SECURE TECHNOLOGY ALLIANCE

Challenges to the mDL Ecosystem

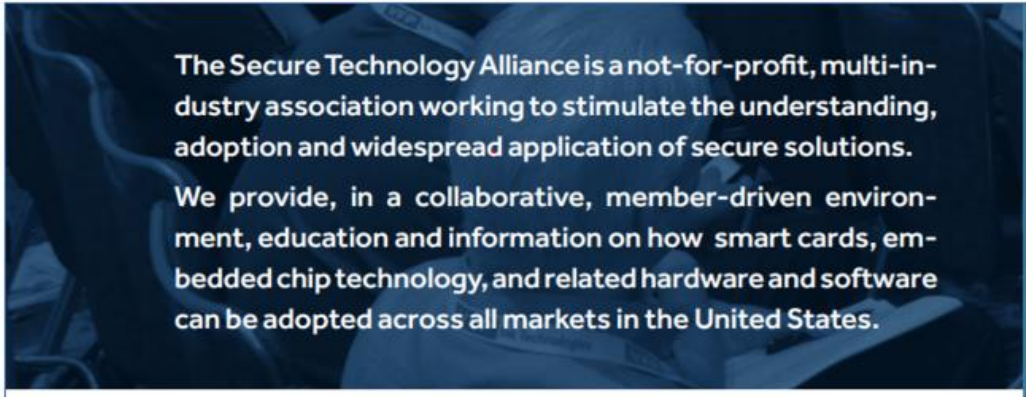
Identity Council Webinar

October 28, 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

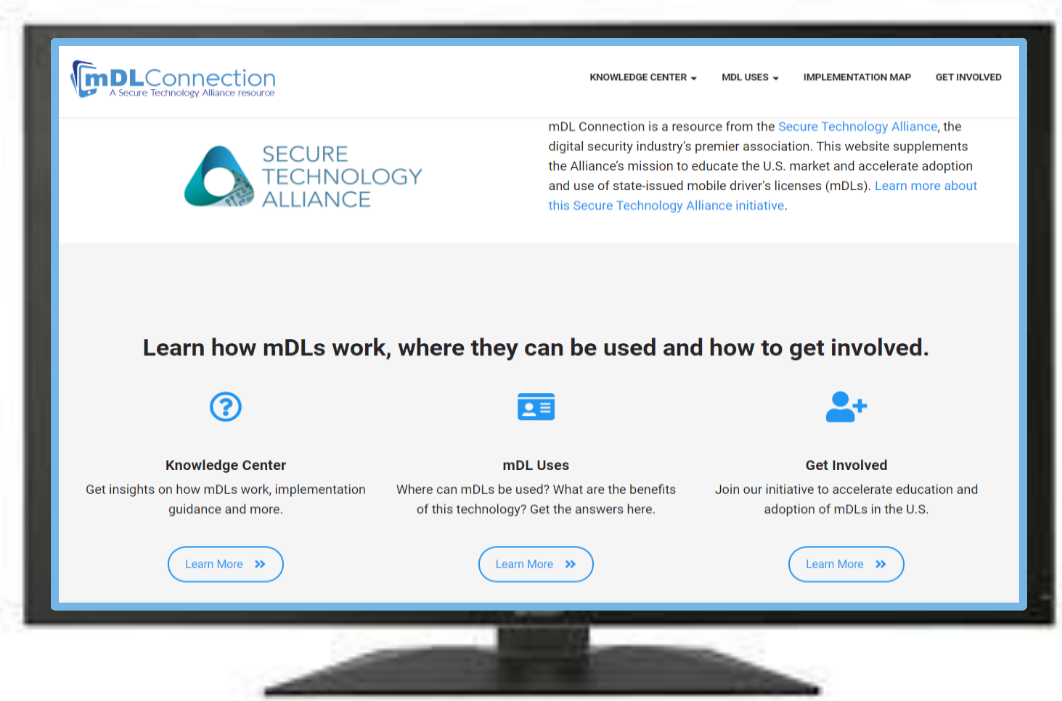
- Assurance Levels Overview and Recommendations
- FICAM in Brief: A Smart Card Alliance Summary of the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance
- Identifiers and Authentication – Smart Credential Choices to Protect Digital Identity
- Identity Management 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

SECURE TECHNOLOGY ALLIANCE

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



mDL Connection is a resource from the Secure Technology Alliance, the digital security industry's premier association. This website supplements the Alliance's mission to educate the U.S. market and accelerate adoption and use of state-issued mobile driver's licenses (mDLs). Learn more about this Secure Technology Alliance initiative.

Learn how mDLs work, where they can be used and how to get involved.

Knowledge Center
Get insights on how mDLs work, implementation guidance and more.

mDL Uses
Where can mDLs be used? What are the benefits of this technology? Get the answers here.

Get Involved
Join our initiative to accelerate education and adoption of mDLs in the U.S.

www.mdlconnection.com

Webinar Panelists

- Randy Vanderhoof, Secure Technology Alliance
- David Kelts, GET Group North America
- Mindy Stephens, AAMVA
- Loffie Jordaan, AAMVA
- Arjan Geluk, UL
- Tom Lockwood, NextgenID

SECURE TECHNOLOGY ALLIANCE

SECURE TECHNOLOGY ALLIANCE

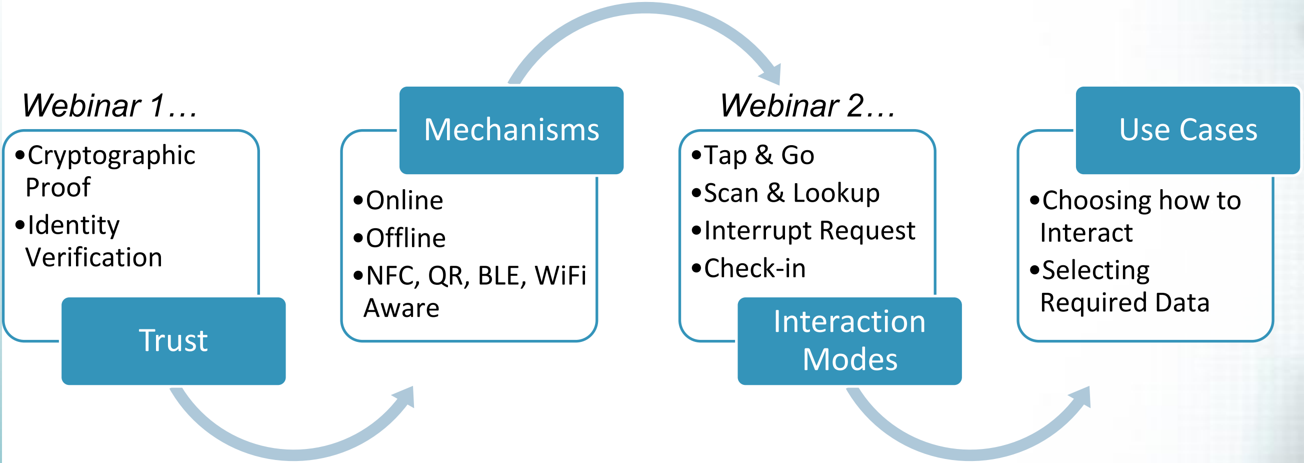
The Mobile Driver’s License (mDL) Ecosystem

