SECURE TECHNOLOGY ALLIANCE

mDL Uses Cases on Day One and Beyond

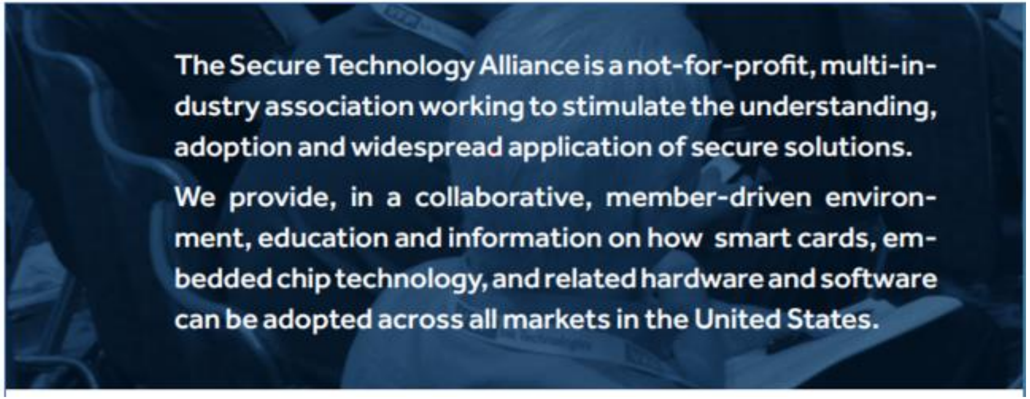
Identity Council Webinar

May 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

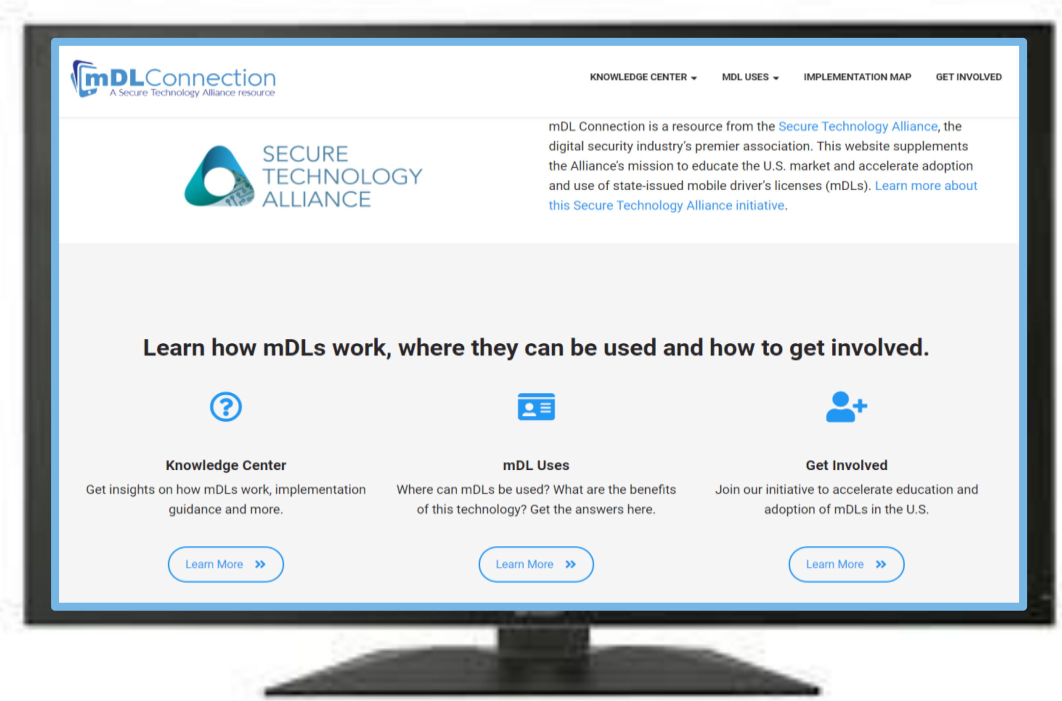
- Assurance Levels Overview and Recommendations
- FICAM in Brief: A Smart Card Alliance Summary of the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance
- Identifiers and Authentication – Smart Credential Choices to Protect Digital Identity
- Identity Management 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 NA
- Brandon Gutierrez, DHS TSA
- Andreas Aabye, Visa
- Paul Steier, AAMVA
- Justin Gage, Consult Hyperion
- Tom Lockwood, NextgenID

