The webinar will begin shortly
Identity on a Mobile Device: Healthcare, Banking and Transportation Payment Use Cases

Identity Council Webinar
September 20, 2018
Introductions

• Randy Vanderhoof, Secure Technology Alliance

• Tom Lockwood, NextgenID

• Jeffrey Fountaine, Ingenico Group

• Judy Keator, SecureKey Technologies

• Jerry Kane, SEPTA
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

- **Assurance Levels Overview and Recommendations**, Smart Card Alliance Identity Council position paper
- **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**
- **Identity on a Mobile Device: Mobile Driver’s License and Derived Credential Use Cases**
- **Smart Card Technology and the FIDO Protocols**, Smart Card Alliance Identity Council white paper
Mobile Identity Landscape Assessment

Secure Technology Alliance  Identity Council & Identity Community Stakeholders

Tom Lockwood, NextgenID
Strategic Trending

...Identity is moving from vertical to horizontal...

## Identity Trends

- **Delivery Verticals Continuing Evolution**
  - Complementary / Blended: In-person, Desktop, Mobile, Kiosk/Machine
  - Expansion of Mobile and Kiosk Markets
- **Privacy – Compliance & “Allow-ability” (GDPR)**
- **Identity Proofing – Remote & Supervised Remote**
- **Automation of Backend Services & Machine Learning**
- **Biometrics Adoption & Matching Enhancements**
- **Distributed Ledger Technology**
- **Blurring between Physical & Digital Security**
- **Physical Identity Documents, augmented, Not Replaced by Digital Identity/Identifiers**
- **Zero Trust Models – Identity Centric**
- **Modularization of Identity Services**

---

**Immediate Focus Mobile Device Landscape Assessment**

**Connects & Defines Systems, Boundaries, & Transactions**

**Tangible, Necessary Real Market Relevance**

**Identity, Authentication, Authorization**
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.

**Resources**
- Current Secure Technology Alliance Members
- Identity & IT Community Members & Associations

**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
- Executing Organizations and agencies

---

**Value/Outcome:**
- Enhanced User Experience
- Raise community awareness
- Mobile device best-practices guidelines
- Stabilize & expand trusted identity & authentication opportunities & markets
- Enhanced opportunities for integrators & service providers across use-cases
- Improved interoperability & integration
- Recommendations to support open standards & Interfaces
Approach

• Provide a Broad Overview of Mobile Identity Credentials
• Collaborative Approach: Across Alliance Councils & Partnering Organizations
• Use-Cases: Community Lead, Community Identified
• Raise Awareness of Approaches & Value Across Verticals
• Common Templates to support collaborative discussions
  ❑ Value Prop, Implementation, Challenges
  ❑ Security, Human Factors, Privacy, Technology, Arch, Policy
• Phased-set of Deliverables
  ❑ Initial Deliverable Focus at Concept Level
  ❑ Trends, Key Issues (Convergence, Conflicts, Synergies, Gaps)

This Webinar - Raise Awareness of the effort
• Provide a Broad Overview of Mobile Identity
• We Seek Your Feedback & Comments
• Encourage you to follow-up Adoption/Expansion/Leverage
Landscape Assessment

✓ Webinar #1 – In-Person Proofed Identities on Mobile Devices, Moderate & High Assurance Applications - Mobile Drivers License Use-Case (AAMVA/Gemalto, IDEMIA); Derived PIV/PIV Use-Case (ID Council/Intercede, DHS, DoD)

✓ Webinar #2 – Mobile Devices for Physical & Logical Access - Physical & Logical Access Use Cases (Access Council/Leidos, X Tec, HID, Exponent)

• Webinar #3 - Mobile Devices in Transportation, Health, & Banking - Transportation Use-Case (Transportation Council/SEPTA, SF-TA, Volpe), Banking Use-Case (Payment/SecureKey), Medical Use-Case (Health & Human Services Council/Ingenico, LifeMD-ID)

• Webinar #4 - Mobile Devices Enabling Users & Use Cases - Airport Use-Case/Facilities - Campus Wayfinding (AAAE); Colleges & Universities - Academic Integrity/Remote Proofing (IBIA/BioSig-ID)

• Webinar #5* - Mobile Devices Back-End Integration & Interoperability - Generic Physical & Logical Back End (Access Council, X Tec, AAAE) & Interoperability (Mobile Council, ID Council, IBIA)

* Note: Horizontals Discussion - Identity (Identity Council), Mobile (Mobile Councils), Biometrics (IBIA); to determine if need to present horizontals separately or if they can be included in Webinar #5.