October 28, 2020, **David Kelts**, *GET Group North America*

SECURE
TECHNOLOGY
ALLIANCE

Trust creates the Context of this “Challenges” Webinar

Webinars 1-3: Mobile Driver’s License, Trust & Uses



Webinar 1…

- Cryptographic Proof
- Identity Verification

Trust

Mechanisms

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

Webinar 2…

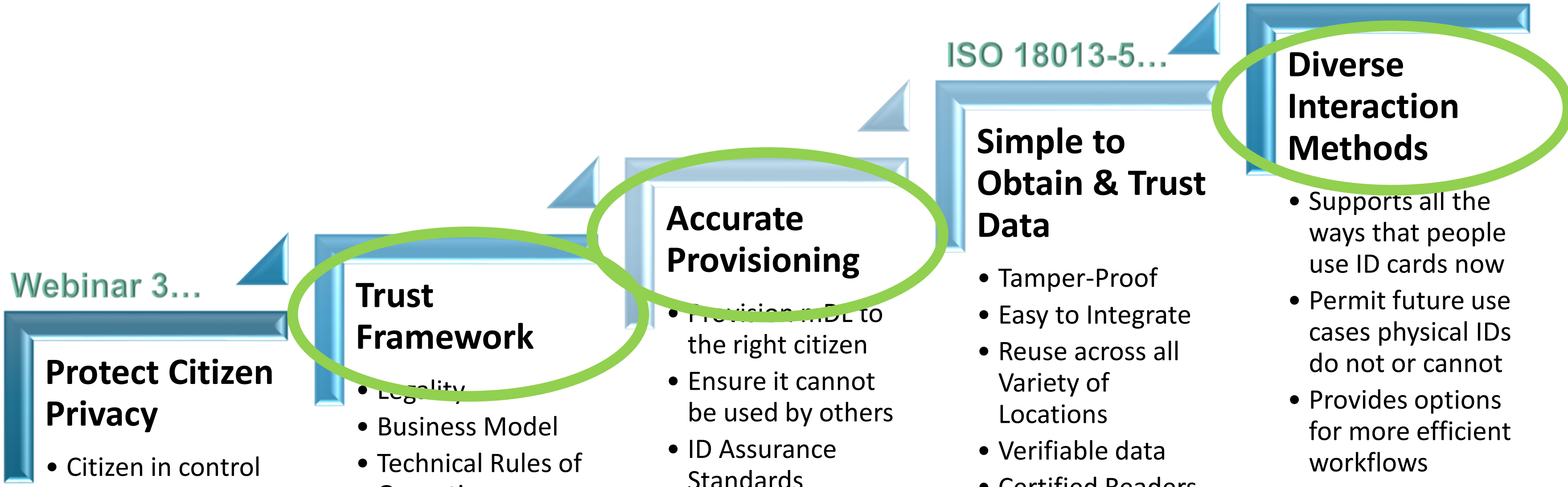
- Tap & Go
- Scan & Lookup
- Interrupt Request
- Check-in

Interaction Modes

Use Cases

- Choosing how to Interact
- Selecting Required Data

How do we build **trust** for **widespread** mobile identity?



Webinar 3…

Protect Citizen Privacy

- Citizen in control
- Transparent Operation
- No hidden monetization or data leaks
- Not Trackable

Trust Framework

- Legality
- Business Model
- Technical Rules of Operation
- ID Assurance Levels
- Global Exchange

Accurate Provisioning

- Provision mDL to the right citizen
- Ensure it cannot be used by others
- ID Assurance Standards

ISO 18013-5…

Simple to Obtain & Trust Data

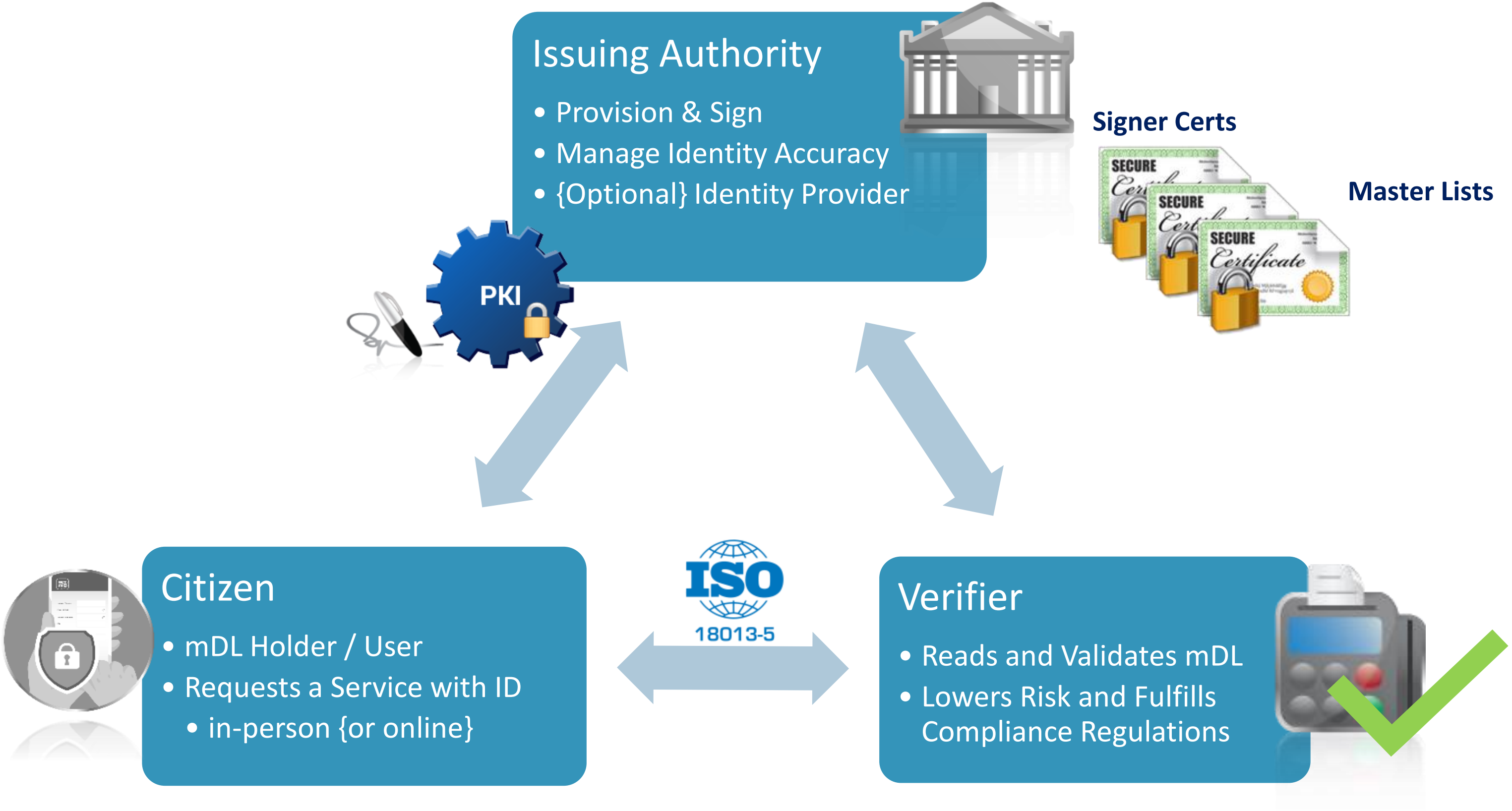
- Tamper-Proof
- Easy to Integrate
- Reuse across all Variety of Locations
- Verifiable data
- Certified Readers