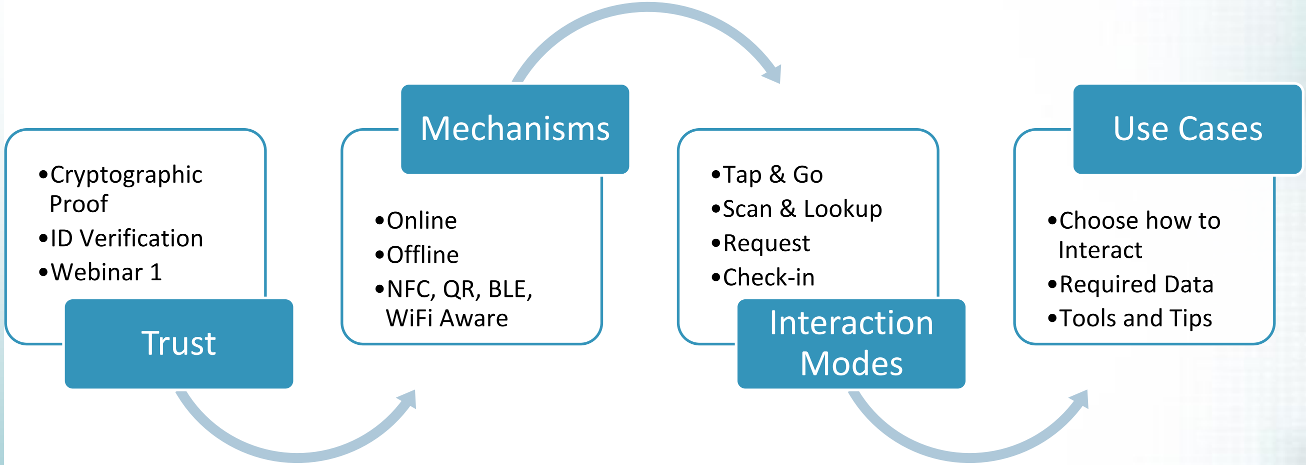
SECURE TECHNOLOGY ALLIANCE

SECURE TECHNOLOGY ALLIANCE

Mobile Driver’s License (mDL) Use Cases

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

Webinar #2: Mobile Driver's License Uses



Trust
- Cryptographic Proof
- ID Verification
- Webinar 1

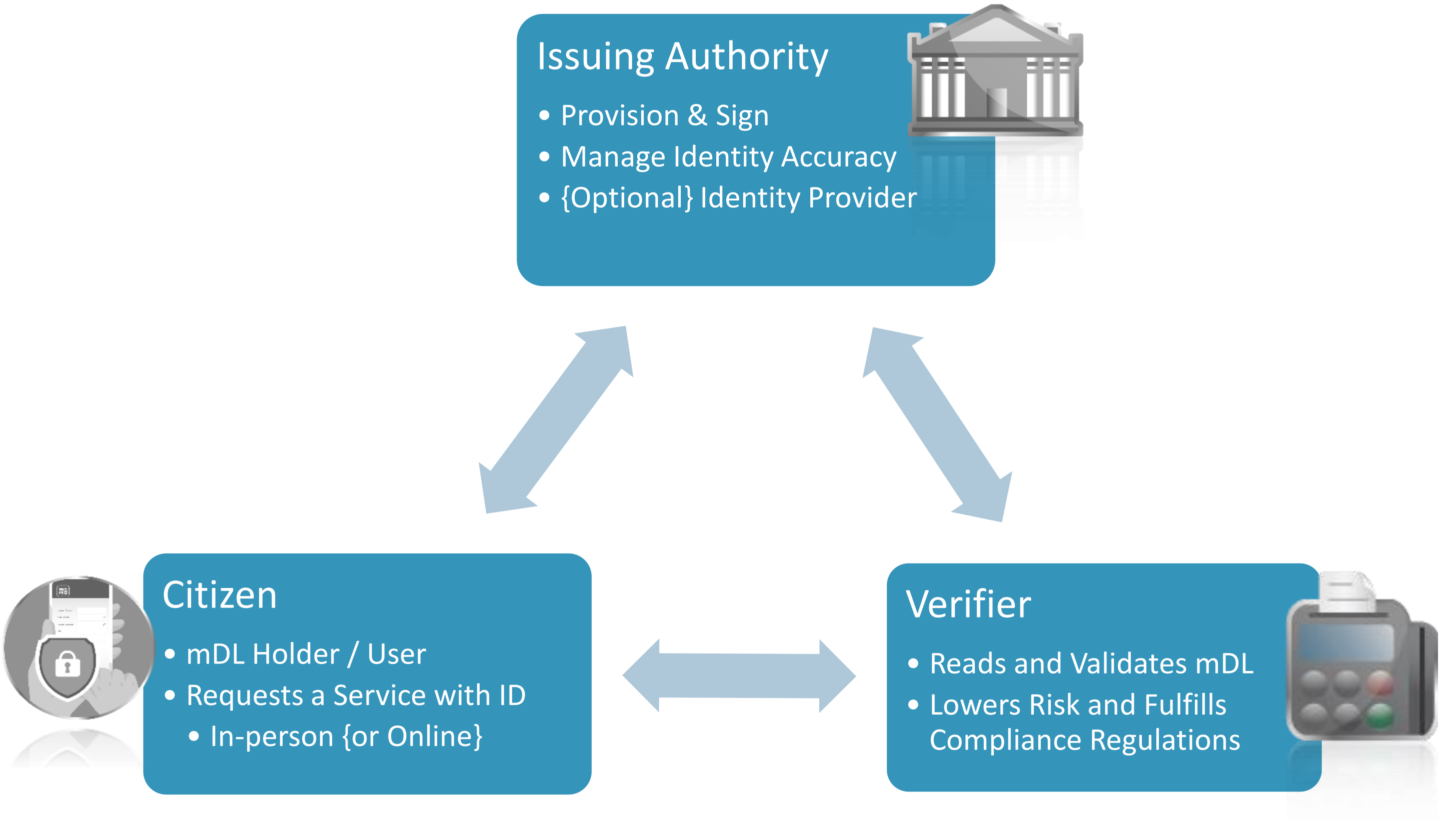
Mechanisms
- Online
- Offline
- NFC, QR, BLE, WiFi Aware

Interaction Modes
- Tap & Go
- Scan & Lookup
- Request
- Check-in

Use Cases
- Choose how to Interact
- Required Data
- Tools and Tips

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

mDL Creates an Ecosystem



Issuing Authority

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

Citizen

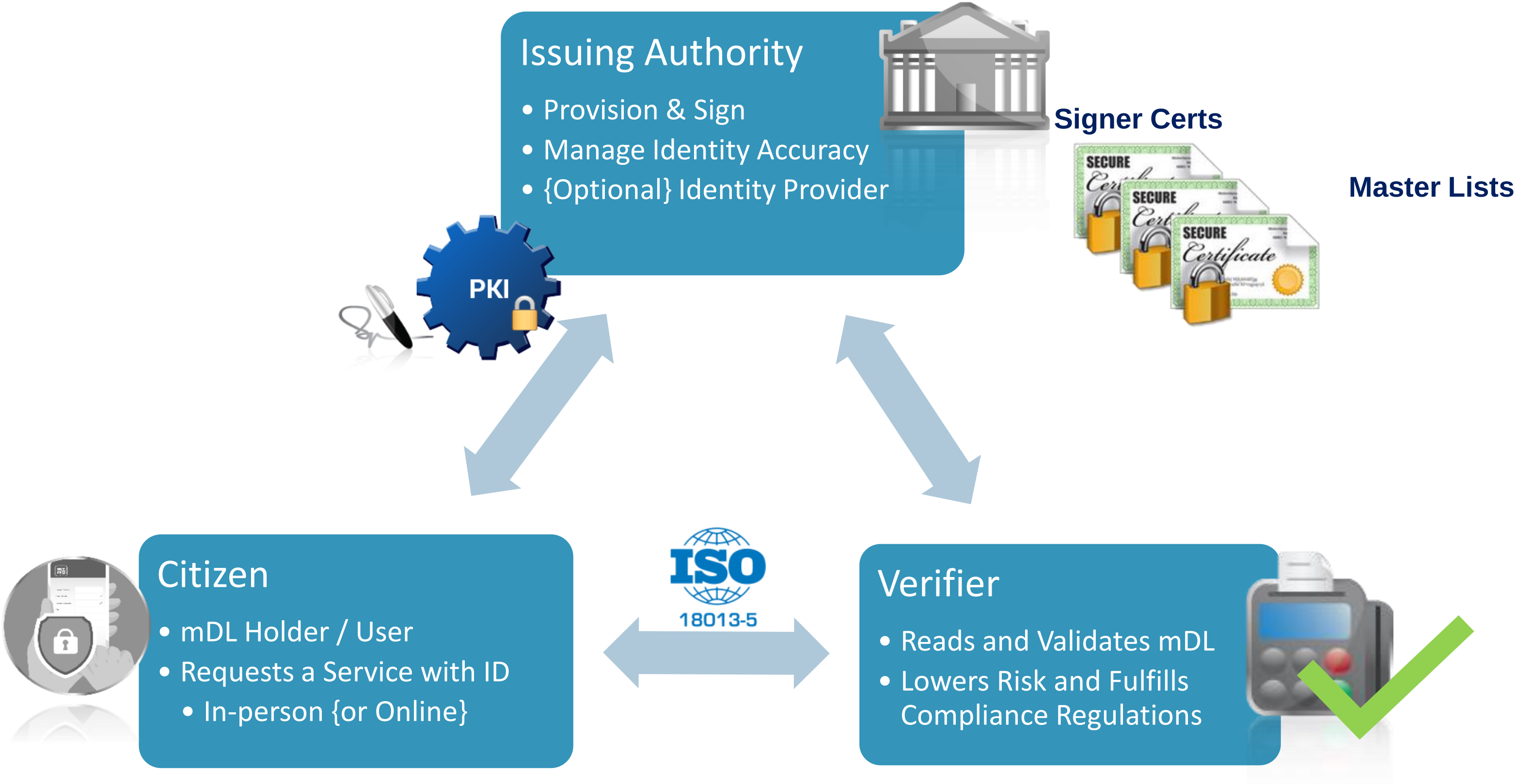
- mDL Holder / User
- Requests a Service with ID
  - In-person {or Online}