Participating Councils: Access, Transportation, Health & Human Services, Payments, Mobile
Partnering Associations:
  AAAE - American Association of Airport Executives
  AAMVA – American Association of Motor Vehicle Administrators
  IBIA - International Biometric & Identity Association
Poll Question

What kind of identity form would you prefer to use in a healthcare setting?

A) Smart card with chip
B) Credit card with chip
C) Mobile wallet pass on smartphone
D) Biometric
E) Driver’s license
Identity Proofing: “You are who you say you are”

- Healthcare providers face identification problems due to lack of systems/processes
- Patients may be presenting with lack of information and common names/DOB
- Merging patient information in a Master Database may occur without awareness of inaccuracies or faulty data
- Lack of interoperable systems between facilities and, even, within Integrated Delivery Networks can lead to patient record matching issues
- If patient authentication processes exist, it is not always utilizing industry best practices for identity proofing
Identifying Patients across Care Continuum

Duplicate Records
Places patients at risk for undue treatments and medical errors while burdening the healthcare provider with unnecessary processes

- 92% of duplicate medical records are created during inpatient registration according to Johns Hopkins study
- ONC seeking to reduce that number of duplicate medical records to 2% in 2017 and 0.5% in 2020

Medical Identity Theft
Risk exposing PHI and all the burdensome pain associated with managing a breach

- Victims pay, on average, $13,500 to resolve medical identify theft, which may be a burden of the breached entity
- Incidents increased 22% between 2014 and 2015 impacting more than 2.3 million people in United States

Payment Fraud
Huge losses impacting public and private healthcare sector totaling tens of billions

- It is estimated that Medicare fraud costs taxpayers between $60 and $90 billion each year
- The entire United States healthcare system may experience $272 billion in fraud each year out of $2.7 trillion in spending
A patient’s identity must be accurately determined across the institutions that are sharing information before healthcare data about a specific patient can be integrated.

The complexity of linking patient identity across providers is exacerbated by the presence of multiple patient identifiers, syntactic and semantic differences in key patient demographic attributes, and duplicate patient registration records.
Example Use Case in Action: AIME™ by LifeMed ID

- Strong Identity Proofing within ONC Recommendations
- Standardized Identity Proofing training via NAHAM
- Establishes an interoperable “Master Record”: providing each unique patient identity with a Unique Health Safety Identifier (UHSI) with multi-factor authentication via a “token” (ex: credit card, biometric, smartphone)
- Links the UHSI to patient’s medical record(s)
Multiple Approaches to Identity including Mobile

- Patient owning and maintaining their identity in the format they prefer to use for authentication will be key to success, one size does not fit all.
- Identity proofing combined with improved process design will lead to higher collections of patient financial responsibility at time of service and post-service.
- Elimination of record duplication will improve medical record increasing patient safety and enabling care provider to make more informed decisions on care.
- Key aspect to improving interoperability across technological systems and care providers.
ADVANCING DIGITAL IDENTITY GLOBALLY: Banking Use Case

Judy Keator, SecureKey Technologies
Around the world banks face big challenges

- The price of Payment transactions is going to Zero
- Information about payments is worth more than the fee for processing
- Regulators are creating requirements to be more open
- Faster Payments is a growing reality – brings additional fraud risks, and competition
- The Bank’s presence at transaction in decline – they are losing their moment with the customer
- Digital ID is a market requirement
Canadian Banks: Started with Authentication

- 80+ departments
- 10 million registrations
- 99.99 availability
- Integrated at Affinity Credit Union, ATB Financial, BMO, Choice Rewards, CIBC, Desjardins, Caisses Populaires, National Bank, RBC, Scotiabank, Tangerine, TD, UNI
- Full customer indemnity agreements, call center support, soft handoffs, operational processes in place.
$30 MILLION INVESTMENT IN SECUREKEY FROM MAJOR BANKS TO DEVELOP DIGITAL IDENTITY NETWORK
WHY BUILD A DIGITAL IDENTITY ECOSYSTEM?