ISO

Diverse Interaction Methods

- Supports all the ways that people use ID cards now
- Permit future use cases physical IDs do not or cannot
- Provides options for more efficient workflows
- **= Accepted Everywhere**

Trust Mechanisms - ISO 18013-5 mDL & mID



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

Cryptographic Trust in the ID provided by ISO 18013-5

AAMVA

American Association of
Motor Vehicle Administrators

Verifier Assurance

October 28th, 2020

OUR VISION

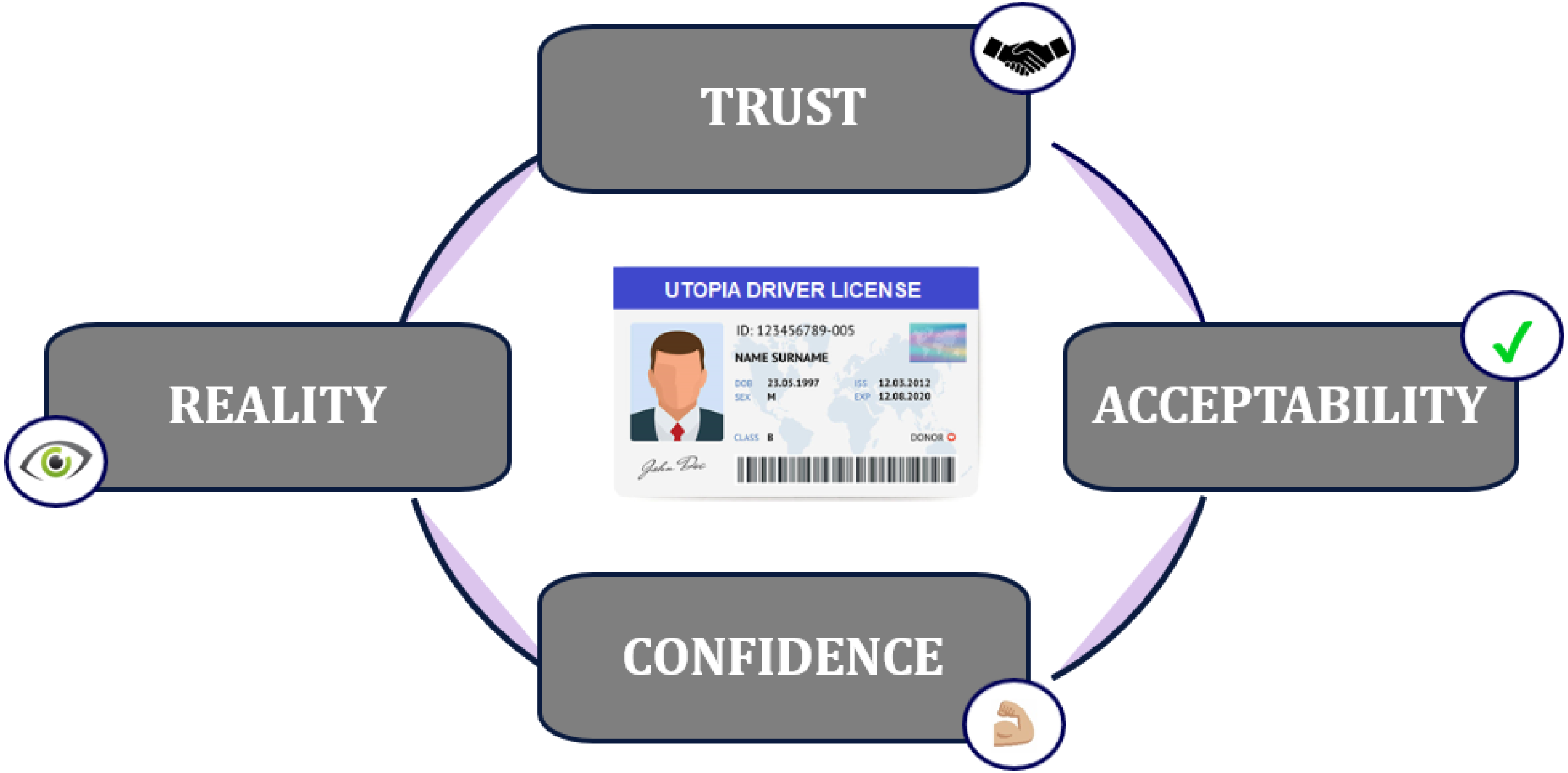
Safe drivers
Safe vehicles
Secure identities
Saving lives!