Verifier

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

Putting government signed attributes in the Citizen's hands to manage

Trust Mechanisms - ISO 18013-5 mDL & mID



Issuing Authority

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

Signer Certs

Master Lists

Citizen

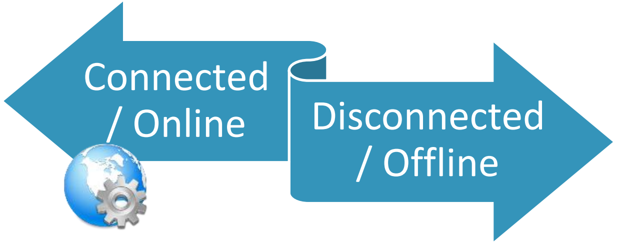
- mDL Holder / User
- Requests a Service with ID
  - In-person {or Online}

Verifier

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

Cryptographic Trust in the ID Provided by ISO 18013-5

Variations to In-Person Interactions using a Mobile ID



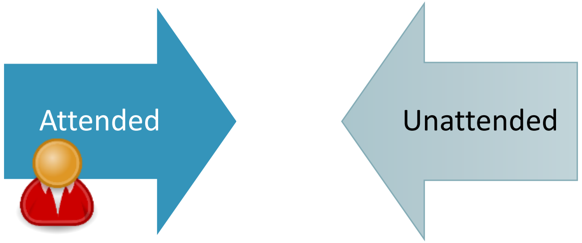
Server Retrieval

Device Transfer

- Largest factor in a Use Case
- Online seems to be quicker than device-to-device
- Sometimes devices are not connected to the Internet
  - mDL needs to provide online token in QR/NFC
  - Reader chooses if connected
- *Consider the privacy concerns if particular Issuers lack Do-Not-Track policies*

Darker shape means supported in Day One. Lighter means this will be standardized in Day Two.

Variations to In-Person Interactions using a Mobile ID

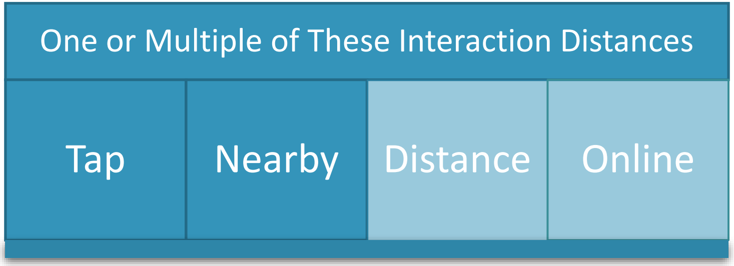


- Human Attendant to perform the identity verification
  - Day One ISO 18013-5
- Display Device necessary to show the attendant photo
- Biometric identity verification using signed photo is possible
- User Authentication (Day Two)
  - Using mDL application
  - Using online (Open ID Conn)
  - Trusting user device?

SECURE TECHNOLOGY ALLIANCE

Darker shape means supported in Day One. Lighter means this will be standardized in Day Two.

