SECURE TECHNOLOGY ALLIANCE

Identity on a Mobile Device: Access Control Use Cases

Identity Council Webinar
July 26, 2018

Introductions

- Randy Vanderhoof, Secure Technology Alliance

- Tom Lockwood, NextgenID

- Neil Fallon, HID Global

- Dr. John Fessler, Exponent

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.

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

SECURE TECHNOLOGY ALLIANCE

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

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, 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
- 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

Connects & Defines Systems, Boundaries, & Transactions

Tangible, Necessary Real Market Relevance

Identity, Authentication, Authorization

Immediate Focus Mobile Device Landscape Assessment

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

The Problem & Value Outcome - Continued

OBJECTIVES

Phased-set of Deliverables

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

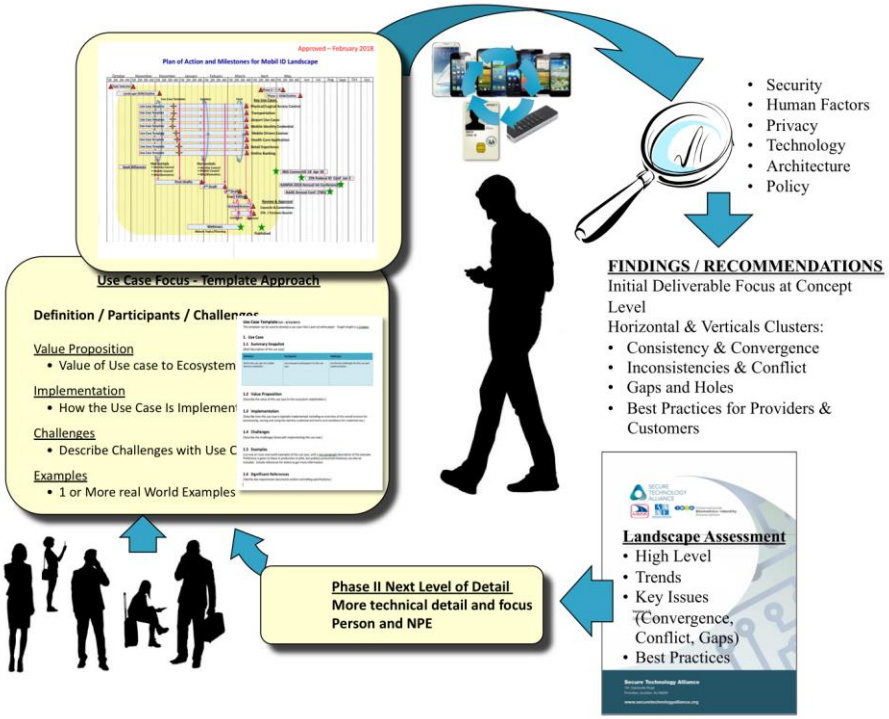
Approach

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 Webinar - 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

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 and Logical Access** - Physical & Logical Access Use-Case (Access Council/Leidos, XTec, HID, Exponent)
- **Webinar #3 - Mobile Devices for Ease of Use - Payment Integrity** - 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, XTec, AAAE) & Interoperability (Mobile Council, ID Council, IBIA)

* **Note: Horizontals Discussion - Identity (Identity Council), Mobile (Mobile Councils), Biometrics (IBIA); to determine if there is 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

Physical Access Use Cases

Neil Fallon, HID, Inc.

Poll Question

What are your plans for deploying a mobile or derived credential for physical access?

a. Already have deployed
b. Plan to deploy within the next 12 months
c. Plan to deploy within the next 24 months
d. Plan to deploy in more than 24 months
e. No current plans to deploy

What Do We Mean by “Mobile Devices?”