Agenda

- Existing trust model (physical credentials)
  - Confidence/Trust in Issuing Authorities
  - REAL ID Standards for Vetting and Proofing
- Vision for Mobile Driver License
  - Continued confidence/trust in Issuing Authorities
  - Provisioning Guidelines for Issuing Authorities
  - Trust model

Trust Model for Physical Credentials

Verifier Confidence in IA



TRUST

ACCEPTABILITY

CONFIDENCE

REALITY

REAL ID Standards

Published 2008

Establishes minimum standards for state issued DLs/IDs to be used for federal ID purposes

Compliance

Date pushed out one year for states to Oct 1st, 2021

Requirements

Minimum documentation requirements and issuance standards

Non-REAL ID

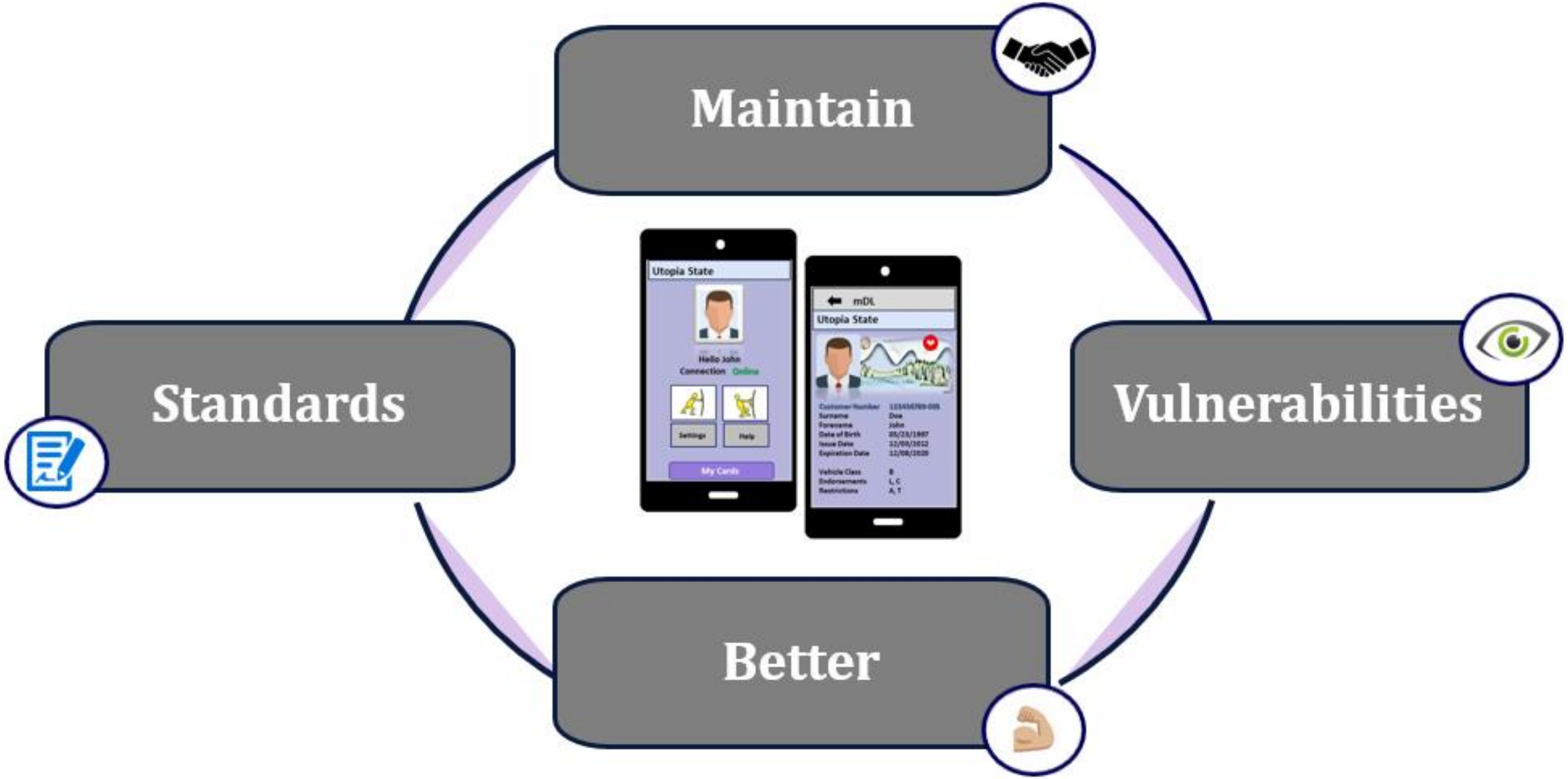
Issuing Authorities still offer other types of credentials

Improvement

Standards improve ID proofing and vetting process, creating stronger confidence and trust in DLs/IDs

Vision for Mobile Driver License

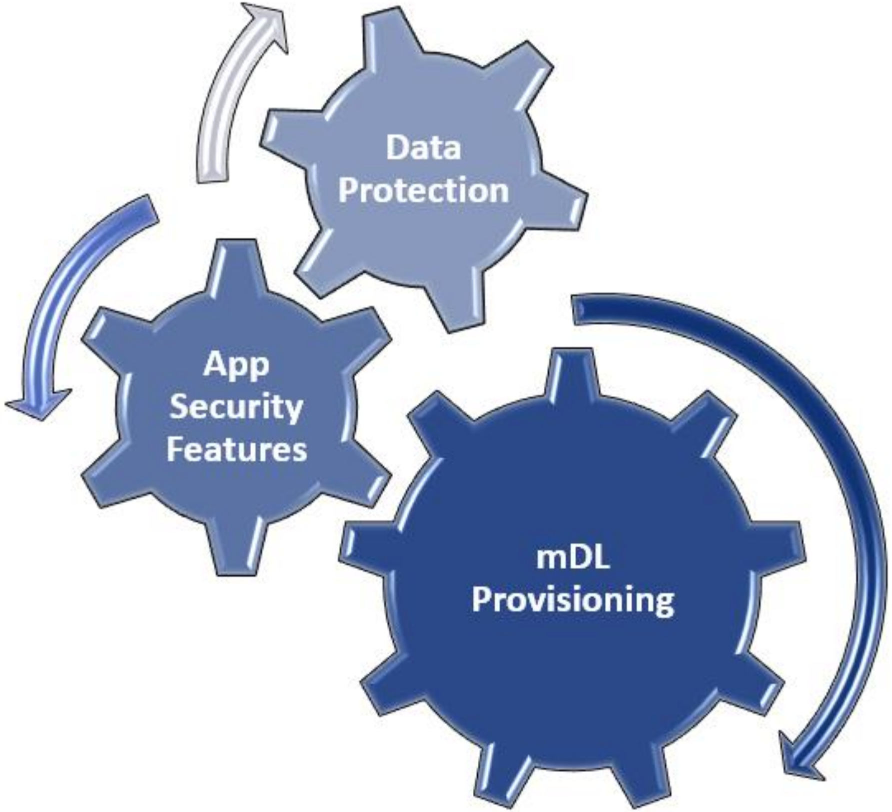
Verifier Confidence in IA



Customer Number 123456789-005
Surname Doe
Forename John
Date of Birth 05/23/1987
Issue Date 12/08/2012
Expiration Date 12/08/2020