Variations to In-Person Interactions using a Mobile ID



One or Multiple of These Interaction Distances

Tap

Nearby

Distance

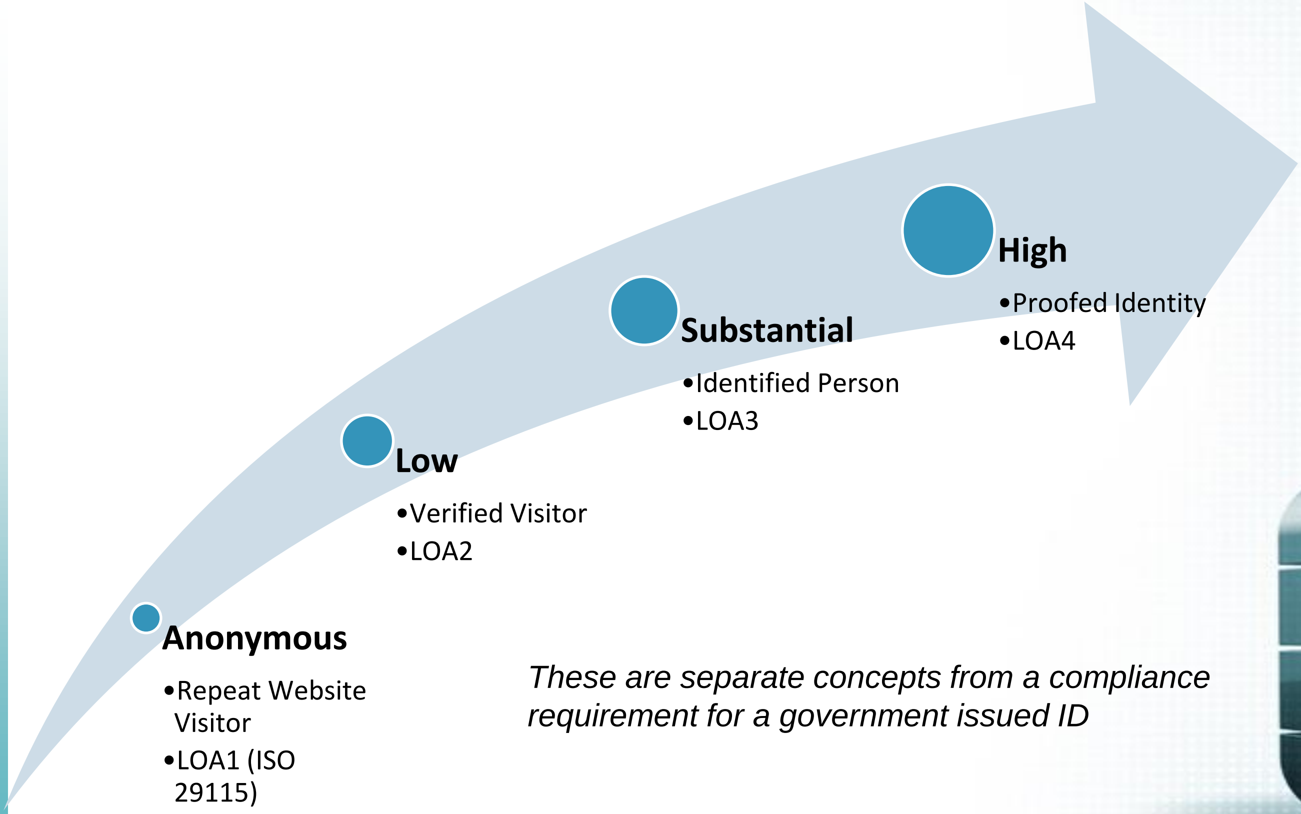
Online

- NFC and QR for Device Engagement limit the range or distance of the interaction
  - Day One
  - Day Two will extend range
- Single step (atomic) interactions in Day One
  - Use Case of online alcohol is inherently multi-step
  - Data is same each iteration

Darker shape means supported in Day One, Lighter means this will be standardized in Day Two 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?

Verifier Risk: Met by Level of Assurance



Anonymous

- Repeat Website Visitor
- LOA1 (ISO 29115)

Low

- Verified Visitor
- LOA2

Substantial

- Identified Person
- LOA3

High

- Proofed Identity
- LOA4

These are separate concepts from a compliance requirement for a government issued ID

Day One ISO 18013-5 does not have a mechanism for requesting Identity Assurance

Interaction Modes (Connections x Transfers)

	NFC	Bluetooth (WiFi Aware)	Online REST	Online OIDC w/ authToken	OIDC w/ User AuthN	Any w/ Biometric Camera
NFC	Tap & Hold	Tap & Go	Tap & Request	Tap & Request	Tap & Consent	Tap & Look
QR		Scan & Go	Scan & Request	Scan & Request	Scan & Consent	Scan & Look
Day Two	Distance	Check-In	Check-In	Linked DL/ID	Login	

Privacy Considerations Owned by Verifiers

Verifiers, specifically, are responsible to protect the privacy of mDL Holder within the bounds of their operational, security, and legal requirements:

- **Minimizing Data** requested from the mDL Holder
- Notifying the mDL Holder of Verifier **Intent To Store** data
- Strictly adhere to the mDL Holder’s consent/approval, Verifier policies, and regulations about **Storing PII**
- Resisting and **preventing the tracking** of mDL Holder
  - Not storing information that identifies the mDL Holder with transaction logs and securing transaction logs
  - Not submitting PII or transaction info to a centralized service
  - Not tracking information that identifies the mDL Holder at the online/server interfaces

Privacy Protection is the Shared Responsibility of all Ecosystem Parties: Verifier, Issuer, Frameworks

SECURE TECHNOLOGY ALLIANCE

Airport Security Use Case

Brandon Gutierrez, DHS TSA

TSA Identity Management:

