IDENTITY & ACCESS TRACK

Next Steps on mDL Implementation

DAVID KELTS, SPRUCEID

HENK VAN DAM, UL SOLUTIONS

JOEL PEREZ, GET GROUP NA

JEFF SCOTT, INTERCEDE

ED PEREZ, VERIFONE

MICHAEL MCCASKILL, AAMVA

Moderated by

Deb Ferril, Ascend Consulting

IDENTITY & PAYMENTS SUMMIT

Next Steps on mDL Implementation

Now that you know how US Issuers want you involved, learn the next steps toward mDL acceptance for your business. STA's "Jumpstart mDL" Committee has published a use case template for your mDL Use Cases. Jumpstart members are joined by application, equipment, and certification service providers to lay out resources available and the next steps in your path to accepting mDLs as an accurate digital government ID. Leave with actionable guidance for how mDLs can impact your business' perception with customers, security, and your bottom line.

IDENTITY & PAYMENTS SUMMIT

Motivations for Accepting mDL Now

When accuracy and authenticity matter

- "Know Your Customer" flows **too low assurance & costly**
- "Valid Doc" API is Costly
- Exceed Legal Requirements
- Lower Liability of Operations
- **Government Signed ID**

Customer Positioning

- **Privacy for Your Customers**
- Facilitate Convenience
- Don't send people home who forgot physical documents
- Turnaway because KYC failed
- Be Positioned Early:
  - Thought Leader
  - Tech for Customer Service

Learn, Investigate ROI of Accepting mDL

- Learn the Technology as a Competitive Advantage
- Gain Statistics from Pilot
- **"Partnering" with DMV** on privacy & new technology creates positive image

Early Integration

- Take a Phased Approach
- Host Onsite Events for Cust
- **Learn how mDL improves customer interactions**
- Plan for Over-the-Internet
- Lower pressure now than when in mDL full swing

IDENTITY & PAYMENTS SUMMIT

Privacy Considerations Owned by Verifiers

Minimize Data	• Request only the least data you legally require to approve transactions
Don't Store PII	• Re-evaluate your policies now that issuer-signed, identity assured data • Is monetizing stored identity data greater than cost of security & breach? • PII Data Stores are actually toxic waste, not treasure
Respect Consent	• Strictly adhere to the mDL Holder's consent/approval • Notify the mDL Holder of **Intent To Store** data through 18013-5 • Follow your (updated) policies, and regulations about storing PII
Prevent tracking the mDL Holder	• Don't store information that identifies the mDL Holder in transaction logs • Don't submit PII or transaction info to any *other* commercial service • Mask IP, location, or machine information from server interfaces

Verifiers are responsible to protect the privacy of mDL Holder within the bounds of *new* operational, security, and legal requirements

IDENTITY & PAYMENTS SUMMIT

How to use STA's Use Case Template

Mobile ID Education	Capture your Requirements	Design Proof of Concept	Obtain Wide Feedback	Return to Finalize Section 1
Watch mDL Webinars 2 & 3 - Relying Parties	Document your legal & ethical requirements	Reimagine a new interaction for max ROI	Review your POC; Complete 1.4 Challenges and 1.5 Security & Privacy	You may now have new viewpoints on how you would accept a Mobile Identity
Read mDL White Paper Section 2 - Interaction	List pain & slow points of existing customer interaction with IDs	Design a simple interaction that just replaces physical ID	Circulate to a wider audience and your stakeholders	Rewrite 1.1 in final form as Exec Summary
Discuss with Industry and mDL Experts	Identify Your Decision Makers & Stakeholders	Write Section 1.3: Implementation	Seek consultant review	Duplicate 1.x with your reimagined interaction into Section 2.x
Write a preliminary Section 1.1: Interaction	Collaborate on Section 1.2: Value Proposition	Implement POC		

https://www.mdlconnection.com/mdl-uses/

IDENTITY & PAYMENTS SUMMIT

Ways for you to get involved now…

Jumpstart mDL Working Subcommittee is willing to help you

- Get a demo; download verifiers – publicly available in app stores
- Join the “Jumpstarting the mDL Ecosystem” Group —>
- Build Your ROI (+Intangibles) for Company Approval
- Build your Use Case from STA’s Downloadable Template
  - https://www.mdlconnection.com/mdl-uses/
- Examine or Re-evaluate your Workflows & PII Storage

