



SECURE
TECHNOLOGY
ALLIANCE

The Mobile Identity Landscape

Identity Council

Introduction

Randy Vanderhoof, Secure Technology Alliance



Tom Lockwood, NextGen ID



Geoff Slagle, AAMVA



David Kelts, Idemia



Suraj Sudhakaran, Gemalto



Dave Coley, Intercede



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.

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



Our Focus

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

Member Benefits

Certification
Council Participation
Education
Industry Outreach
Networking
Technology Trends

”...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

White Papers:

- [Assurance Levels Overview and Recommendations](#), Smart Card Alliance Identity Council position paper
- [FICAM in Brief: A Smart Card Alliance Summary of the Federal Identity, Credential, and Access Management \(FICAM\) Roadmap and Implementation Guidance](#), Smart Card Alliance Identity Council and Physical Access Council summary
- [Identifiers and Authentication – Smart Credential Choices to Protect Digital Identity](#), Smart Card Alliance Identity Council position paper
- [Identity Management in Healthcare](#), Smart Card Alliance Healthcare Council webinar
- [Identity Management Systems, Smart Cards and Privacy](#)
- [Interoperable Identity Credentials for the Air Transport Industry](#)
- [Smart Card Technology and the FIDO Protocols](#), Smart Card Alliance Identity Council white paper

The Problem & Value Outcome

Problem

We are faced with inconsistent solutions, methodologies, practices, and assumptions for implementing mobile identity credential capabilities.

This impacts quality and consistencies of products, services and user experiences.

Value/Outcome

- Enhanced User Experience
- Mobile device best-practices guidelines - inclusive/acceptable across mobile device providers and vertical market segments.
- Stabilize & expand market direction and opportunities within trusted identity and authentication markets
- Enhanced opportunities for integrators and service providers across use-cases
- Much improved interoperability & integration
- Raised awareness & content to support open standards & Interfaces

The Problem & Value Outcome - Continued

TARGET AUDIENCES

- Organizations Implementing IDMSs Issuing & Consuming Mobile Identity Credentials
- Product & Service Providers Supporting Mobile Identity Credential Offerings
- Organizations supporting & leveraging Mobile Identity Credential Standards & Best Practices

OBJECTIVES

Phased set of Deliverables/Projects to Assess the Market Landscape including:

- Provide a Broad Overview of Mobile Identity Credentials
- Identify Consistencies/Convergence, Inconsistencies/Conflicts & Gaps of the Disparate Hardware/Software Mobile Architectures
- Provide Methodologies & Best Practices to Address Gaps & Inconsistencies
- Educational Resources Raising Awareness/Influencing Requirements & Implementations
- Support more Consistent Common Build & Customer Requirements.
- Provide Input to Standards Development & Requirement Organizations to Support Standardization Processes.

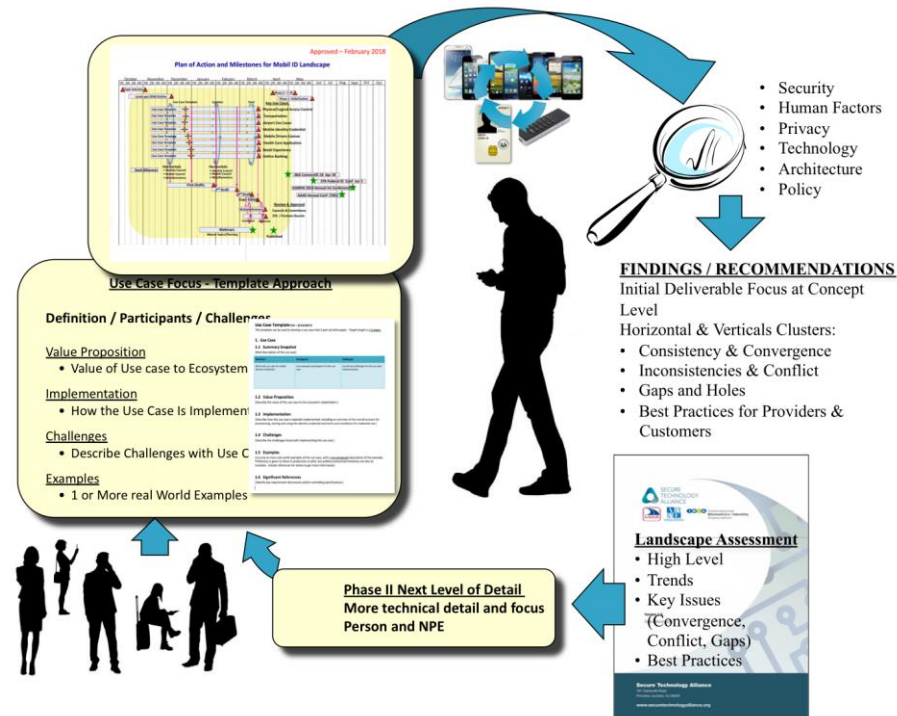
Approach

Approach

- Collaborative Approach: Across the Alliance Councils & Key Partnering Organizations
- Community Lead, Community Identified Use-Cases
- Common Templates to support collaborative discussions
 - Security, Human Factors, Privacy, Technology, Architecture, Policy
- Findings / Recommendations – Initial Deliverable Focus at Concept Level

