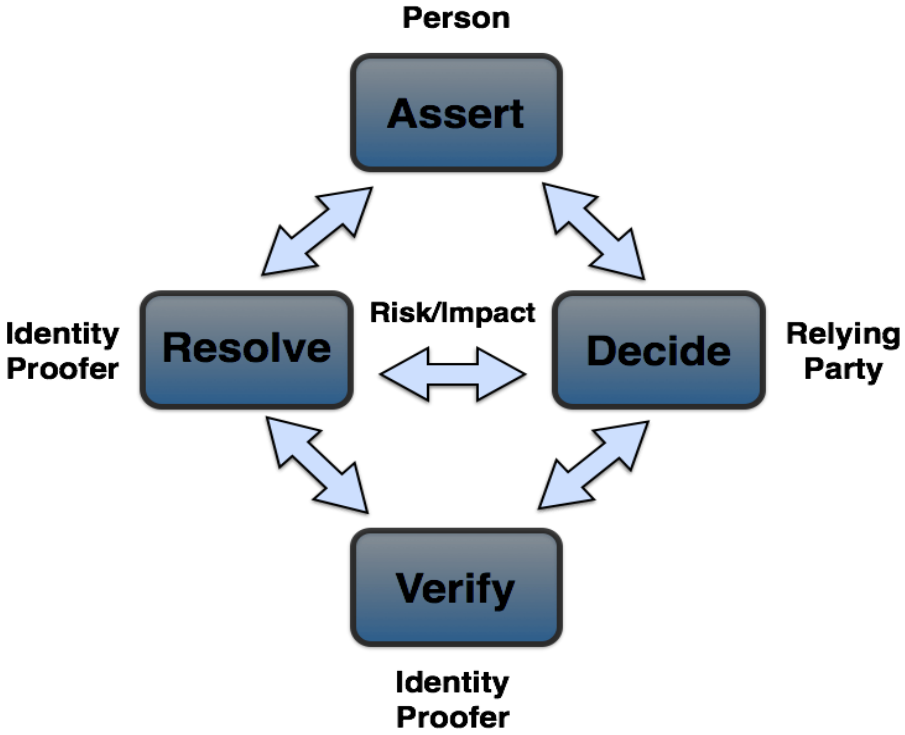
- Public summaries of PIAs
- Public summaries of Breach Reports
- User Portals for users to see how their data has been used
- Consider Kantara Consent receipts

SECURE TECHNOLOGY ALLIANCE

Identity Proofing, Issuance Processes and Relying Party Trust

Ted Sobel, DHS and Christopher Williams, Exponent, Inc.

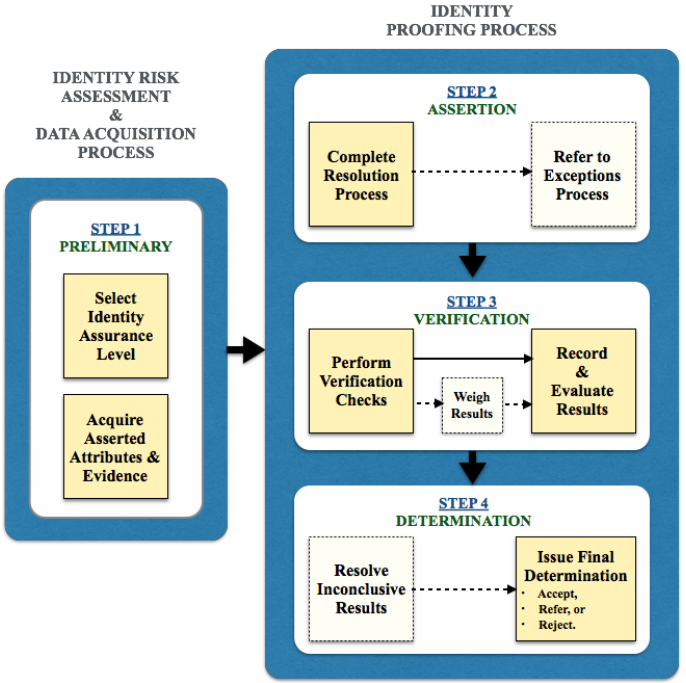
Roles and Relationships in Identity Proofing