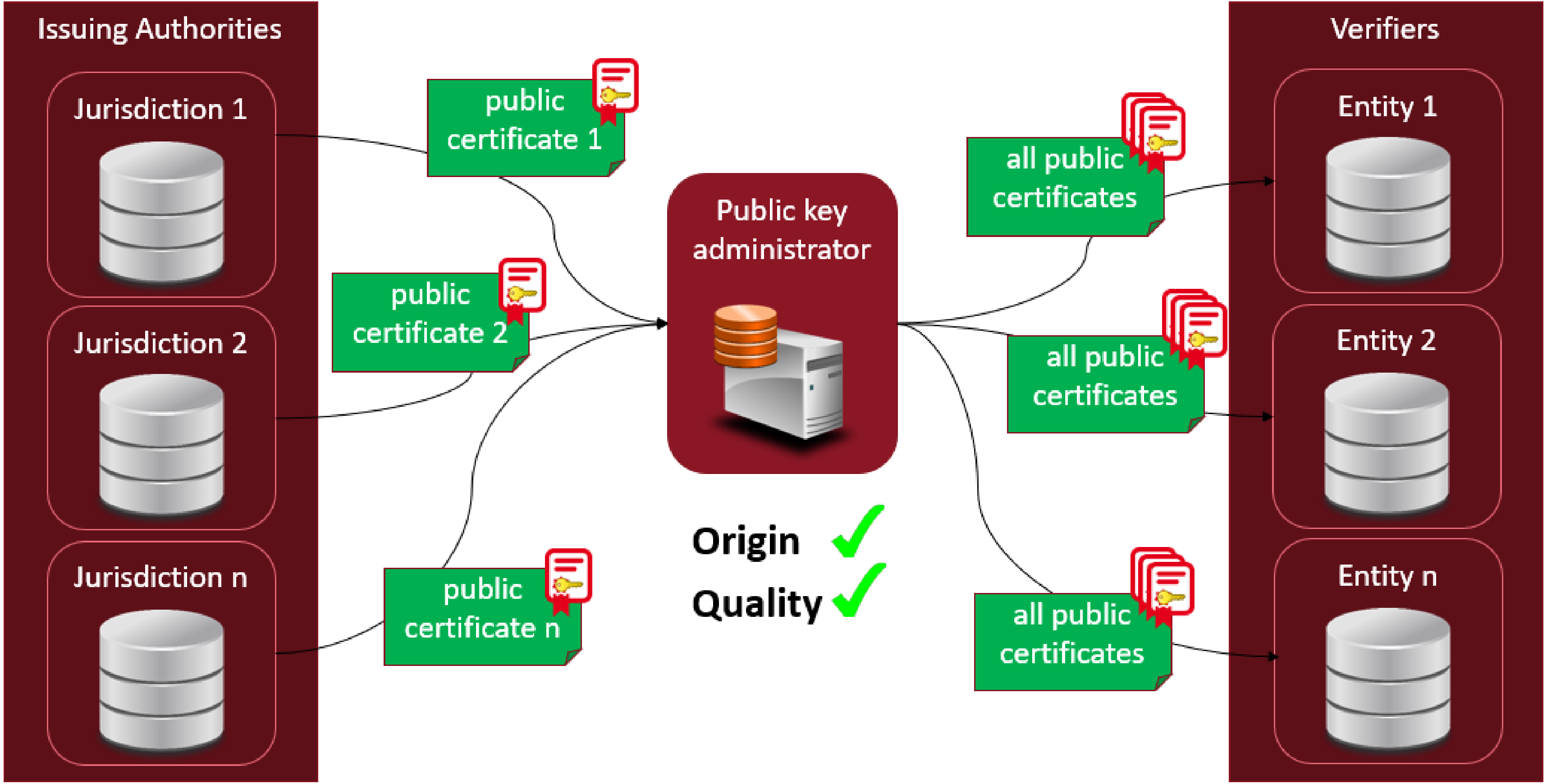
Vehicle Class B
Endorsements L, C
Restrictions A, T

Provisioning Guidance



American Association of Motor Vehicle Administrators

Trust Model – Public Key Administration



Contact Information

Mindy Stephens

mstephens@aamva.org

+1.571.201.3472

Loffie Jordaan

ljordaan@aamva.org

+1.703.908.5864

SECURE TECHNOLOGY ALLIANCE

Issues & Risks to mDL Ecosystem Adoption & Expansion

October 12, 2020, **David Kelts**, *GET Group North America*

Opportunities to Kick-Start a Robust mDL Ecosystem

Full-Featured ISO 18013-5 Rollout

(Whitepaper 6.1)

- **Robust** Interaction Modes give Verifiers choice in how they accept mDLs to fit their business
- Few connect and transfer options could leave Verifiers deciding to wait to deploy

Jumpstarting the mDL Ecosystem

(Whitepaper 6.11)

- Driving Forces, Market Forces
- New Market Opportunities
- What incentives exist, or could be created, that will help us start on the right path?
  - For Issuers?
  - For Consumers?
  - For Verifiers?

SECURE TECHNOLOGY ALLIANCE

The Variety of Ways Verifiers May Want to Accept mDL

While we continue to accept all PAYMENTS
Please Consider Card or Contactless Payments When Possible. Thank You!

Restaurant

- QR Scan over your shoulder
- Quick Online Request to IA

TSA/Travel

- NFC Tap
- WiFi Aware Data Transfer
- No BLE for Security Policy
- Avoid Connectivity for Security Policy