Smart Phones

Tablets

Wearables

“Mobile Devices”

Mobile Device Suitability

Smart Phones

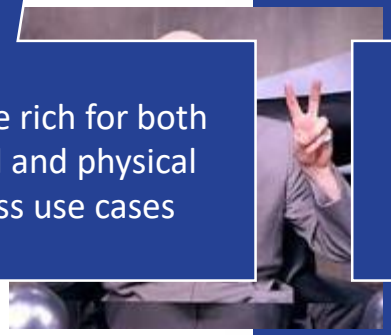
Feature rich for both logical and physical access use cases

Tablets

On par with smart phones for logical access to applications and services

Wearables

Not quite there yet as a multi-purpose credential platform



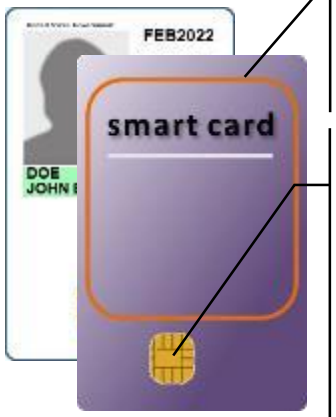
Feature-Rich and Ubiquitous Smart Phones

"Smart Phones"

- Everybody has one
- Everybody has one with them all the time
- Everybody knows how to use one

Comparison:
Smart Card and Smart Phone Features

Smart Cards



Contactless Interface
ISO 14443 (13.56 MHz)
and/or
RFID Prox (125KHz) Antennae

Micro-Chip
- CPU
- Memory (64 - 256 KB
- Crypto Engine
- Secure Element
- Keystore
- Timer
- Contact Interface

Smart Phones

Components
- CPU, GPU
- Memory
- Crypto Engine
- SIM
- Keystore/KeyChain
- Clock & Timers
- Display, Touchpad

Communications
- Cellular Service
- WiFi
- BlueTooth (5.0, LE)
- NFC*
- USB*

Sensors
- Camera (Photo, Vid)
- GPS
- Compass
- Accelerometer
- Gyro
- Proximity
- Fingerprint Scanner
- Barometer
- Iris Scanner*

Miscellaneous
- Visible Light Source
- IR Light Source*

Common Features	
• **Crypto Engine**	• **Keystore, Secure Element**
• **CPU**	• **Interface (ISO 14443 / NFC*)**
• **Memory**	

* Some Phones

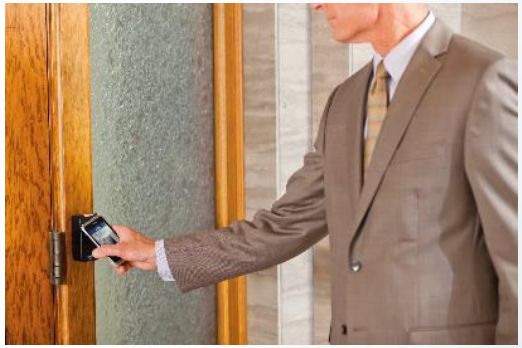
Smartphones Are Not the Future
They Are Now!

- Mobile Driver License
- Mobile Passport

- Vending Machine
- Mobile Payment

Smartphones Are Not the Future They Are Now!