Identity Proofing and Verification

Steps in Enrolling an Identity

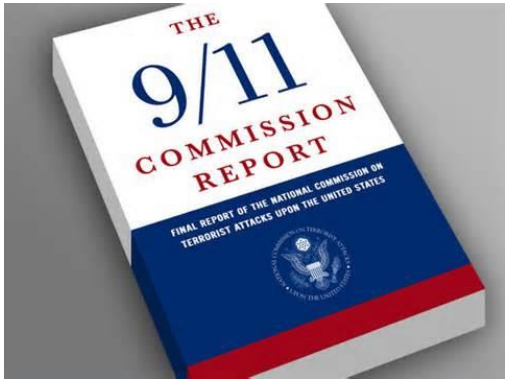
- Design considerations
  - Risk Assessment
  - Data Acquisition
- Identity Proofing
  - Assertion of a Unique Identity
  - Verification of Evidence
  - Determination



Source: Requirements and Implementation Guidelines for Assertion, Resolution, Evidence, and Verification of Personal Identity (ANSI/NASPO-IDPV-2018)

REAL ID Overview

- Establishes minimum security standards for issuance and production to Driver's Licenses and ID cards issued by 50 states, 5 territories, and DC
  - State participation is voluntary
  - Does not apply to tribal and local Identification or other forms of State ID
- Requires Proof of Identity & Lawful Status through **presentation & verification of documents** showing:
  - Full legal name;
  - Date of birth;
  - Social Security Number;
  - Address of principal residence; and
  - Lawful status.
- Requires Card Design to Include:
  - Biographic information, digital photo, signature, & card number;
  - Physical/Anti-counterfeit security features; and
  - Common machine-readable technology.
- Requires Safeguards for the Issuance and Production of Licenses
- Copy & retain source document information;
- Secure production facilities & document materials; and
- Background checks & fraudulent document training for employees.



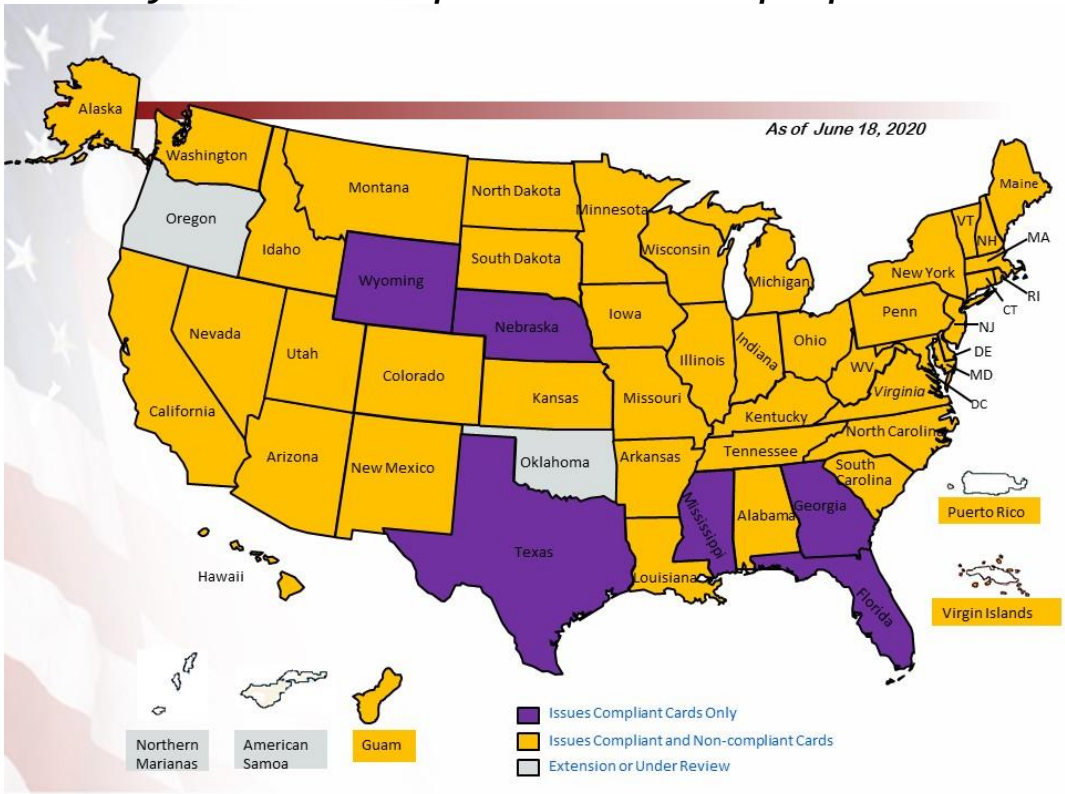
Sources of identification are the last opportunity to ensure that people are who they say they are…"