This Call - Raise Awareness of the effort

- Provide a Broad Overview of Mobile Identity
- Feedback and reaction –
- Encourage you to follow-up



We Seek Your Feedback & Comments:

Landscape Assessment & Supporting Use-Case Adoption/Expansion/Leverage



SECURE
TECHNOLOGY
ALLIANCE

Mobile Driver's License





SECURE TECHNOLOGY ALLIANCE

Mobile Identity Landscape

Mobile Driver's License



Geoff Slagle, AAMVA

David Kelts, IDEMIA

Suraj Sudhakaran, GEMALTO

What is mDL?



- ✓ Your Identity
- ✓ Your Trusted Attributes
- ✓ Secure
- ✓ Privacy Protecting

Defining mDL



FUNCTIONAL
REQUIREMENTS



Not just an image or app
on the phone!



- Visual Representation
- Confirm Identity
- Convey Driving Privileges
- Establish Trust

- ✓ A supplement to the traditional driver license
- ✓ Continually evolving
- ✓ Optional and flexible for end users

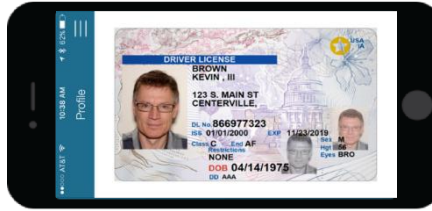
To be TRUSTED, an mDL must be...