- Access to Hotel Room

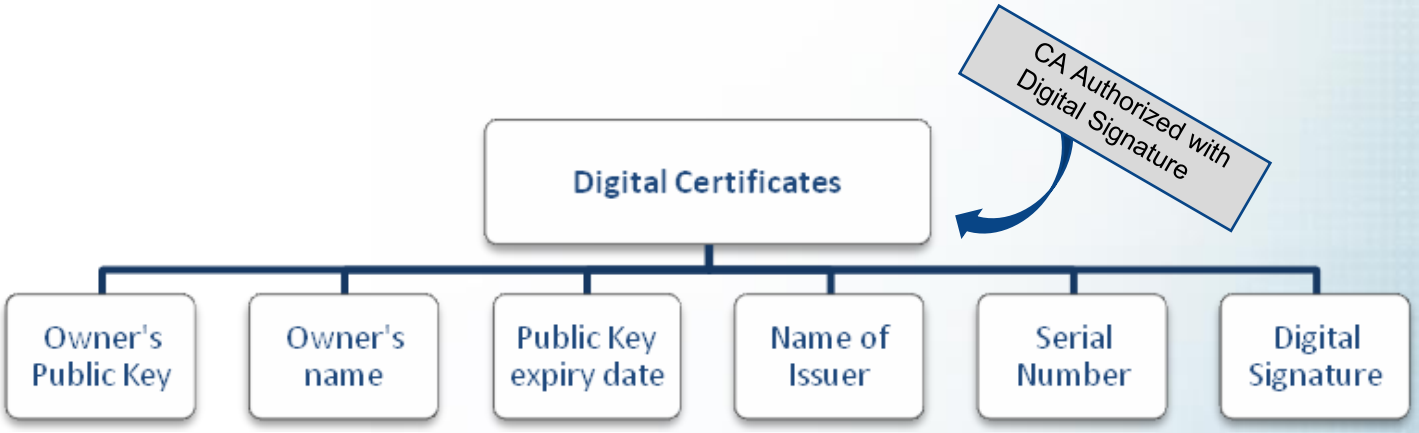


- Physical Access

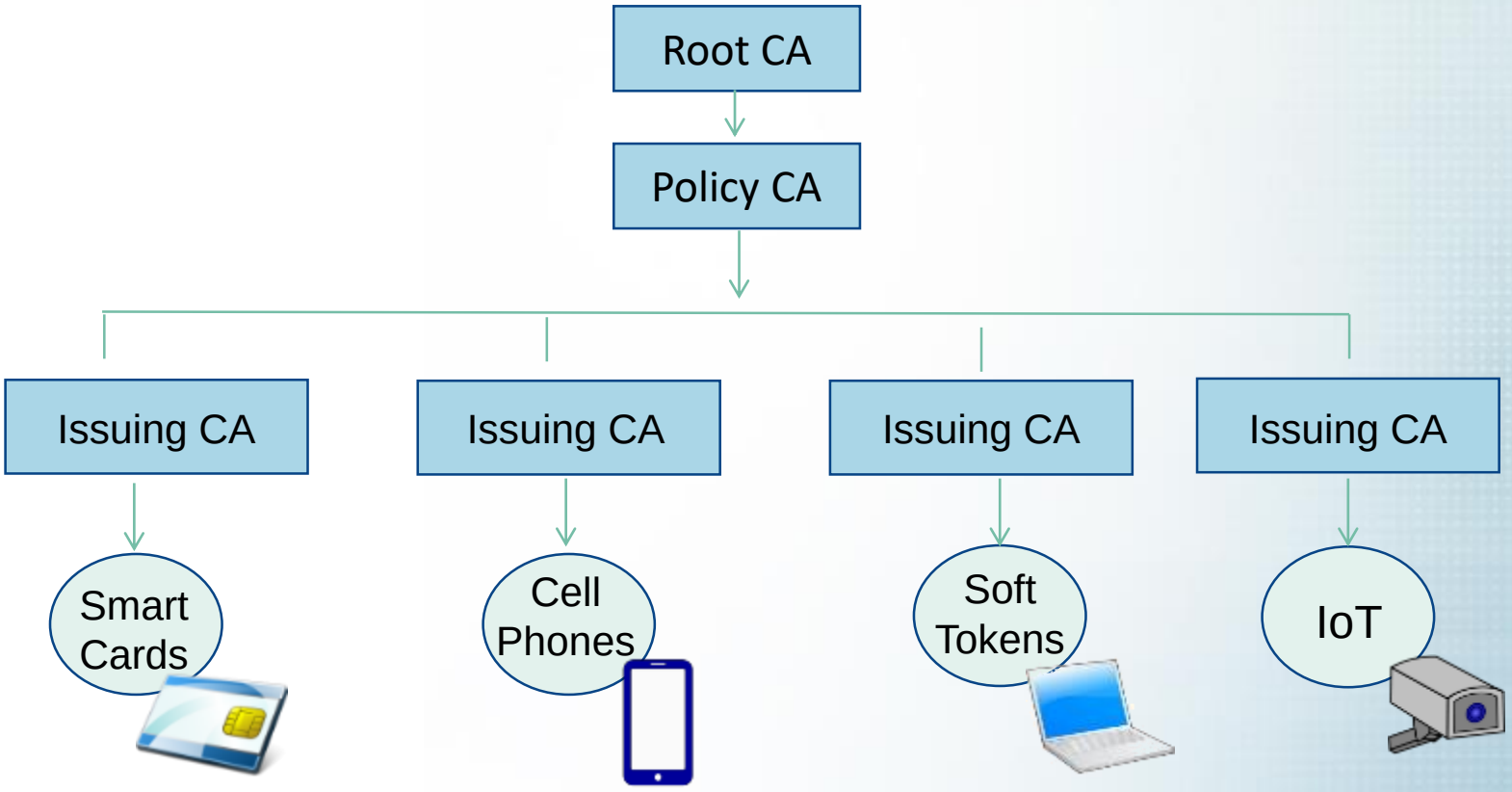
Digital Certificates

Certificate = identity information authenticated by a trusted third party called a Certification Authority

Certificates are the keys that control access to critical resources and data



Public Key Infrastructure



Symmetric vs Asymmetric Keys

Symmetric Key

- Locks
- Unlocks
- Must be kept private
- Same key for every user

Pro – fast for encryption

Con – one key compromised all keys compromised

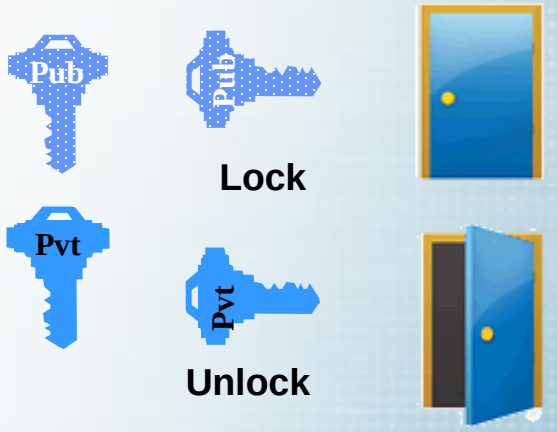
Asymmetric Key Pair

- One key encrypts; can be public
- Separate key decrypts; must be private
- Unique key pair for every Identity

Pro – one key compromised, others unaffected

Con – slower for encryption

Door Analogy



Physical Access Authentication Type

Traditional PACS