REAL ID: Compliant v. Non Compliant Cards

For any reason, a compliant state may also choose to offer a noncompliant card that clearly indicates that the document may not be accepted for official purposes

Noncompliance Statement

Compliance Mark



Trust in Issuance

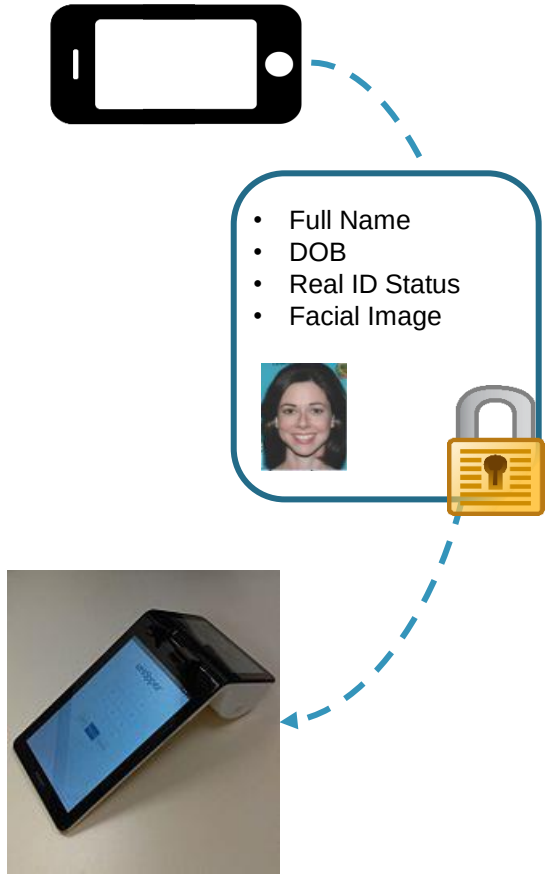
- How should Relying Parties trust the mDL data is legitimate and provisioned correctly?
  - *Look for the "Gold Star" compliance mark on the phone screen?*

Trust in Issuance

- How should Relying Parties trust the mDL data is legitimate and provisioned correctly?
  - *Look for the "Gold Star" compliance mark on the phone screen?* – **NO!**
- **Flash pass on phone screen is <u>very</u> insecure**
  - **Fake apps can easily be made to duplicate the appearance of an mDL**
  - **No way to visually verify the authenticity of an mDL**

Trust in Issuance

- How should Relying Parties trust the mDL data is legitimate and provisioned correctly?
  - *Look for the "Gold Star" compliance mark on the phone screen? – **NO!***
  - **Flash pass on phone screen is <u>very</u> insecure**
- All mDL data that is passed to the Relying Party will be cryptographically signed by the issuer



Trust in Issuance

- How should Relying Parties trust the mDL data is legitimate and provisioned correctly?
  - *Look for the "Gold Star" compliance mark on the phone screen?* – **NO!**
  - **Flash pass on phone screen is <u>very</u> insecure**
- All mDL data that is passed to the Relying Party will be cryptographically signed by the issuer

1. Verify these signatures by computing data hash functions and cryptographic signatures with the issuer's public key
2. **Only accept data that has been generated and signed by issuers <u>you</u> <u>trust</u>**
3. Verify the issuer signed facial image matches that of the person presenting the ID
   - Through an in person visual comparison
   - Facial recognition algorithm which does match on Relying Party hardware

SECURE TECHNOLOGY ALLIANCE

Testing & Certification of mDL Processes and Solutions

Arjan Geluk, UL

Testing and Certification of mDL Processes and Solutions

- Ensuring Trust in mDL standards
  - Testing started 5+ years ago!
  - mDL Test Events
- Ensuring Trust in mDL Processes and Solutions
  - For whom? – primary stakeholders
  - What? – testing processes and solution
  - Example: conformity assessment
- Harmonizing Trust in mDL Processes and Solutions
  - Towards certification
  - Conveying trust