SCAN ME

IDENTITY & PAYMENTS SUMMIT

Next Steps in mDL implementation

Jeff Scott

Solution Architect

Intercede

IDENTITY & PAYMENTS SUMMIT

International Interest in 18013-5

Warrant Card Credential

- **Why**:
  - Impersonations, forgery, fraud, easily replicated paper badge, citizen perception
- **Solutions:**
  - Digital Credential provided to Warrant Card holder that are active and that can be revoked when no longer employed.
  - Baseline 18013-5 standards, ability to verify identity and share attributes and active information with citizens using known URL or QR code
  - Full Audit Trail
- **Results**:
  - Reduces the risk of impersonation, forgery and fraud and increase citizen trust

Verification of Identity for Public Trust

IDENTITY & PAYMENTS SUMMIT

International Interest in 18013-5

South America Financial Solution

- **Why:**
  - Fraud prevention for consumer mobile transactions
- **Solution:**
  - 18013-5 standards for collection and issuance of attributes into a wallet
  - Increased anti fraud checks (Liveness, selfie 1:1, 1:1 attribute confirmation)
  - Storage of credential with signed attributes on mobile device
- **Results:**
  - Relying Party trust of appropriate individual receiving services
  - Validation of presented credential and owner via QR code, shared attributes and biometrics
  - Full Audit Trail

Relying Party Services – Identity Verification

IDENTITY & PAYMENTS SUMMIT

International Interest in 18013-5

National ID

- **Why:**
  - Citizen demand for government services on phones
- **Solutions:**
  - Leveraging existing government ID program that pre-dates 18013-5 standards
  - Multiple Languages, onboarding document, facial biometrics and OTP verification
  - Issuance Driver's license, vehicle registration, healthcare and family ID credentials to a singular wallet
- **Interest in 18013-5:**
  - Global interoperability, Standards based and enhanced PII security

Government Services

Multiple Credentials - Reduced Paper Infrastructure

IDENTITY & PAYMENTS SUMMIT

US Customers and Relying Parties

Next Steps in mDL Implementation

- **mDL Next Steps**
  - Support Relying Parties and enabling state governance & digital transformation
  - Citizens need to be able to use it (Simple process, usable by RP's, PII Security, audit trail)
- **mDL as onboarding for another credential**
  - Utilize mDL as initial onboarding document for secondary credentials
- **Credential Binding**
  - Additional identities, connected identities
  - Single point of revocation for bound credential

Relying Parties - Multiple Credentials

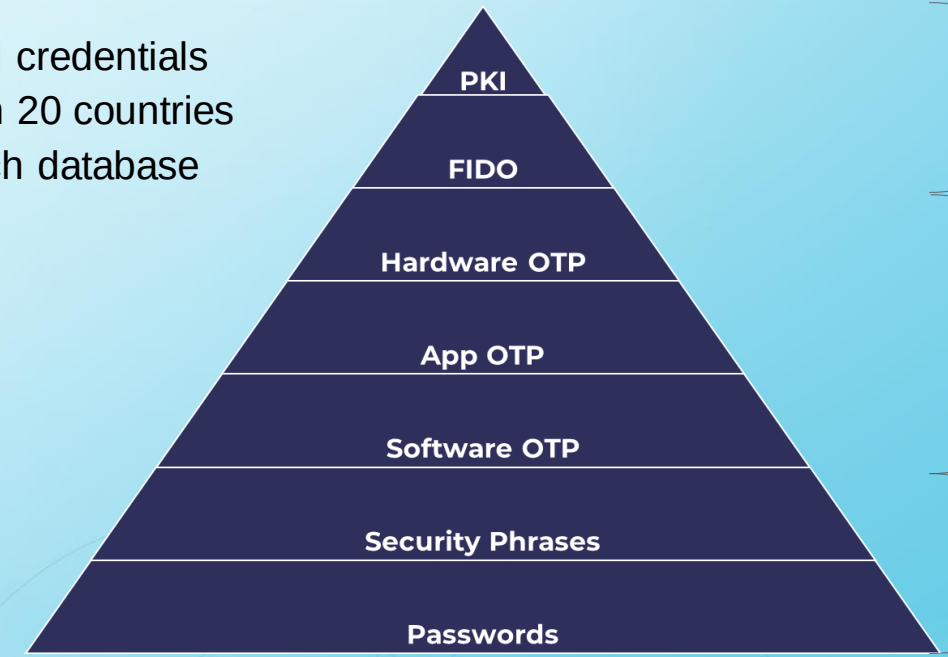
Digital Transformation -

IDENTITY & PAYMENTS SUMMIT

Intercede

- Many millions of managed credentials
- Deployments in more than 20 countries
- 8.5 billion credential breach database