Secure Technology Alliance (STA) Identity Council's mDL Webinar

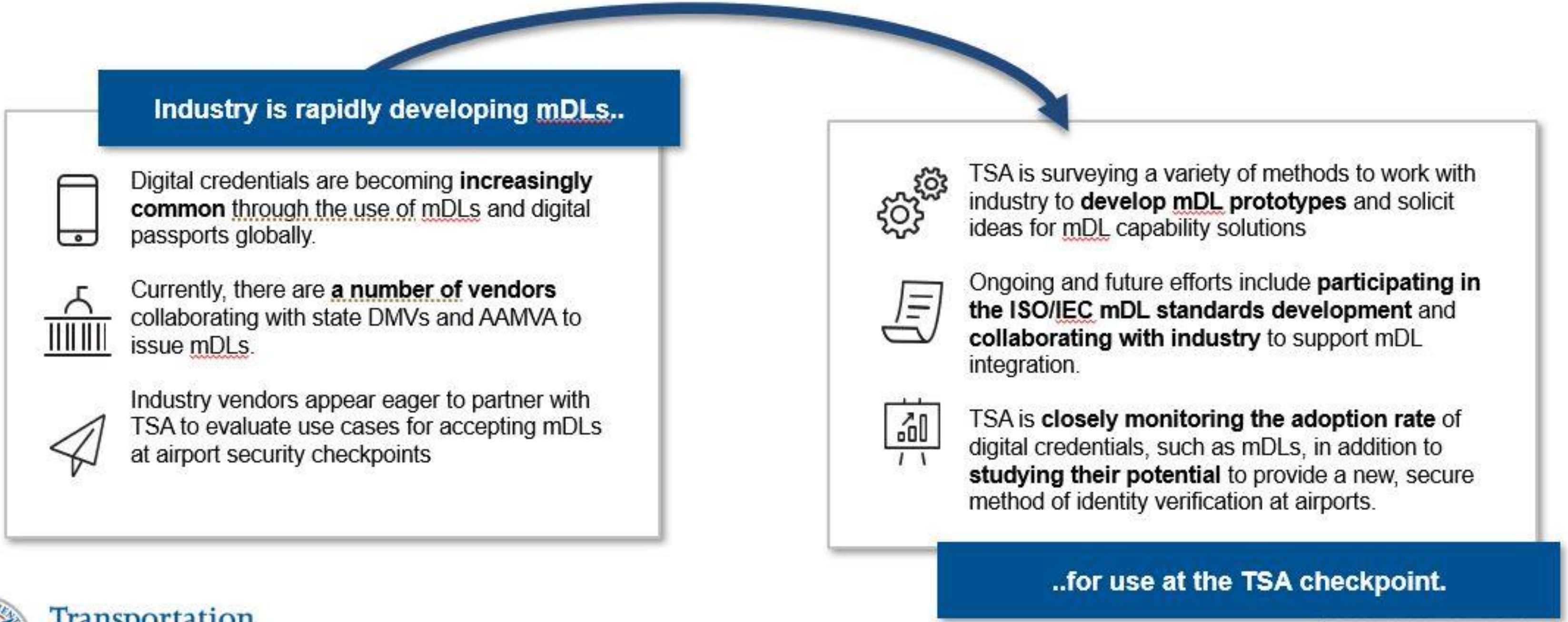
May 28, 2020

Transportation Security Administration

RCA | REQUIREMENTS & CAPABILITIES ANALYSIS

TSA's Exploration of mDL Capabilities

In recognition of the increased adoption of digital credentials and as part of its approach to identity management, **TSA is assessing the feasibility of accepting mDLs in the airport environment.**



Industry is rapidly developing mDLs..

- Digital credentials are becoming **increasingly common** through the use of mDLs and digital passports globally.
- Currently, there are **a number of vendors** collaborating with state DMVs and AAMVA to issue mDLs.
- Industry vendors appear eager to partner with TSA to evaluate use cases for accepting mDLs at airport security checkpoints

- TSA is surveying a variety of methods to work with industry to **develop mDL prototypes** and solicit ideas for mDL capability solutions
- Ongoing and future efforts include **participating in the ISO/IEC mDL standards development** and **collaborating with industry** to support mDL integration.
- TSA is **closely monitoring the adoption rate** of digital credentials, such as mDLs, in addition to **studying their potential** to provide a new, secure method of identity verification at airports.

..for use at the TSA checkpoint.

Key Issues for mDL Integration

TSA is exploring verifying party technologies or requirements aligned with ISO 18013-5 to **increase efficiency, security, and ensure that all security and privacy standards will be met**. The below outlines TSA's priorities as a potential verifying entity.

Interoperability

Facilitate an interoperable interface with **multiple devices and applications** from different issuing authority jurisdictions

Speed

Decrease the time needed for the traveler to present an identity document

Authentication

Increase the **ease of authentication** against a trusted source

Tamper/Fraud Detection

Increase the capability to **identify indicators of tampering or fraud**

Privacy

Integrate privacy protections that protect travelers' personally identifiable information (PII)

CAT Capabilities and Notional mDL Upgrades

Acceptance of mDLs will require the integration of mDL authentication capability with existing TSA technologies to **transmit digital identity information at the airport checkpoint and verify a person's identity.**

Credential Authentication Technology (CAT)

(Current Technology)

Verifies a passenger's physical ID is authentic

Confirms passenger's flight reservation and Secure Flight status

Scans passenger IDs tendered by TSOs

TSA started deploying CAT units to airports in early FY20.

Self-Service CAT-Camera (CAT-C) w/ mDL Capabilities

(Notional Prototype)

Verifies a passenger's physical or **mobile ID** is authentic

Confirms passenger's flight reservation and Secure Flight status

Verifies the passenger's identity by comparing their biometric facial image (via camera capture) with a reference photo

Allows passengers to scan their own IDs as a touchless feature

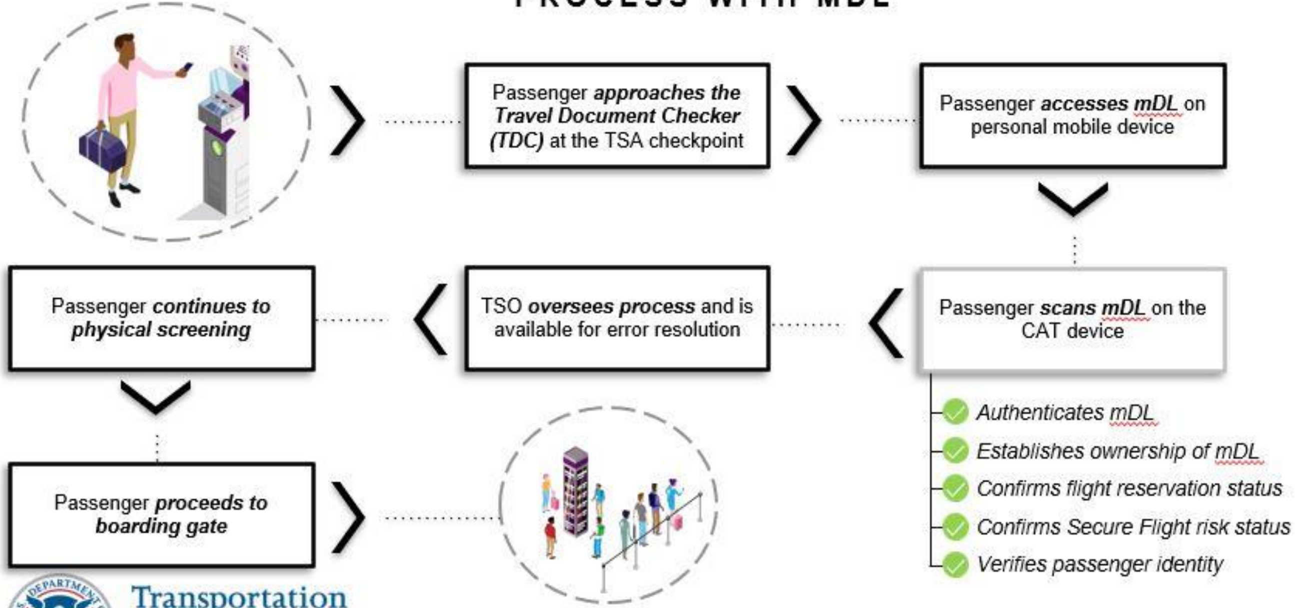
Instructs the passenger using an updated user interface

TSA is developing and testing this capability.

mDL at the TSA Checkpoint

TSA is evaluating the feasibility of incorporating mDLs into Credential Authentication Technology (CAT), **which increases security at airport checkpoints by verifying a traveler's ID.**