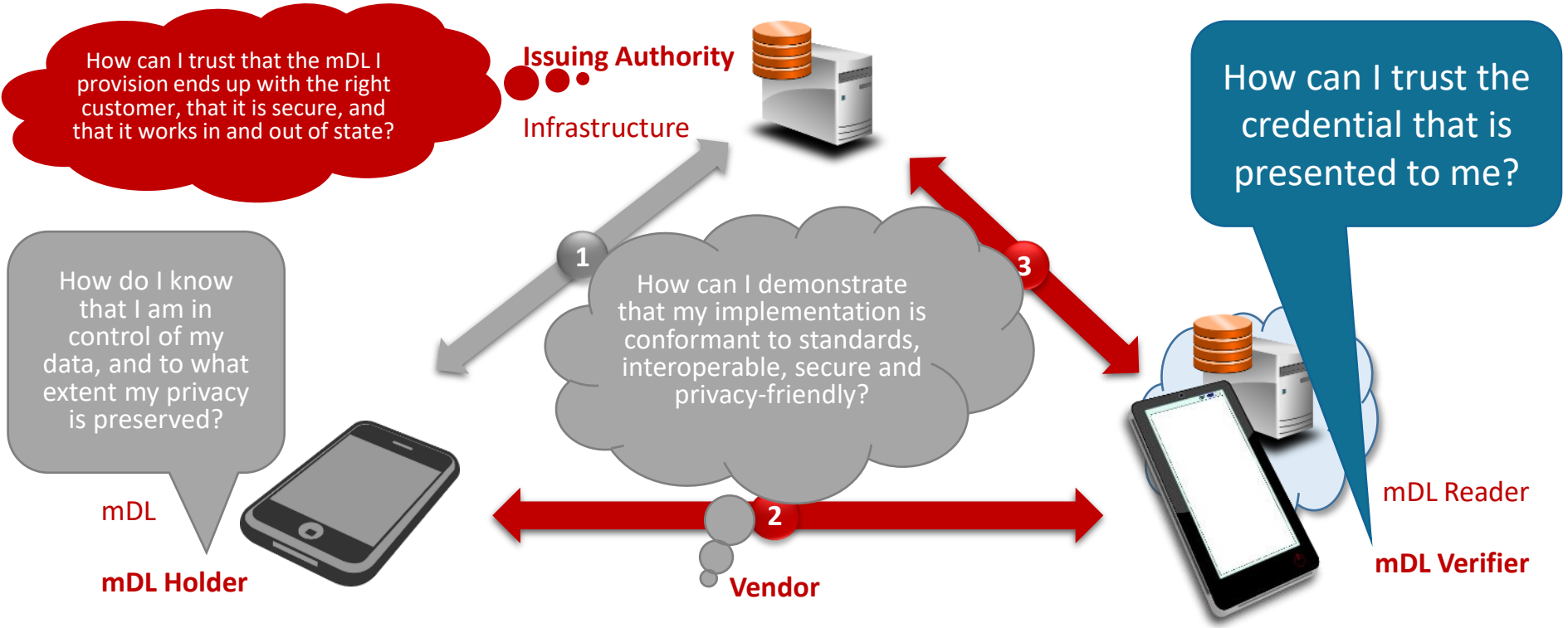
Ensuring trust in mDL – testing started 5+ years ago!

- Feb. 2014: ISO mDL Task Force established
- Dec. 2014: **test ideas** – put a chip on a DL, or a DL on a chip?
  - First prototype of a functioning ISO 18013-2/3 compliant DL on a SIM card, using NFC with Android and Windows phone demo apps
- 2015/16: functional needs (AAMVA) & technical concepts (ISO) merge
  - First Working Draft of ISO/IEC 18013-5 on mDL
- 2016/17: **prove concepts** proposed for standardization - reality check
  - mDL PoC by RDW and AAMVA (https://youtu.be/cFoSvMabBaE)

SECURE TECHNOLOGY ALLIANCE

2018-19-20: mDL test events – vetting the standard

Ensuring Trust in mDL processes and solutions – for whom?



Ensuring Trust in mDL processes and solutions – what?

Accept **qualifying technology** of a **qualifying vendor** for operational use

Issuing Authority (IA)

Define IA Policies, governing security, enrolment & issuance processes and technology

Review/audit of policies, processes, practices and technology used for enrolment and issuance of the mDL

Publish IACA public key certificate and **audited** Security Policy and Certificate Policy

Review IA Policies, and add the IACA certificate of **qualifying IAs** to certificate store or Master List

standards conformity assessment (functional + security protocols)
Privacy assessment
Security evaluation