- Account opening is complex and expensive
- Fraudsters keep getting better
- It’s a mobile first world
- Regulatory requirements
- Customers resent friction
- Governments-driven identity models
- Consumers want more control over their data
FINDING WAYS TO ADD VALUE

- Open Data – Open Banking
- Increased competition from Fintech
- Need to create new sources of value
- Customers are increasingly living their lives digitally
- How do we leverage unique position of trust with customers to make their lives easier?
Key Considerations as we build Digital ID of the Future

- Resiliency against denial of service attacks
- No honeypots of data
- Consumer centric with a strong consent model
- Separation of Authentication and Attestation Service Providers
- Triple blind privacy matter – where Data Providers and Data Consumers are blinded from each other and Broker Operator can not observe data
- Standard - OAuth 2.0 / OpenID Connect, NIST 800-63-3, GDPR
A new ecosystem - Trusted Identity In Your Control

A new service for customers to manage their digital identity

Leverages a user’s existing connections with trusted public and private organizations

Enables simple, safe and secure sharing of personal information to 3rd parties from those sources

Provides high assurance by combining multiple factors and ID claims

What I Know

What I Have

What I Am
Financial Institution Roles

Digital Assets
- Name, DOB, Address, Account Duration, Phone #
- Name, Phone #, Account Duration, SIM Confirmation, Location
- Name, Address, DOB, ID#, Age of Majority, Photo
- Name, Address, DOB, Credit Score

Public Private Partnership
- Open bank/telco account
- See my medical records
- Access Gov Services
- Prove age of majority
- Get a Loan
- Prove that I am trusted
- Change address

SecureKey Technologies Inc. All rights reserved. Proprietary and Confidential
# A BANK’S VIEW

<table>
<thead>
<tr>
<th>Eliminate Costs / Drive Efficiency</th>
<th>Re-Intermediate with Customers</th>
<th>Generate Incremental Revenues</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Improve onboarding experience across product line and channels</td>
<td>• Provide tool for customers to reduce friction online</td>
<td>• Provide ‘identity as a service’ for onboarding and authentication</td>
</tr>
<tr>
<td>• Enable shift to lower-cost, automated channels</td>
<td>• Create strong, multi-factor authentication platform for use across industries</td>
<td>• Leverages assets generated for business-as-usual activities (verified data, strong authentication)</td>
</tr>
<tr>
<td>• Streamline cross- and up-sell capabilities</td>
<td>• Enhance brand positioning</td>
<td></td>
</tr>
<tr>
<td>• Leverage data from other partners to provide better customer offerings</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Experience – Credit card sign-up

- **Use case:** Financial Services companies want to offer customers the ability to sign up for new credit products online.

- **Business Driver:**
  - Current onboarding methods are expensive to complete – often allow customers to start sign-up process online, but require additional work to complete – e.g., come in-store to receive the card, outbound call centre for validation, etc.
  - High drop off rates for existing ID verification methods – e.g., low match rates for manually entered data, failure to answer knowledge-based credit-based questions, etc.

- **Web flow experience:** [link](#)
  - Select My Bank as the provider, and use any password for the demo.
Sun Life Case Study

- **Use case:** Sun Life group benefits customers registering for access to self-serve sunlife.ca account

- **Business Driver:**
  - Encourage customers to use self-serve channels (online, mobile app), which provides better customer experience and lower cost
  - Streamline online portal registration which can take up to 7 days (for postal mail codes) and requires customers to know their contract / member # (often forgotten)
  - Reduce cost of customer support (call centre based)

- **Attributes used:** bank name, date of birth, address, contact details; phone verification

- Further cost savings possible by eliminating password resets by leveraging Verified.Me to login and/or reset

“As part of our relentless focus on making it easier for our Clients to do business with us through new digital capabilities, we are proud to team up with SecureKey to offer an even more simplified online experience. As we take the next step along our digital transformation journey, we’ll soon be able to streamline and simplify the onboarding process for new Clients by using SecureKey’s permission-based tools and Blockchain security to instantly verify personal information.”