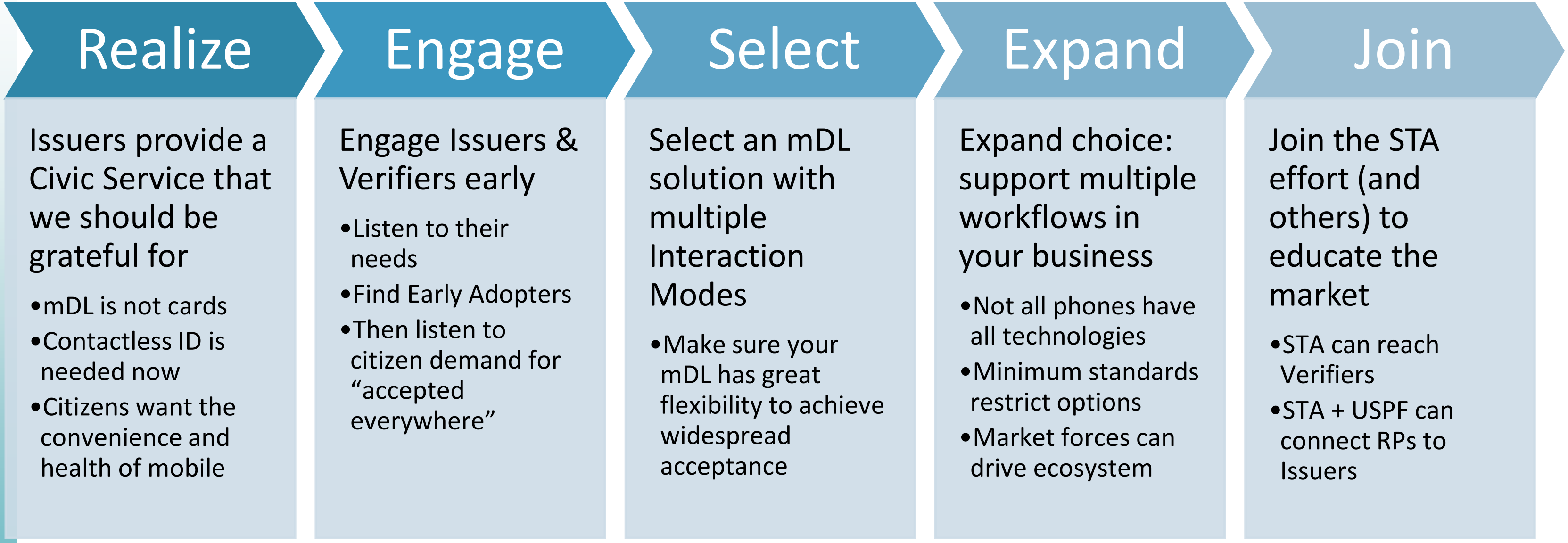
Supermarket

- Existing Connected NFC POS Device
- NFC Tap
- Online Request falls back to NFC Data Transfer

Law Enforcement

- Roadside Stop – Car to Car/Truck
- Distance Connection
- Online Request falls back to BLE Data Transfer

Working Together to Make a Rich mDL Ecosystem



Realize

Issuers provide a Civic Service that we should be grateful for

- mDL is not cards
- Contactless ID is needed now
- Citizens want the convenience and health of mobile

Engage

Engage Issuers & Verifiers early

- Listen to their needs
- Find Early Adopters
- Then listen to citizen demand for “accepted everywhere”

Select

Select an mDL solution with multiple Interaction Modes

- Make sure your mDL has great flexibility to achieve widespread acceptance

Expand

Expand choice: support multiple workflows in your business

- Not all phones have all technologies
- Minimum standards restrict options
- Market forces can drive ecosystem

Join

Join the STA effort (and others) to educate the market

- STA can reach Verifiers
- STA + USPF can connect RPs to Issuers

Pulling a Nascent Marketplace Together

Consumer Has the Demand

Consumers may not adopt until they know where they can use mDL

Channels to tell Issuers & Verifiers of Needs & Protections they Desire

Choice in mDL Apps is possible in some Issuer models

mDL Demand:

Leave purse or wallet home
Convenience and Speed
Accepted Everywhere
Health & Safety
Privacy Protection

Verifiers Hold the ID Risk

Verifiers may not adopt until seeing a significant number of mDLs

Card Standards have made their risk lower and their job easier… **ISO 18013-5**

Used to complying with identification regulations

mDL Fulfills:

- Not Accepting Fakes / Spoofs
- Faster Processing
- Personalized Service
- Health & Safety of Employees

How can we, as Secure Tech Alliance, assist…?

Build Channels to hear Consumers, Issuers, & Verifiers

Create Incentives for Participants to start early

Ensure all citizens have access to full-featured solutions

Educate about the benefits of adopting early

Expand the Options to Consumers AND Verifiers

SECURE
TECHNOLOGY
ALLIANCE

mDL promises a revolution in Customer Service delivery – we can now trust identity from distances, scenarios, and devices that we could not previously.