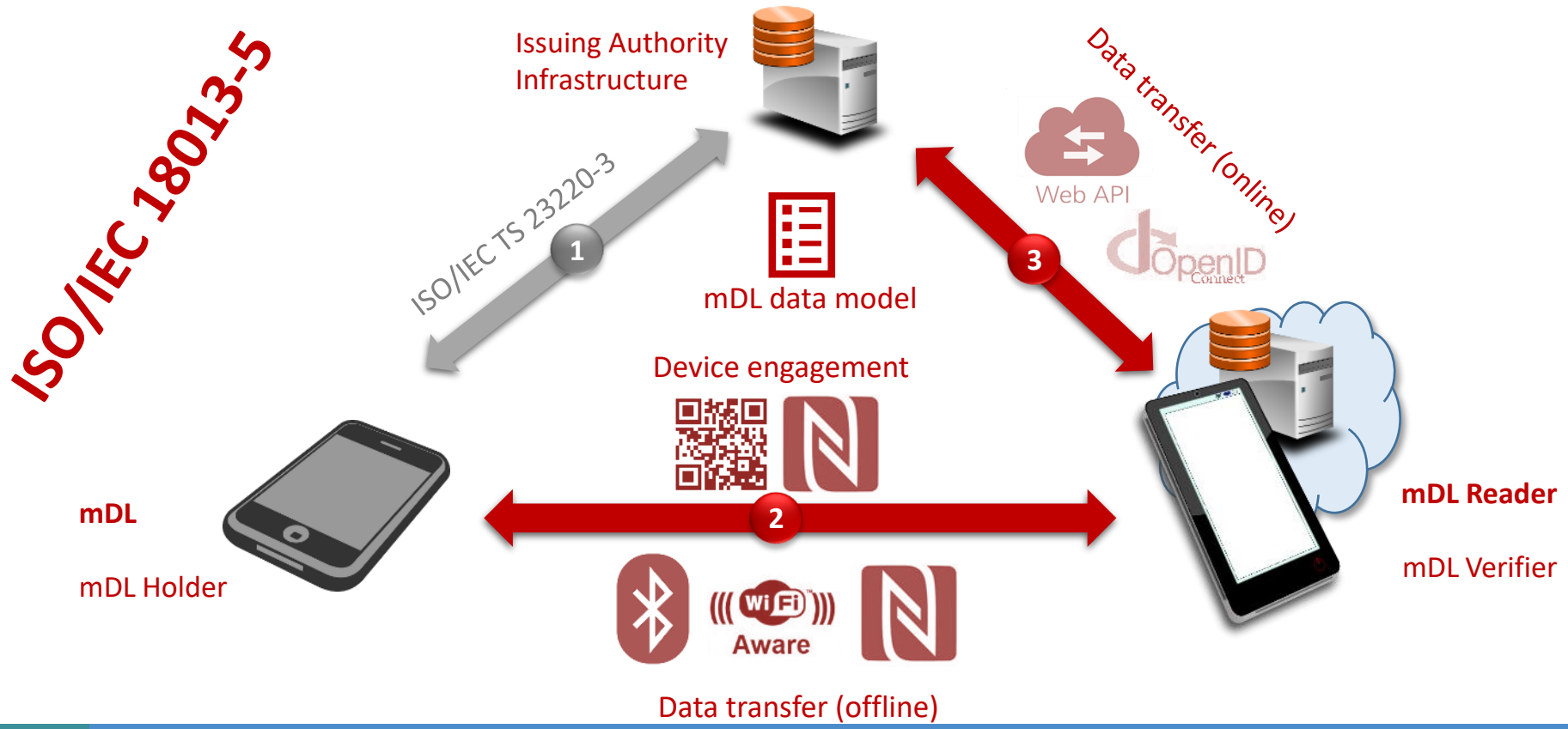
Define requirements for vendor processes and technology (privacy, security, standards conformity)