- Mark Saunders, Executive Vice-President & Chief Information Officer, Sun Life Financial.
We're here to help you build your financial future and live a bright, healthier life.
Call Center
Verified ID Helps Across the Customer Lifecycle

**Onboarding**
- New account opening / new user onboarding
  - Verify identity for service delivery
  - KYC / financial services (accounts, loans, etc.)

**Registration**
- Self-serve account registration
  - Transition existing customers to online, self-serve channels

**Account Maintenance**
- Update customer account information
  - Update address information and contact details
  - Sign up for direct deposit

**Transaction Verification**
- Validate user eligibility
  - Age and location verification for product sales (across channels)
  - Background check for sharing/gig economy, tenant screening

**Login / Authenticate**
- Authenticate returning users
  - Account login or recovery
  - Authenticate customers for support
Transportation Payments Use Case

Jerry Kane, SEPTA
Poll Question

What level of government or what organizations do you see leading the way toward deploying mobile ID for transportation?

A) City
B) State
C) Federal
D) Private-Public Partnerships
What is the Value Proposition?

Convenience

Reduced Fraud

Increased Efficiency

Providers can improve service efficiency and customer experience by supporting integrated, regional mobile identity service.

Mobile Identity would support verification to allow individualized services related to trip planning and fare payment.

The mobile I.D links the use of an existing credential to fare tariffs and apply rates and discounts for the traveler.
Transport NFC Compatibility

• Public transportation electronic ticketing is compatible with NFC mobile devices.

• NFC Mobile Device current uses:
  • Serve as the fare payment card or token;
  • Provide a channel to gain service and product information;
  • Offer multi-modal travel planning and payment.

NFC Agency
Contactless Cards

Mobile Ticketing – Bar Codes

Open payments with contactless cards…

…and mobile wallets.
Using Mobile Identity for Travel Account Registration and Management

• Today riders must provide ID at the operator’s location, sign an application, etc.; or register online to access services and wait for approval of personal data.

• A seamless approach could use an electronic primary identity that interfaces with the NFC enabled mobile device.

• No need for additional agency cross check before activating the account.
Mobility and Mobile NFC Platform

Building a Seamless Regional Travel Experience

- Mobile device for transit service interface
- Identity Management
- Account Based Ticketing
- Regional Interoperability
- Open payment service integration
- Bike Sharing Rental
- Public Transportation
- Parking
- Open payment service integration
- Mobility applications
## Challenges

<table>
<thead>
<tr>
<th>Absence of a Unifying Framework to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Integrate back office data management systems;</td>
</tr>
<tr>
<td>• Unify account and user data verification</td>
</tr>
<tr>
<td>• Verify account to support seamless travel among providers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business Relationships and Contracts</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Coordination between multiple operators and services</td>
</tr>
<tr>
<td>• Competing interests between proprietary vs. public information standards</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Complex Technology Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Complex legacy technologies</td>
</tr>
<tr>
<td>• High data security and privacy expectations</td>
</tr>
<tr>
<td>• Lack of industry standards</td>
</tr>
</tbody>
</table>
Selected Secure Technology Alliance Resources

- **Identity on a Mobile Device: Driver’s License and Derived Credential Use Case and Access Control Use Cases** webinar recordings - [https://www.securetechalliance.org/knowledge-center/](https://www.securetechalliance.org/knowledge-center/)

- **Secure Technology Alliance Knowledge Center** - [https://www.securetechalliance.org/knowledge-center/](https://www.securetechalliance.org/knowledge-center/)
  - [Smart Card Technology and the FIDO Protocols](https://www.securetechalliance.org/knowledge-center/), Secure Technology Alliance Identity Council white paper
  - [Mobile Devices and Identity Applications](https://www.securetechalliance.org/knowledge-center/), Secure Technology Alliance Identity Council white paper
  - [Mobile Identity Authentication](https://www.securetechalliance.org/knowledge-center/), Secure Technology Alliance Mobile Council white paper
  - [Smart Cards and Biometrics](https://www.securetechalliance.org/knowledge-center/), Secure Technology Alliance Access Control Council white paper

Contact Information

- Randy Vanderhoof, rvanderhoof@securetechalliance.org
- Tom Lockwood, tlockwood@nextgenid.com
- Jeffrey Fountaine, Jeffrey.Fountaine@ingenico.com
- Jerry Kane, jkane@septa.org
- Judy Keator, Judy.Keator@securekey.com