CONCEPTUAL TDC PROCESS WITH MDL



Passenger *approaches the Travel Document Checker (TDC)* at the TSA checkpoint

Passenger *accesses mDL* on personal mobile device

Passenger *scans mDL* on the CAT device

- ✓ *Authenticates mDL*
- ✓ *Establishes ownership of mDL*
- ✓ *Confirms flight reservation status*
- ✓ *Confirms Secure Flight risk status*
- ✓ *Verifies passenger identity*

TSO *oversees process* and is available for error resolution

Passenger *continues to physical screening*

Passenger *proceeds to boarding gate*

BENEFITS

- **Increases security effectiveness** at the checkpoint with mDL's embedded security features
- **Limits physical contact** between TSOs and passengers at TDC
- **Relieves cognitive stress** on TSOs to study all state IDs and passports
- **Reduces risk** of encountering stolen or counterfeited physical IDs
- **Limits data sharing** to essential information only (e.g. name, DOB)
- **Improves passenger experience** with self-service and digital procedures

Transportation Security Administration

RCA | REQUIREMENTS & CAPABILITIES ANALYSIS

Overview of Technical Challenges

Substantial **collaboration with all stakeholders** will be necessary to ensure that TSA can use mDLs effectively and securely.

CHALLENGES

Cybersecurity constraints surrounding offline transactions and communication protocols such as Bluetooth or Wi-Fi Aware

Establishing, managing, and communicating with a **Private Key Database** (PKD) for verification and trust

Deployment of mDLs and mDL readers to the field

SOLUTIONS

At a **minimum**, offline mDLs must be able to confirm an mDL holder's identity and driving privileges. Communication protocols should be chosen based on a combination of metrics including **security**, **performance**, and **interoperability**.

TSA will collaborate with state governments and AAMVA to determine **best practices** and a unified approach to verifying an mDL with the issuing authority.

TSA is developing an mDL reader a **test & evaluation** plan adhering to ISO 18013-5 to ensure an efficient deployment.

Questions or Comments?

Please email the TSA Identity Management inbox at
TSAIDM@tsa.dhs.gov.

SECURE TECHNOLOGY ALLIANCE

Banking Use Case

Andreas Aabye, Visa

Account Opening in Branch

Account Opening today:

- Applicant completes application
- Applicant would present a driver's license
- Bank would validate the cardholder is the person presenting the driver's license and manually validate the name matches the application, validate SSN, etc.
- In some cases, this is performed remotely through taking pictures of the license

Account Opening in Branch

Account Opening with mDL:

- mDL Holder completes application
- mDL Holder would then tap the mDL against the reader, cross-verifying information
- Bank would validate the cardholder is the person presenting the mDL
- In Day 2, this could be performed remotely

What does this solve for?

- Two electronic sources of information: the application and the mDL – lessens chance of typos
- Clerk is not required to assess authenticity of license – improves KYC
- Day 2 would allow remote opening with much stronger sense of authenticity

Banking Needs

- Assurance that the identity validation and security is sufficient for KYC requirements
- Readers that are easy to integrate into the current banking experience and allows various settings for intent to store
- Accurate, updated information, such as address

A digital identity would allow the banking staff to focus on the customer as opposed to the validation of the information, with a higher level of authenticity at higher speed

SECURE TECHNOLOGY ALLIANCE

Law Enforcement Use Case

Paul Steier, AAMVA

Law Enforcement Use Case – Traffic Stops

- **Identify Vehicle Operator and Possibly Vehicle Passenger(s)**
  - Identity and driving privilege (may be more than one person)
  - Record identity for follow-up, warning, or citation
  - Information transferable
  - Implications of incorrect identity information
  - Identifying someone not conscious

- **Officer needs**
  - Safety and hands free
  - Focus on people and interaction
  - Efficient
  - Operational with no cell connection
  - Compatible and interoperable

Law Enforcement Use Case – Remote Identity Validation

- **Validating Identity Away from Vehicle or Office Setting**
  - Public contact in-person or remote, and checking other licenses or permits
  - Validating status of identification and licenses/permits
  - Recording and transferring information
  - Providing information to the person contacted

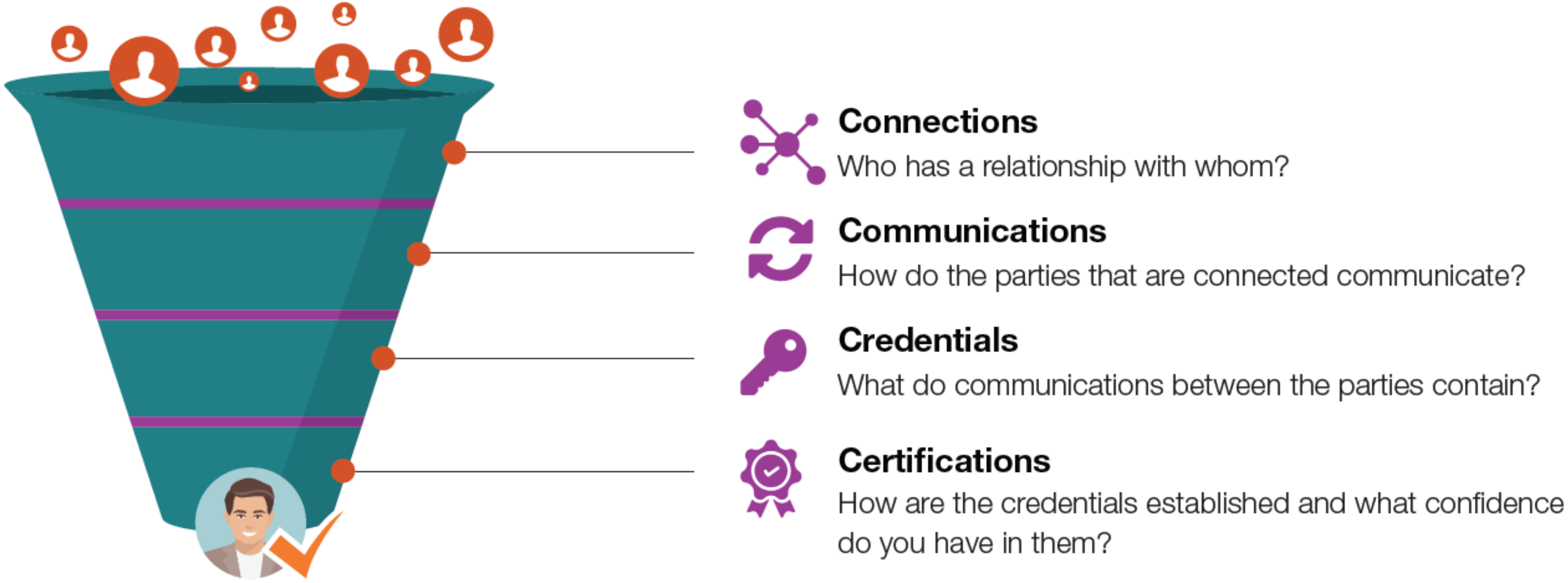
- **Officer needs**
  - Safety and hands free
  - Focus on people and interaction
  - Efficient
  - Operational with no cell connection
  - Compatible and interoperable

SECURE TECHNOLOGY ALLIANCE

Alliance mDL Use Case Template

Justin Gage, Consult Hyperion

All identity networks have the same basic layers



Connections
Who has a relationship with whom?