mDL Holder

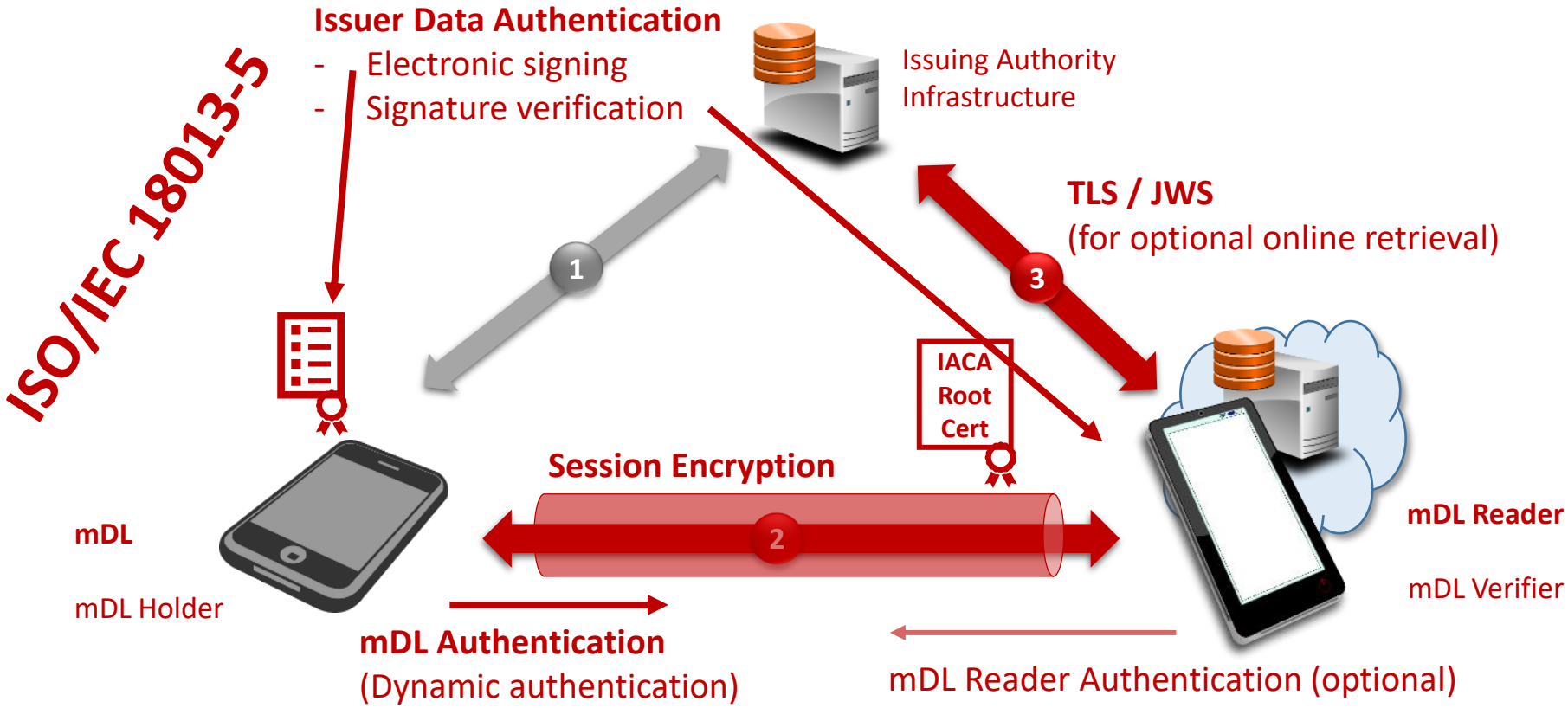
Vendor(s)

mDL Verifier

Ensuring trust in mDL: conformity assessment (functional)



Ensuring trust in mDL: conformity assessment (security)

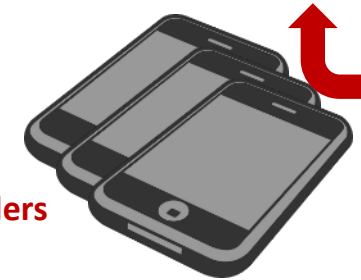


Harmonizing Trust in mDL processes and solutions – how?

Trusted Master List with mDL Provider Attestation CA certificates of **certified** mDL solutions

Certify

standards conformity assessment (functional + security protocols)
Privacy assessment
Security evaluation



mDL Holders

Issuing Authorities

Common IA Policies, governing security, enrolment & issuance processes and technology

Publish **certified** Security Policy and Certificate Policy and IACA public key certificate

Common requirements for vendor processes and technology (privacy, security, standards conformity)

Vendors

Review/audit of policies, processes, practices and technology used for enrolment and issuance of the mDL

Certify

Trusted Master List with IACA certificates of **certified** Issuing Authorities

mDL Verifiers

SECURE TECHNOLOGY ALLIANCE

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/mDLQuiz3

Selected Resources

- **Introduction to the mDL Webinar and mDL Use Cases Recordings** - https://www.securetechalliance.org/activities-events-webinars/
- **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
- Matt Thompson, Matt.Thompson@us.idemia.com
- John Wunderlich, john@wunderlich.ca
- Ted Sobel, ted.sobel@hq.dhs.gov
- Christopher Williams, cwilliams@exponent.com
- Arjan Geluk, Arjan.Geluk@ul.com

SECURE TECHNOLOGY ALLIANCE

SECURE
TECHNOLOGY
ALLIANCE

191 Clarksville Road
Princeton Junction, NJ 08550