Accurate

Accepted
Everywhere



Secure



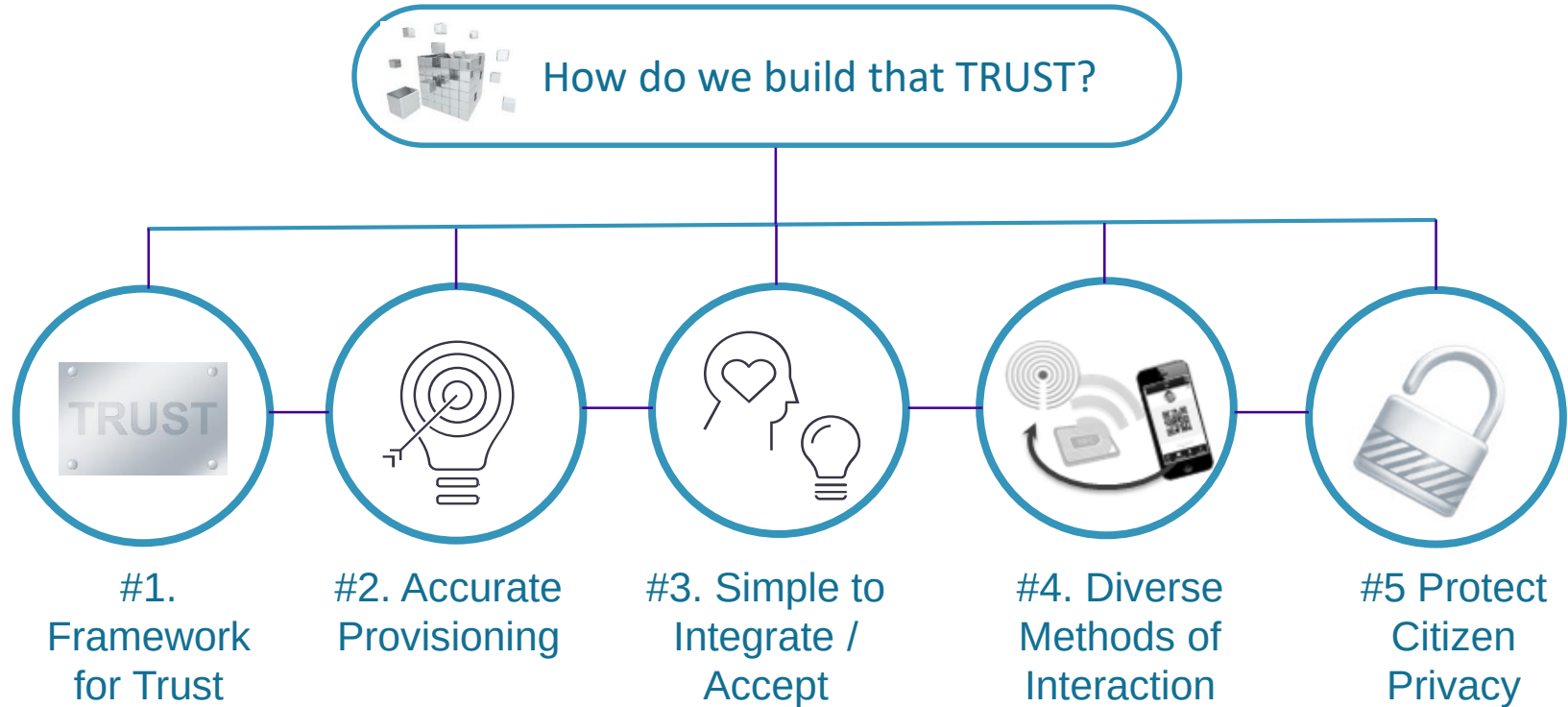
Protects
My Privacy



Reliable &
100% Available

Convenient
to Use

mDL Trust can be a Platform for Innovation





SECURE
TECHNOLOGY
ALLIANCE

mDL Use Cases



Use Cases - Traditional

Proof of Age



Identity verification



Use Cases – eServices (Government & Private)



FUNCTIONAL
REQUIREMENTS



2.11.4 Other use cases

Additional traditional use cases where a DL is used include the following:

- Car rental. In this case, a DL is used to identify the renter, as well as to provide driving privileges.
- Confirming identity in order to obtain social services.
- Confirming identity to a hotel on checking in.
- Confirming identity to financial institutions when conducting face-to-face business.
- Confirming identity in order to vote. (This is not a requirement in all jurisdictions.)
- Access control, e.g. to federal facilities. This can be seen as an extension of the TSA use case discussed earlier.

New use cases brought about by the nature of a mDL can be expected. Online use is one example. Online use can take many forms, e.g.:

- Signing documents electronically
- Improving security of other solutions/credentials on a mobile phone.

eServices

mDL Use Cases Re-Imagined – Identity as a Platform



Identity Verification

- ✓ Civil or social services
- ✓ Hotel check-in
- ✓ Access control
- ✓ Financial institutions



eServices

- ✓ Signing documents
- ✓ Attribute sharing online
- ✓ Driver's services
- ✓ Vital record management



Other uses

- ✓ Payment
- ✓ User Engagement
- ✓ Anonymous Attributes
- ✓ Think Beyond....



SECURE
TECHNOLOGY
ALLIANCE

Meeting the Challenge of TRUST



Regional trust models: Can mDL operate across all of them?



eIDAS	STORK 2.0	GPB 45	RSDOPS	Canada	SP 800-63	ISO 29115	ISO 29003
N/A	N/A	N/A	Level 01	N/A	N/A	N/A	N/A
Low	QAA Level 1	Level 1	Level 1	IAL/CAL 1	AAL/IAL1	LoA 1	LoA 1
N/A	QAA Level 2	Level 2	Level 2	IAL/CAL 2	N/A	LoA 2	LoA 2
Substantial	QAA Level 3	Level 3	Level 3	IAL/CAL3	AAL/IAL2	LoA 3	LoA 3
High	QAA Level 4	Level 4	N/A	IAL/CAL4	AAL/IAL3	LoA 4	LoA 4

Provisioning to the Right Person for THEM to Manage



Citizen Managed Identity

- Avoid In-Person Burden for Provisioning
- Accuracy MUST exceed Emailed PIN
- Email or SMS is easy to take over and steal Access Codes
- Mailed PIN codes can be swiped or forgotten
- Mobile Users Expect Apps On-Demand
- Accurate Provisioning and Strong Citizen-Management protects User Privacy

Simplify Integration for Relying Parties through Diverse Methods

- Standards are Key to Mass Adoption
- Common Data Model
- Must be Accepted Globally
- Open Standards Ensure Security and Interoperability
- Open Source Tools for Easy Integration
- Distance Usage... Unattended Usage

Transmit
(Signed Data)

Lookup
(Token)