Communications
How do the parties that are connected communicate?

Credentials
What do communications between the parties contain?

Certifications
How are the credentials established and what confidence do you have in them?

Source: https://diacc.ca/2020/05/13/making-sense-of-identity-networks/

What are the requirements of an identity network?

Governance

Participation

is concerned with rules that may restrict who is allowed to be a provider or relying party, or place requirements on network users to be vetted in some manner.

Transparency

recognizes that users need to know that personal data is processed in line with data protection laws, including obtaining explicit consent from the subject to whom that data pertains.

Accountability

is concerned with ensuring all parties act responsibly, upholding their obligations.

Operation

Confidentiality

is concerned with ensuring credentials are protected from unauthorized or inappropriate disclosure.

Integrity

of credentials is vital to maintaining confidence in the network. Network users need to be sure that credentials are transmitted reliably and cannot be altered maliciously or otherwise.

Availability

identifies the requirement for networks to ensure that it and its inputs (e.g. providers) are available when they need to be. Without this, digital services will not function.

Source: https://diacc.ca/2020/05/13/making-sense-of-identity-networks/

What to look for in an identity network

Utility

- Sector
- Transaction types
- Identity types
- Interoperability
- Adoption

Trust

- Governance
- Transparency
- Assurance
- Funding
- Maturity

Privacy

- Choice
- Data protection
- Transparency
- Accountability

Source: https://diacc.ca/2020/05/13/making-sense-of-identity-networks/

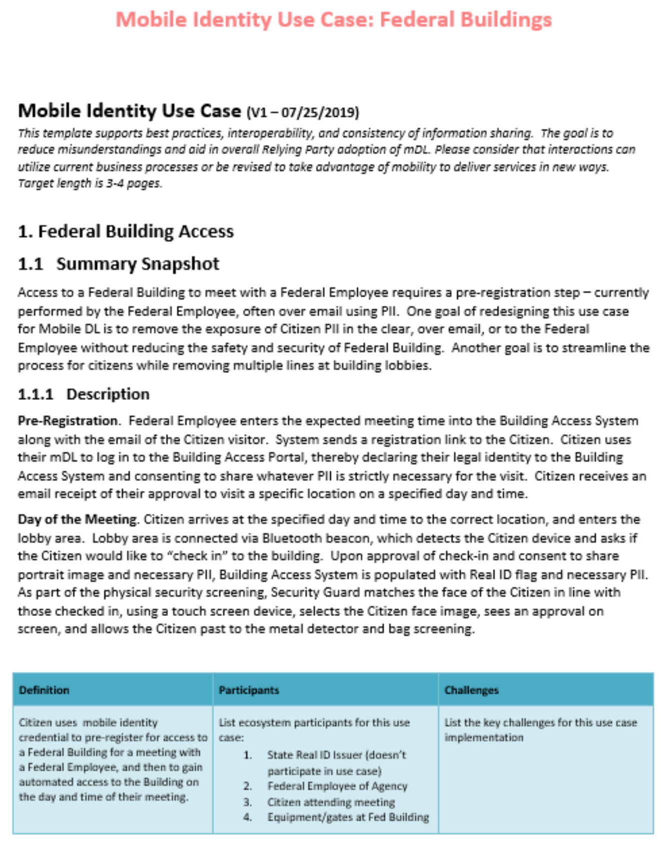
Secure Technology Alliance mDL Use Case Template

This template supports best practices, interoperability, and consistency of information sharing for mDL use case analysis

Includes considerations for:

- Use case description, participants, and interaction modes
- Value proposition for all stakeholders
- Legal and compliance
- Data requirements
- Implementation details including provisioning, storing and using the identity
- Security measures and risk mitigation

Secure Technology Alliance mDL Use Case Template



Mobile Identity Use Case: Federal Buildings

Mobile Identity Use Case (V1 – 07/25/2019)

This template supports best practices, interoperability, and consistency of information sharing. The goal is to reduce misunderstandings and aid in overall Relying Party adoption of mDL. Please consider that interactions can utilize current business processes or be revised to take advantage of mobility to deliver services in new ways. Target length is 3-4 pages.

1. Federal Building Access

1.1 Summary Snapshot

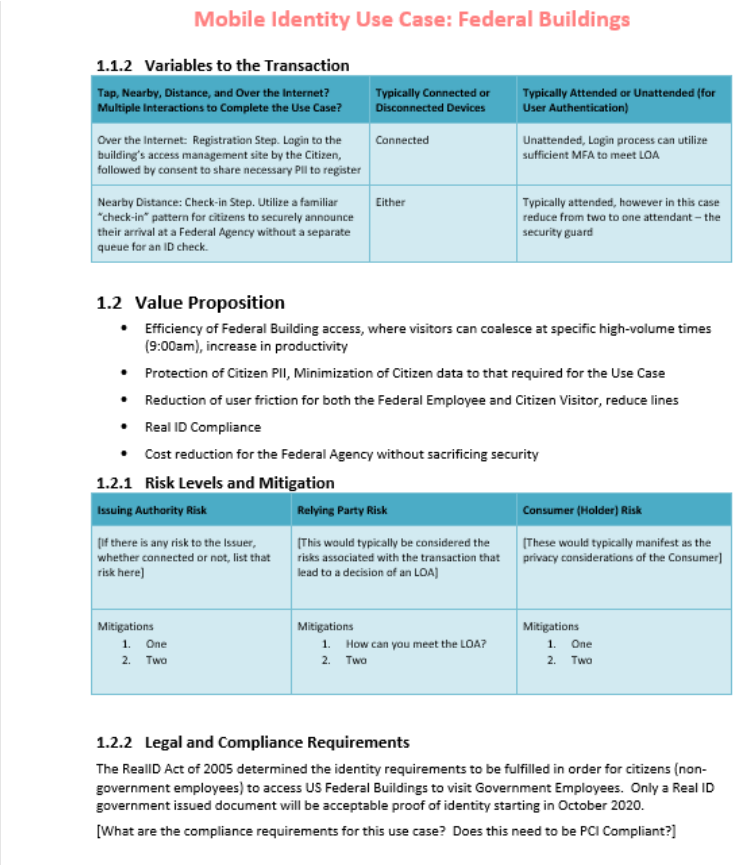
Access to a Federal Building to meet with a Federal Employee requires a pre-registration step – currently performed by the Federal Employee, often over email using PII. One goal of redesigning this use case for Mobile DL is to remove the exposure of Citizen PII in the clear, over email, or to the Federal Employee without reducing the safety and security of Federal Building. Another goal is to streamline the process for citizens while removing multiple lines at building lobbies.