Encrypted communication with symmetric keys known by both the card and the reader

Certificate based PACS

Encrypted communication with certificate and public/private key
Private key is known only by the card
Certificate can be validated to ensure card has not expired or card was not stolen
Enables federation (employee's card from organization A is trusted by organization B)

Certificate Based PACS

- Certificate-based PACS –
  - Example: US Federal Government
    - CAC & PIV cards
    - 5.5 million active cards today
  - Example: CIV Credential

Certificate Based Card Enables the future

- Derived Credential to a Mobile Phone
- Virtual Smart Card issued to a Mobile Phone

Logical Access Use Cases

John Fessler, Exponent, Inc.

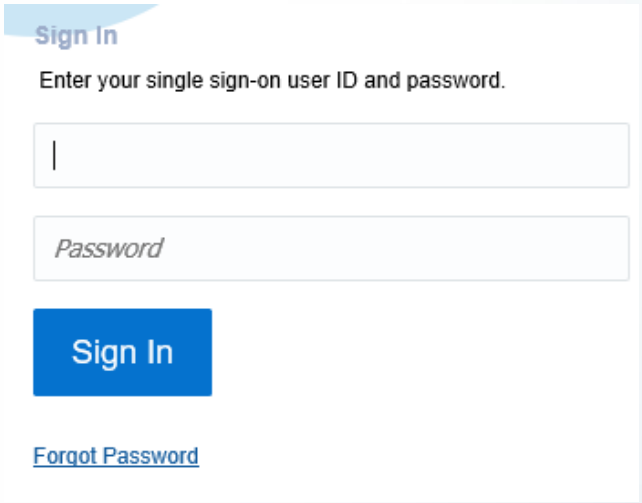
24

Poll Question

What are your plans for deploying a mobile or derived credential for logical access?