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

SECURE TECHNOLOGY ALLIANCE

Testing & Certification

Arjan Geluk, UL

Ensuring trust in mDL standards – vetting ISO/IEC 18013-5

AAMVA

Austroads

EReg
ASSOCIATION OF EUROPEAN VEHICLE AND DRIVER REGISTRATION AUTHORITIES

UL

cbn
CANADIAN BANK NOTE
COMPANY, LIMITED

Panasonic

SAMSUNG

Google

IDEMIA
augmented identity

GET
NORTH AMERICA
GROUP

TOSHIBA

gemalto
a Thales company

FAST
ENTERPRISES

OSD

UTMS
JAPAN

SCYTALES

HID

THALES

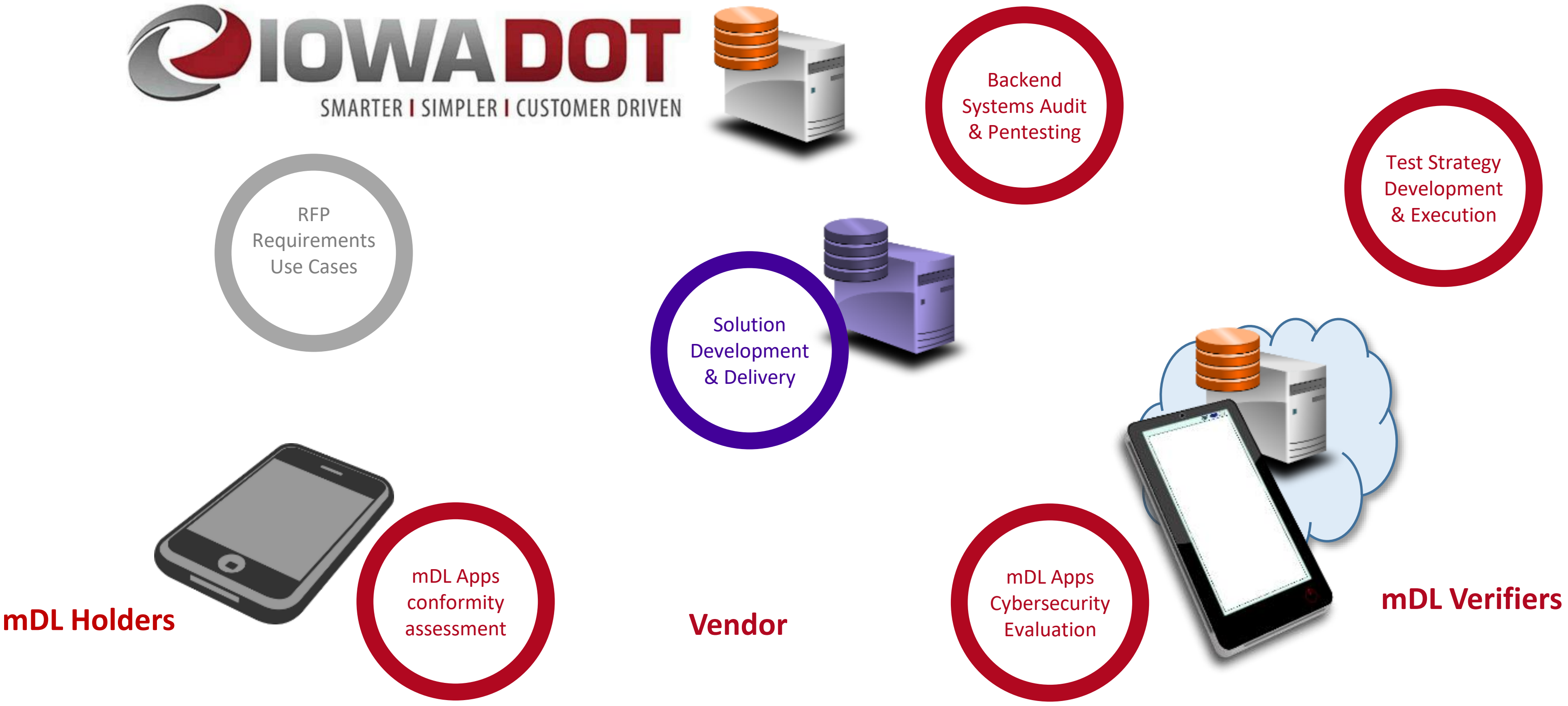
multicert

bdr.
BUNDESDRUCKEREI

YOUNIQX

VERIDOS
IDENTITY SOLUTIONS

Case study: mDL Assurance in Iowa



IOWA DOT
SMARTER | SIMPLER | CUSTOMER DRIVEN

RFP
Requirements
Use Cases

Backend
Systems Audit
& Pentesting

Test Strategy
Development
& Execution

Solution
Development
& Delivery

mDL Holders

mDL Apps
conformity
assessment

Vendor

mDL Apps
Cybersecurity
Evaluation

mDL Verifiers

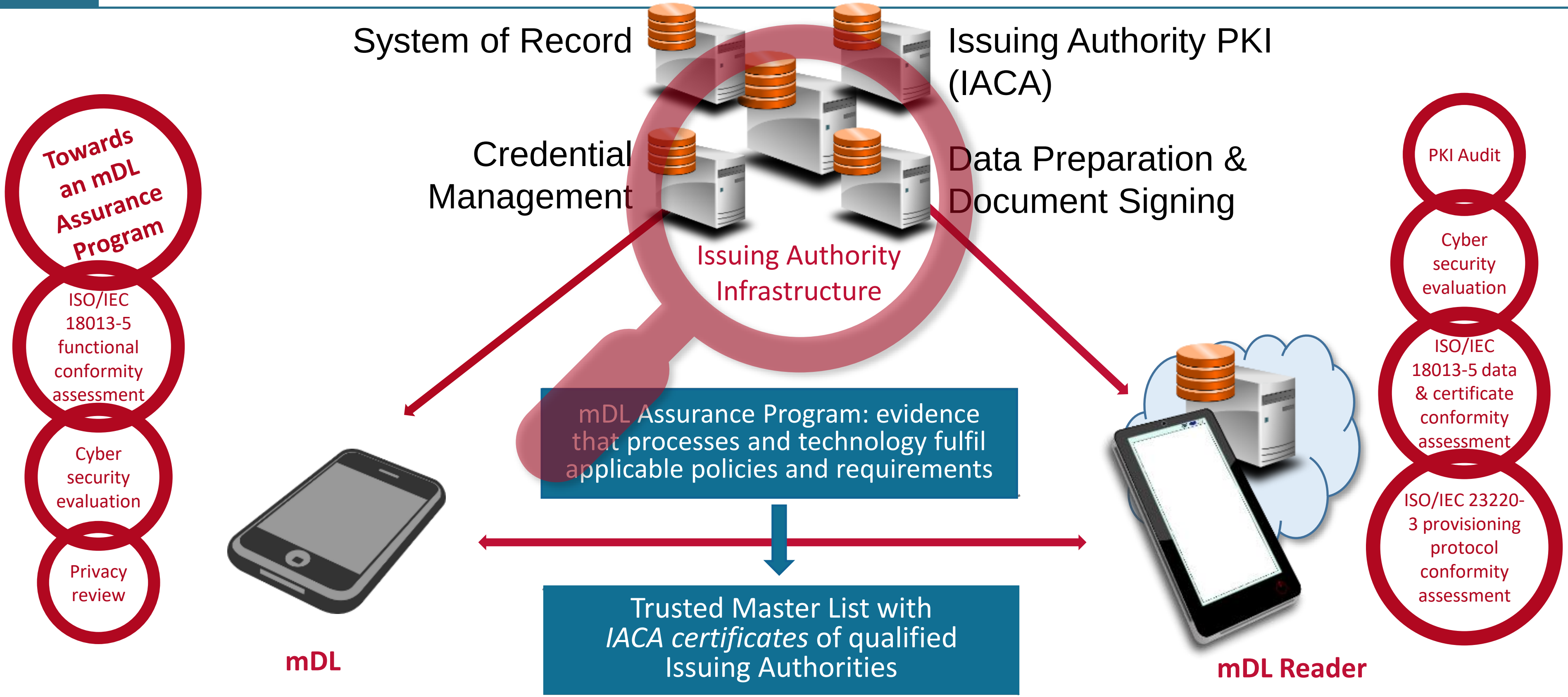
Case Study: mDL Assurance in Iowa

"The testing and security evaluation activities have provided real value towards the assurance that the Iowa mDL is conforming to the latest ISO standard, and to confirm that appropriate security measures are in place, both with our agency and with our vendor. This value is not only for Iowa as an individual jurisdiction, but also for other states and stakeholders in the mDL ecosystem. ***We encourage the adoption of an mDL assurance program****, as it really helps to* ***jointly achieve the shared goal of trustable, interoperable mDL solutions****."*

IOWA DOT
SMARTER | SIMPLER | CUSTOMER DRIVEN

Melissa Gillett
Director, Motor Vehicle Division

mDL Assurance: IA policies, processes and technology



Towards an mDL Assurance Program

ISO/IEC 18013-5 functional conformity assessment

Cyber security evaluation

Privacy review

System of Record

Issuing Authority PKI (IACA)

Credential Management

Data Preparation & Document Signing

Issuing Authority Infrastructure

mDL Assurance Program: evidence that processes and technology fulfil applicable policies and requirements