1.1.1 Description

Pre-Registration. Federal Employee enters the expected meeting time into the Building Access System along with the email of the Citizen visitor. System sends a registration link to the Citizen. Citizen uses their mDL to log in to the Building Access Portal, thereby declaring their legal identity to the Building Access System and consenting to share whatever PII is strictly necessary for the visit. Citizen receives an email receipt of their approval to visit a specific location on a specified day and time.

Day of the Meeting. Citizen arrives at the specified day and time to the correct location, and enters the lobby area. Lobby area is connected via Bluetooth beacon, which detects the Citizen device and asks if the Citizen would like to "check in" to the building. Upon approval of check-in and consent to share portrait image and necessary PII, Building Access System is populated with Real ID flag and necessary PII. As part of the physical security screening, Security Guard matches the face of the Citizen in line with those checked in, using a touch screen device, selects the Citizen face image, sees an approval on screen, and allows the Citizen past to the metal detector and bag screening.

Definition	Participants	Challenges
Citizen uses mobile identity credential to pre-register for access to a Federal Building for a meeting with a Federal Employee, and then to gain automated access to the Building on the day and time of their meeting.	List ecosystem participants for this use case: 1. State Real ID Issuer (doesn't participate in use case) 2. Federal Employee of Agency 3. Citizen attending meeting 4. Equipment/gates at Fed Building	List the key challenges for this use case implementation



Mobile Identity Use Case: Federal Buildings

1.1.2 Variables to the Transaction

Tap, Nearby, Distance, and Over the Internet? Multiple Interactions to Complete the Use Case?	Typically Connected or Disconnected Devices	Typically Attended or Unattended (for User Authentication)
Over the Internet: Registration Step. Login to the building's access management site by the Citizen, followed by consent to share necessary PII to register	Connected	Unattended, Login process can utilize sufficient MFA to meet LOA
Nearby Distance: Check-in Step. Utilize a familiar "check-in" pattern for citizens to securely announce their arrival at a Federal Agency without a separate queue for an ID check.	Either	Typically attended, however in this case reduce from two to one attendant – the security guard

1.2 Value Proposition

- Efficiency of Federal Building access, where visitors can coalesce at specific high-volume times (9:00am), increase in productivity
- Protection of Citizen PII, Minimization of Citizen data to that required for the Use Case
- Reduction of user friction for both the Federal Employee and Citizen Visitor, reduce lines
- Real ID Compliance
- Cost reduction for the Federal Agency without sacrificing security

1.2.1 Risk Levels and Mitigation

Issuing Authority Risk	Relying Party Risk	Consumer (Holder) Risk
[If there is any risk to the Issuer, whether connected or not, list that risk here]	[This would typically be considered the risks associated with the transaction that lead to a decision of an LOA]	[These would typically manifest as the privacy considerations of the Consumer]
Mitigations 1. One 2. Two	Mitigations 1. How can you meet the LOA? 2. Two	Mitigations 1. One 2. Two

1.2.2 Legal and Compliance Requirements

The RealID Act of 2005 determined the identity requirements to be fulfilled in order for citizens (non-government employees) to access US Federal Buildings to visit Government Employees. Only a Real ID government issued document will be acceptable proof of identity starting in October 2020.

[What are the compliance requirements for this use case? Does this need to be PCI Compliant?]

SECURE TECHNOLOGY ALLIANCE

SECURE TECHNOLOGY ALLIANCE

Secure Technology Alliance mDL Initiatve

Tom Lockwood, NextgenID

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

3). IDC Partnering Projects - Multiple Efforts Including mDL

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

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

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

Follow-on Webinars

mDL Relying Parties - Trust Across States (September)

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 Use Cases
- First Responder Use Cases

c). mDL Guidance Documents

Secure Technology Alliance Relying Party Guidance - this effort is focused on 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 & Secure Technology Alliance - National Association of State CIOs represent state leaders' IT priorities, policies, best practices, and issues and challenges. The Alliance 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/Verifier Understanding of Another State's

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 (mDL) and Ecosystem Paper, Chapter 6 – Identified Technical and policy considerations…

…the greater mDL community is preparing for those next step in supporting adoption

Alliance Mobile Driver’s License Efforts

“The Ask”

- Support your organization’s or community’s awareness and education of the coming implementation of ISO 18013-5 based mDLs.
- Consider business processes and interactions where your organization or community relies upon driver’s licenses or identity and age verification.
- Work jointly with the Alliance to:
  - identify where mDL capabilities reduce risks, costs, or enhance user experiences
  - discuss your organization and community’s priority use cases;
  - Consider initial mDL adoption issues and implementation
- Consider having representatives directly participating in Alliance mDL awareness, education and coordination activities and efforts or form your own working group – we will work with you
- If it’s a great experience and provides value, consider joining the Alliance.

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/mDLQuiz2

Selected Resources

- **Introduction to the mDL Webinar Recording -** https://www.securetechalliance.org/the-mobile-drivers-license-and-ecosystem-webinar-series/introduction-to-the-mdl/
- **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
- David Kelts, dkelts@getgroupna.com
- Brandon Gutierrez, Brandon.Gutierrez@tsa.dhs.gov
- Andreas Aabye, aaabye@visa.com
- Paul Steier, psteier@aamva.org
- Justin Gage, Justin.Gage@chyp.com
- Tom Lockwood, tlockwood@nextgenid.com

SECURE
TECHNOLOGY
ALLIANCE

191 Clarksville Road
Princeton Junction, NJ 08550