a. Already have deployed
b. Plan to deploy within the next 12 months
c. Plan to deploy within the next 24 months
d. Plan to deploy in more than 24 months
e. No current plans to deploy

Best Practice for Logical Access



NOT username and password

Best Practice for Logical Access

Best practice is to use multi-factor authentication.
Two or three of the following:

- Something you have (card, phone, USB token, etc.)
- Something you know (PIN or password)
- Something you are (biometric such as face, fingerprint, voice, gait, etc.)

8675309

Even better to use multifactor with PKI

Public Key Infrastructure (PKI)

As with physical access, a PKI-based system with digital certificates is often used for logical access due to its inherent security.

PKI allows you to:

- Verify that the identity was issued by the proper issuing agency
- Verify that the credential has not been changed or cloned
- Provide non-repudiation

PKI + Multifactor

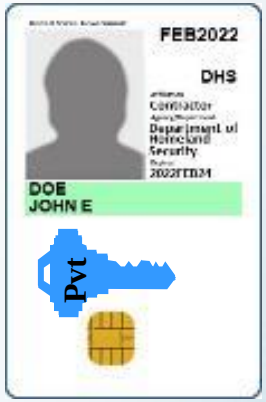
PKI is typically combined with multi-factor authentication as follows:

The “thing you have” securely stores the private key in a tamper-proof container
The “thing you know” or the “thing you are” is used to unlock access to that private key

8675309

and/or

Unlocks



Government Paves the Way

For about the last 20 years, the Department of Defense has been using a smart-card based logical access control system and the rest of the Federal government came on board over 10 years ago.

Implementing this system immediately resulted in a massive reduction in successful penetrations of government information systems.

Overview of implementation

- A public/private key pair is generated by the chip on the card.
- Private key gets locked away and can never leave the card.
- Public key gets incorporated into a publicly available certificate that is signed by the issuing agency
- PIN and/or fingerprint is used to unlock the private key to perform challenge/response authentication with the public key

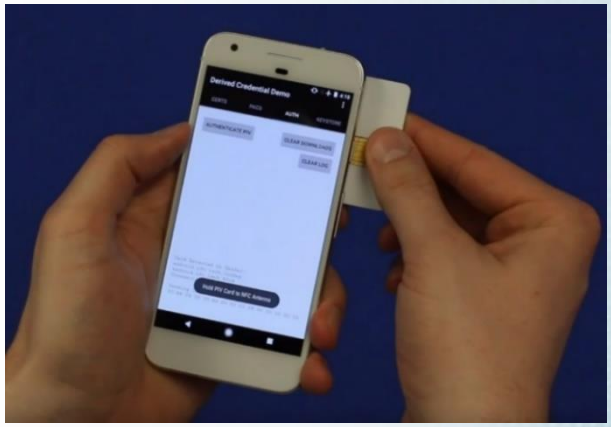
SECURE TECHNOLOGY ALLIANCE

The Problem with Mobile

While it is possible to use a card with a mobile device…

- NFC tap
- Card reader sleds

…it is not convenient enough.



Search for “pivopacity” on YouTube
https://www.youtube.com/watch?v=ftn8-Cth554&feature=youtu.be

We will now look at a few uses cases to see how people are implementing PKI credentials directly on mobile devices to improve security and usability.