Share

- Scan
- Receive



18013



iGov

Now I can use my Identity Everywhere



SECURE
TECHNOLOGY
ALLIANCE

Summary & Conclusion



Summary & Conclusion



- ✓ The user needs to be in control
- ✓ Privacy and security at the core
- ✓ Not just about an application – the complete ecosystem and building blocks to create value
- ✓ Not just any identity – it's a trusted identity issued by a government entity
- ✓ Secure provisioning and management of the credential is the key to preserving the trust provided
- ✓ Standardization and interoperability must follow



SECURE
TECHNOLOGY
ALLIANCE

Secure Mobile Identity in the U.S. Government

Derived Personal Identity Verification (PIV)





SECURE
TECHNOLOGY
ALLIANCE

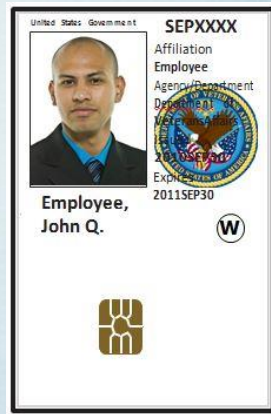
The Personal Identity Verification (PIV) standard, outlined in FIPS 201, provides a strong foundation for traditional desktop environments. However, it does not translate well to mobile and many other user cases across government.

Instead, a new standard, the Derived PIV credential was established in 2014...



Introduction to PIV Derived Credentials

- Standard Outlined in NIST Special Publication 800-157
- Strong identity credentials for computing environments where PIV Cards (smartcards) don't work well:
 - Primarily Tablets & Mobile Phones
 - Clean Rooms, Bio-Hazard Environments, Certain Disabilities
- “Derived” PIV Credential Highlights
 - Issuance & Lifecycle Management Process
 - Proofing Based on Possession & Control of a PIV
 - Ongoing Linkage to PIV
 - No Mathematical Relationship Between PIV and Derived PIV

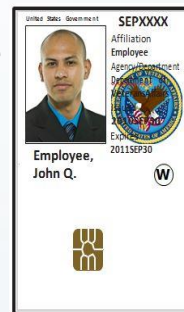


Value Proposition

- The Government is Mobile!
 - Virtually all parts of the government are adopting mobile including civilian, military, and intelligence.
 - Increased effectiveness and reduced costs
 - New business applications are being deployed.
- Derived PIV Credentials
 - Eliminate smartcard reader attachments.
 - Support strong authentication.
 - Support document & data signing
 - Support data encryption/decryption.

Implementation

- Key Functions of a Derived PIV System
 - Validate PIV Card & Expiration
 - Ensure User Entitlement to Derived PIV Credentials
 - Require User to Prove PIV Control by PIN (at a minimum)
 - Issues Derived PIV Authentication Certificate from Federal Bridge CA
 - Links Derived PIV Credential Linked to PIV Card
 - Monitors PIV Issuer for Updates to Cardholder Eligibility
 - Revokes PIV Credentials When Required



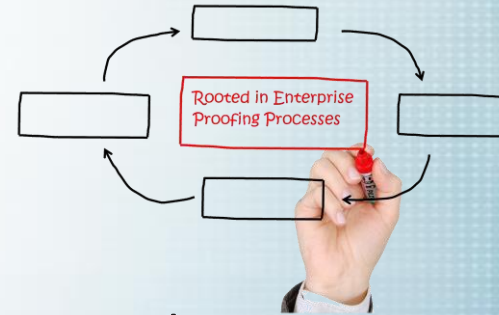
Challenges

- Needs Consistent Understanding Across Government
- Signing and Encryption Certificates
 - NIST SP 800-157 Outlines PIV Derived Authentication Certificate
 - Limited Guidance on Signing or Recovered Encryption Certificates
- Consistent Usage Mechanism (the biggest challenge)
 - As a CIO there is no deploy once, available to all enterprise apps, option.
 - As an ISV there is no standard way to find PKI credentials and each ISV must code for any PKI operation themselves.
 - The Ecosystem Requires a Standard PKI Services Layer



Derived Credential Potential Outside Government

- PIV is a Model for High Assurance Corporate Needs
- Derived PIV is a Model for High Assurance Mobile Identity
- Consider Corporate ID Derived Credentials
 - Mechanism for Issuing Mobile Identity
 - Strong Tie to Corporate Identity Proofing
 - Clear Path for Revocation on Employee Separation
- Is it possible to eliminate some overlap between strongly proofed identity use cases and provide better solutions?





SECURE
TECHNOLOGY
ALLIANCE

Q&A

Tom Lockwood – Tlockwood@NextGenID.com

Geoff Slagle – gslagle@aamva.org

David Kelts – david.kelts@us.idema.com

Suraj Sudhakaran – suraj.sudhakaran@gemalto.com

David Coley – david.coley@intercede.com