- From Password to PKI



Jeff Scott
Solution Architect
jeff.scott@intercede.com

IDENTITY & PAYMENTS SUMMIT

Next Steps in mDL Implementation

By Joel Perez

Programs & Solutions Director

GET NORTH AMERICA GROUP

IDENTITY & PAYMENTS SUMMIT

ISO 18013-5 Compliance

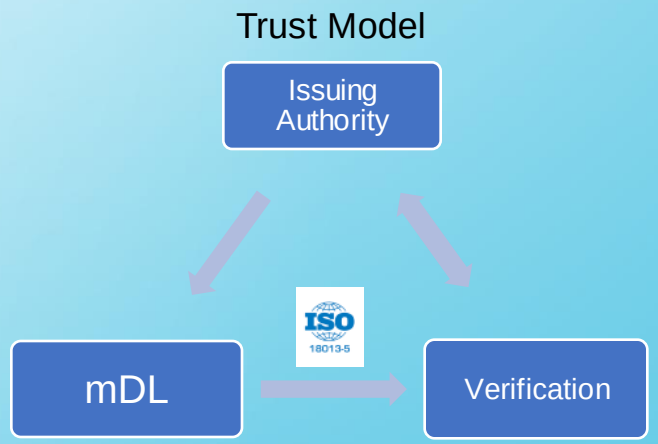
- Challenges:
  - Have implemented an mDL solution
  - Not ISO 18013-5 Certification
    - UL Certification
- Solution:
  - Don’t start from scratch
  - Modular Architecture
    - Microservices (API Gateway)
    - SDK and Libraries compatible with iOS and Android
- Migration or extension to what you already have

Certificate Authority

- Challenges for issuers of mDLs:
  - Issuers' Certificate Authority is a PKI document signing service that is new to jurisdictions and demands strict policy compliance
- Solution:
  - To meet DTS and TSA compliance, for example, choose a vendor with experience in Document Signing, not just a software development organization.
  - Remember, compliant Digital Certificates are the cornerstone of the security for the mDL
    - ISO 18013-5 Annex B

Face to Face Verification

- Challenges:
  - Fraud
  - Privacy
- Solution
  - Digital Certificate verification



IDENTITY & PAYMENTS SUMMIT

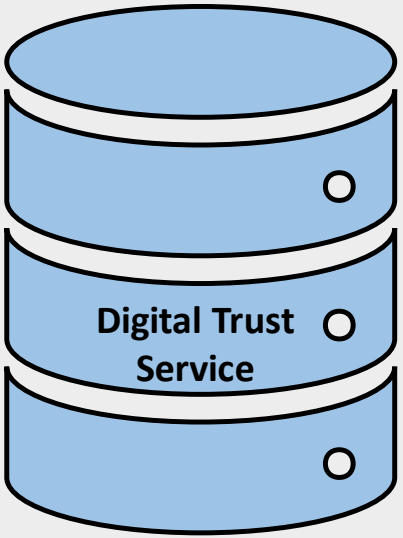
Online Age and Payment Verification

- Challenges are being addressed by:
  - ISO 18013-7 - providing approaches
    - Note - W3C is also discussing more solutions!
- Use Case:
  - Age Verification
  - Secure Payment Verification
    - EU Banks have implemented
- Three solutions: (Best to support all three)
  - OpenID Connect Forum (Verifiable Presentations) protocol
  - Browser API
    - Google and Apple embedded
  - Rest API or RESTful API