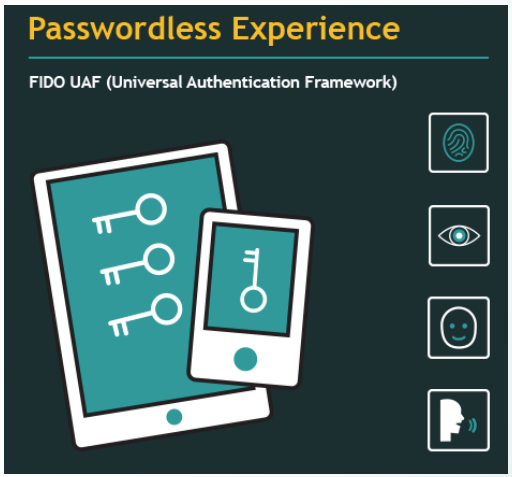
- Web access
- Enterprise Applications
- Peer-to-peer
- IoT and others

SECURE TECHNOLOGY ALLIANCE

Web Authentication with FIDO

The FIDO (Fast Identity On-line) Alliance is a consortium of companies and organizations dedicated to providing authentication solutions that are simple and safer for consumers. (fidoalliance.org)

- For mobile devices they provide a “passwordless experience” using their Universal Authentication Framework (UAF).



SECURE TECHNOLOGY ALLIANCE

Web Authentication with FIDO

Basic concept of FIDO

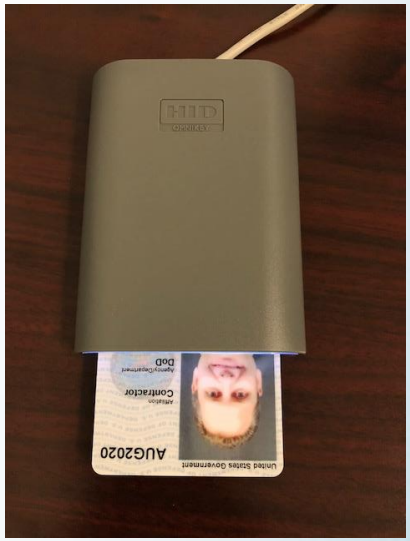
- For every website you go to, you have a separate public/private key pair.
  - All your various private keys are stored on your mobile device (in secure element, keychain, keystore, etc.)
  - You unlock the keys with a biometric
  - Website authenticates using a challenge response with the public/private keypair for that site
- Interesting combination of PKI for security while simultaneously enhancing privacy and even allowing anonymity (if desired)
  - The website doesn't need to know that this is John Fessler logging on, only that it is the same person who initially set up the account
  - Different keys for every website prevents cross-site tracking

PKI = Security + Privacy + Ease of Use

Enterprise Applications

For sensitive enterprise or government applications, card-based PKI credentials are routinely used on desktops/laptops to

- Encrypt messages (to protect contents while in transit)
- Sign messages (to authenticate the author)
- Access corporate information resource assets
  - Timesheets
  - Benefits
  - Calendars
  - Intranet
  - VPN
  - WiFi access



Enterprise Applications

Again, not super convenient to hold your card up to your phone every time you want to send or receive an email.

But, as apposed to FIDO, for enterprise applications you REALLY want to know that only authorized users are accessing your systems

This has led to the development of standards for “Derived Credentials”

- Take your existing, card-based credential and derive a second, software one that can be stored on your mobile device
- Storage options:
  - Inside of an app
  - Native system keychain or keystore
  - Inside a hardware secure element

SECURE TECHNOLOGY ALLIANCE

Deriving a Credential

When deriving a credential you need to start for a root of trust.

- Existing identity that has gone through the level of vetting and identity verification appropriate for the application.
- E.g., your corporate ID, your government-issued PIV card, etc.

Then prove possession of that ID to generate the new one

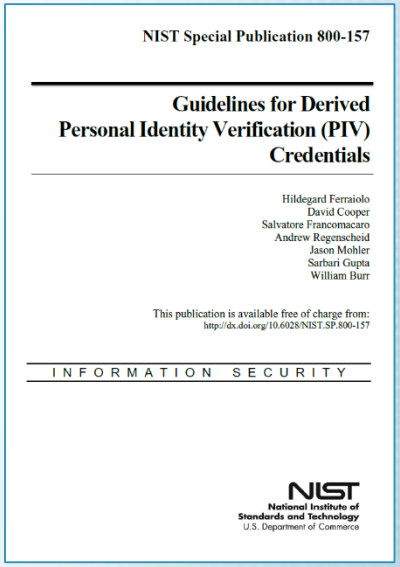
- Must have the original credential (e.g., card)
- Prove it is the rightful cardholder (with some combination of PIN, biometric, and/or in-person issuance, depending on level of assurance desired)

Then you can generate a new, derived credential that is linked to the original and store on the device

More on Derived Credentials

National Institute for Standards and Technology (NIST) has developed a standard for Derived Credentials for the Federal government's Personal Identity Verification (PIV) program.