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

mDL

mDL Reader

PKI Audit

Cyber security evaluation

ISO/IEC 18013-5 data & certificate conformity assessment

ISO/IEC 23220-3 provisioning protocol conformity assessment

SECURE
TECHNOLOGY
ALLIANCE

Secure Technology Alliance mDL Initiative

Tom Lockwood, Alliance Vice Chair - Technology, Council Chair, mDL Lead

Alliance’s Mobile Driver’s License Efforts

Identity Council (IDC) Activities

1). *IDC mDL Awareness, Education and Coordination efforts*

a). *IDC Webinars* - Webinar Series, Individual Webinars, online Demonstrations, & Educational Workshops

b). *mDL Relying Party Focused Activities* - Online and In-Person Demonstrations, Mini-Workshops, Workshops, Conferences

c). *mDL Guidance Documents* - Consensus-based promoting standard based and best practices.

d). *mDL Adoption Needs & Challenges* - Webinars, Guidance, Policy Documents, White Papers, Workshops

2). *Various identity Policies, Process, technologies, Best Practices & Advancement* - Industry Reviews, Projects, Conferences, Special Activities

3). *New/Anticipated Identity Council Priorities* - Industry Reviews. Conference Support, Special Activities, New / Diverse ID Council priorities

4). *IDC Partnering Projects* - Multiple Efforts Including mDL

Consider direct participation in mDL awareness, education and coordination activities…

… form your own relying party working groups – we will work with you!

Alliance’s Mobile Driver’s License Efforts

Identity Council (IDC) mDL Core Project Group

Capability Providers

State Issuers
Manufacturers
Service Providers
Payment Infrastructure & Networks
Access Council
Standards Body
Trust Framework/Ecosystem
Provider Associations

Relying Parties

Private Sector

Merchants & Retailer
Transportation

- Aviation, Sea Port, Overland, Mass Transit

Health & Pharma
Automotive Rental Community
Beverage Community

Public Sector

States, County, City Governments
Federal: DoD (DMDC, DISA), DHS, GSA, ISC

Organizing Core Body of Capability Providers & Relying Parties ....and Relying Party Focused Community Work Groups

a). IDC Webinars

Introduction mDL Webinar 4 Part Series

✓ **Webinar #1 - mDL & Ecosystem Introduction & Strategic Intent**

✓ **Webinar #2 - mDL Capabilities Day 1 and Future (Primary focus is Day 1) & Use Case Examples**

- Strategic Intent: White Paper Chapters #2, Select use cases from appendix, Use Case Template
- Industry Panel: mDL Providers

✓ **Webinar #3 - Privacy & Trust in the mDL Ecosystem**

- Strategic Intent: White Paper Chapters #3-4, near-term strategic priorities of 5
- Panel: Trust Providers, Testers, Strategic Challenger Project Leads
- Privacy-enhancing features and inherent trust in the ISO 18013-5 mDL architecture

◍ **Webinar #4 – Early Relying Parties, Jump-starting Near-term Adoption and Challenges Ahead**

- Strategic Intent: Chapters 10 & Visibility to early Relying Parties / efforts
- Panel: Strategic Effort Leads, Relying Parties, USPF, TSA
- October 28 at 1pm ET/10am PT. Registration Link:

  https://securetechalliance.webex.com/securetechalliance/onstage/g.php?MTID=e4783ce208798231140cc84a966dab9a5.

Follow-on Webinars

mDL Relying Parties - Trust Across States (December)

b). Relying Party Focused Activities

Merchant & Retailer Uses Cases

Transportation

- Aviation Community Use Cases
- TSA Passenger & Crew Screening
- Rental Car Community Use Cases
- Ports Authority/APPA Uses Cases
- Transportation & Shipping Use Cases

Health & Medical Community Use Cases

- Insurance & Patient Enrollment
- Pharma consumer facing use cases

Federal Government Relying Parties

- Federal Interagency Security Committee
- GSA consumer/citizen facing use cases
- Department of Defense - multiple use cases

State, Local & Tribal Relying Parties

- Executive Branch
  - Citizen/Consumer facing transactions
- Judiciary Programs & Use-Case
- Legislative Programs & Use-Case
- Higher Education Systems

Food & Beverage Community Use Cases

- Online & In-person Restricted Consumer Purchases

Public Safety

- Law Enforcement - Multiple Use Cases
- Public Safety / First Responder Use Cases

c). mDL Guidance Documents

STA Relying Party Guidance - this effort is focused of Public & Private Sector Relying Parties in general. The proposed guidance document(s) intent is to support informed decisions on:

- Enterprise adoption, trust, & interoperability
- Interaction modes to accept mDLs;
- Gain the value inherent in ISO-based mDLs.

NASCIO & STA - National Association of State CIOs represent state leaders IT priorities, policies, best practices, and issues and challenges. STA is proposing to partner with NASCIO to:

- Leverage relying party guidance to support ISO standard based mDLs and best practices-base adoption guidance.
- NASCIO's SICAM provides common guidance and best practices for State Identity Credentialing and Access Management which should include mDL, potentially as a SICAM Annex.

d). mDL Adoption Needs & Challenges

Organizing Activities, Leading/Supporting Coalitions, & Integration of Efforts

Identity Council Activities - Notional Near-term Grouping & Priority:

6.1 - Least Common Denominator Roll-out
6.2 - Identity Enrollment Considerations
6.6 - Relying Parties/Trust Across States
6.11 - Jumpstarting the mDL Ecosystem

6.7 - Testing & Certification
6.8 - Considerations to Ensure Interoperability

6.4 - Online Model Challenges

6.5 - Trust Framework Considerations

The Mobile Driver's License & Ecosystem Paper, Chapter 6 identified technical and policy considerations…

…Alliance is organizing collaborative efforts to address needs and challenges to support confidence and adoption

Alliance Mobile Driver’s License Efforts

“The Ask”

- **Support awareness and education of ISO 18013-5 based mDLs**
- **Consider business processes & interactions relying upon driver’s licenses.**

  Where would an ISO 18013-5 based mDL:
  - Reduce Risks, Costs,
  - Enhance Quality of Life, Service, and User Experiences
  - Respond to Growing Interest in Touch-Free Experiences
- **Identify existing or form a new working group – mDL internal Discussion.**
  - Coordinate internal awareness, education and coordination activities.
- **Nominate representatives to participate in Alliance mDL activities**.

  Working jointly with relying parties & capability providers to:
  - Support commonality and reduce overlap, and support interoperability
  - Identify where mDL capabilities reduce risks, costs, or enhance user experiences
  - Discuss priority use cases and their characteristics/ requirements
  - Consider initial mDL adoption issues and implementation

SECURE
TECHNOLOGY
ALLIANCE

Q&A

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
- Mindy Stephens, MStephens@aamva.org
- Loffie Jordaan, LJordaan@aamva.org
- David Kelts, dkelts@getgroupna.com
- Arjan Geluk, Arjan.Geluk@ul.com
- Tom Lockwood, tlockwood@nextgenid.com

SECURE TECHNOLOGY ALLIANCE

191 Clarksville Road
Princeton Junction, NJ 08550