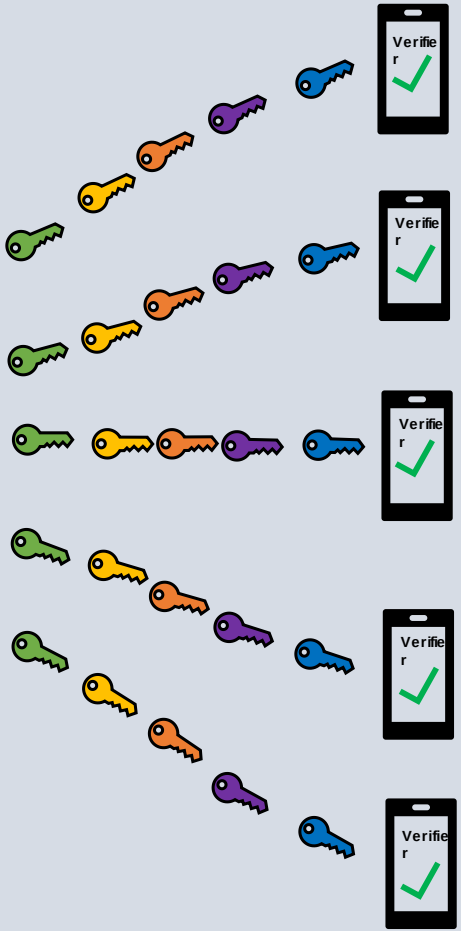
IDENTITY & PAYMENTS SUMMIT

Issuing Authorities (IA's) Provide Public Keys to AAMVA Digital Trust Service (DTS)

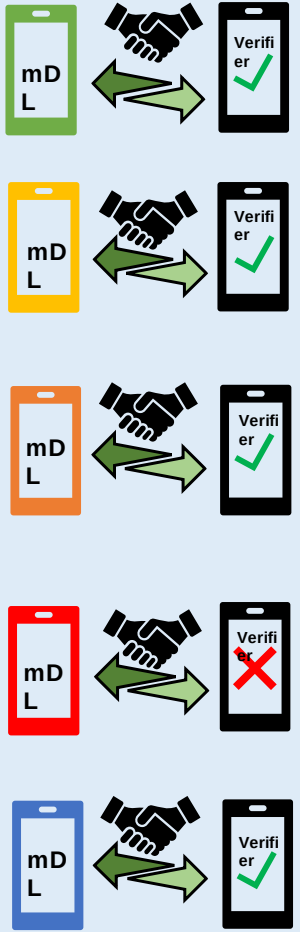
DTS Verifies Legitimacy of Issuing Authority; Confirms Conformance to Privacy, Security, and Interoperability Standards; and Validates IA Public Key



Relying Party mDL Readers Receive Validated Keys from DTS



Relying Party Confirms Authenticity of mDL Using Keys from DTS



Next Steps on mDL Implementation

mDL – Interoperability, Standards, Test and Certification

Tucson, AZ – Feb 27, 2024

Henk van Dam, UL Solutions

UL Solutions

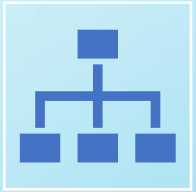
IDENTITY & PAYMENTS SUMMIT

Interoperability & Standards

Interoperability of systems

Communicate and work together

Sharing and processing data



Requires rule set how, when, what to communicate and work together

Standards as the set of agreed way of interoperating

IDENTITY & PAYMENTS SUMMIT

mDL Standard ISO 18013

ISO published 18013-5 standard Sept 30 ,2021

interoperability for in person mDL interactions

mDL holders, readers at verifiers, backend issuing states

ISO is current working on 18013-7

Covers online use cases

IDENTITY & PAYMENTS SUMMIT

UL solutions - Test and certification

UL provides test and certification services

mDL app (holders)

mDL readers (verifiers)

Proven compatibility with standard, hence required interoperability

IDENTITY & PAYMENTS SUMMIT

mDL and ISV Considerations

Thoughts on mDL acceptance at the Point of Sale

Edward Perez, Head of Card Brand & Processor Compliance NA, Verifone

IDENTITY & PAYMENTS SUMMIT

Payment Stakeholder Acceptance Variables

- Adoption Rate
  - Who will be the leader or the laggard?
  - State adoption, merchant awareness/education, readers in production
- Value Proposition and Incentives
  - What are the benefits?
  - Short/Long term, cost/price structure, business case
- Development and Certification
  - What is the effort?
  - PII concerns, cert costs, custom or generic, data elements, NFC v. QRC

BOTTOM LINE: Merchant interest and awareness will be the grassroots approach to help trigger adoption and its potential cascading impact at a POS system. This does NOT imply an mDL must be integrated in a POS.

IDENTITY & PAYMENTS SUMMIT