- Published in Special Publication 800-157
- Information can be used for best practices for non-government use
- https://csrc.nist.gov/publications/detail/sp/800-157/final
- Covers generally-applicable topics like:
  - Lifecycle (issuance, maintenance, linkage with original ID)
  - Technical requirements (certificates, cryptography, activation)
  - Example, best practice issuance processes at two levels of assurance


NIST Special Publication 800-157

Guidelines for Derived Personal Identity Verification (PIV) Credentials

Hildegard Ferraiolo
David Cooper
Salvatore Francomacaro
Andrew Regenscheid
Jason Mohler
Sarbari Gupta
William Burr

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-157

INFORMATION SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

SECURE TECHNOLOGY ALLIANCE

Peer-to-Peer

- Under contract to the DHS, Exponent is working on peer-to-peer authentication that will allow two phone to authenticate each other over NFC or Bluetooth
- Quickly set up encrypted communication with a protocol called Opacity in less than a second
- Can be used to just authenticate the person or establish as secure, encrypted channel to communicate between two devices

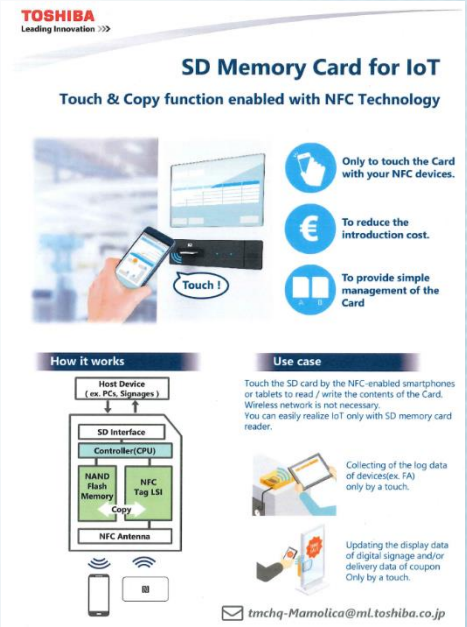
Other Logical Access Use Cases with Mobile Device

IoT

- Configuring and accessing connected devices from your mobile device
- Printer/copier access
- Downloading data from a smart device (e.g., smart power meter, thermostats, etc.)

Cloud access

Anything else you currently use a username and password for



SECURE TECHNOLOGY ALLIANCE

Q&A

Selected Secure Technology Alliance Resources

- **Identity on a Mobile Device: Driver's License and Derived Credential Use Case** – webinar recording - https://www.securetechalliance.org/knowledge-center/
- **Secure Technology Alliance Knowledge Center** - https://www.securetechalliance.org/knowledge-center/
  - Smart Card Technology and the FIDO Protocols, Secure Technology Alliance Identity Council white paper
  - Mobile Devices and Identity Applications, Secure Technology Alliance Identity Council white paper
  - Mobile Identity Authentication, Secure Technology Alliance Mobile Council white paper
  - Smart Cards and Biometrics, Secure Technology Alliance Access Control Council white paper
- **Securing Digital ID 2018**, December 4-5, 2018, Washington, DC - http://securingdigitalid.com/?utm=STA-Next-Event

SECURE TECHNOLOGY ALLIANCE

Contact Information

- Randy Vanderhoof, rvanderhoof@securetechalliance.org
- Tom Lockwood, tlockwood@nextgenid.com
- Neil Fallon, nfallon@hidglobal.com
- John Fessler, jfessler@exponent.com

SECURE TECHNOLOGY ALLIANCE

SECURE
TECHNOLOGY
ALLIANCE