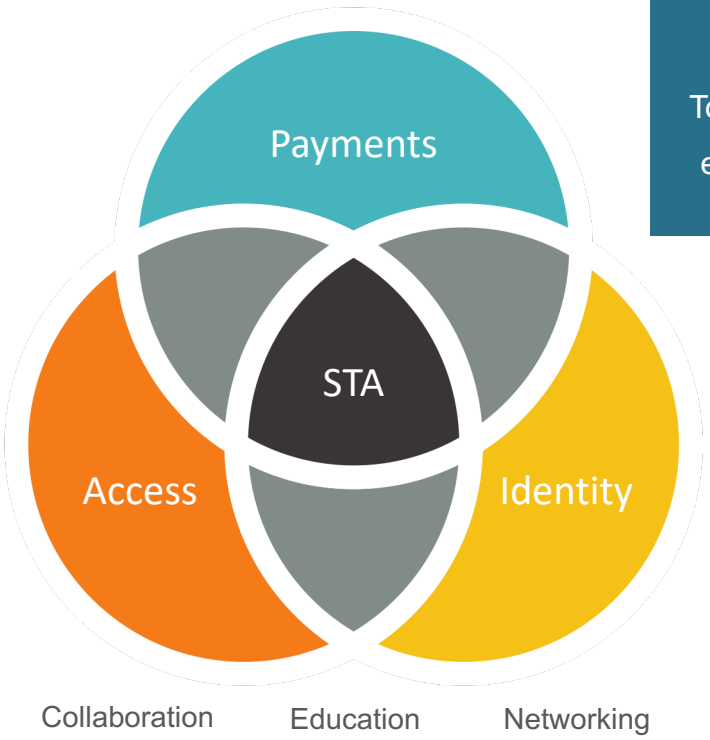
SECURE
TECHNOLOGY
ALLIANCE

The Future of Access Control

Secure Technology Alliance



Our Vision

To work together to continuously enhance security and user experiences in the payments, identity and access markets

Our Mission

To foster open dialogue between industry stakeholders to explore and develop secure technology innovations in the payments, identity and access markets. We will collaborate on education and guidance to stimulate understanding and enable efficient, timely and effective implementation of large-scale, disruptive technologies

SECURE TECHNOLOGY ALLIANCE

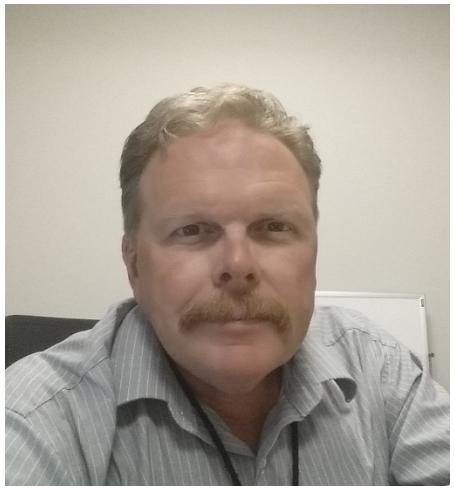
Secure Technology Alliance Access Control Council

Contributors, Access Control Council

- Gerry Smith, NIST Certified TECHNICAL EXPERT for cryptographic and security technology, Sr. Consultant, High Assurance Identity Verification Solutions, ID Technology Partners
- David Ferraiolo, Computer Sciences Team Lead, National Institute of Standards and Technology
- Colin Doniger, PSP, CSEIP, Program Lead, PACS Modernization, Department of Homeland Security
- Steve Rogers, CSCIP, President, IQ Devices, Inc.
- John Jacob, Director, Business Development, Federal Identity Solutions, Idemia Identity & Security
- William Windsor, Sr. Director, ICAM Solutions, Public Security, Federal, Idemia

SECURE TECHNOLOGY ALLIANCE

Panelist – Mark Dale



- Sr. Systems Engineer – Mobility, Xtec
- Background includes the design, development, and application of smartcard, biometric, derived credential, and mobile solutions.
- Focus is on alignment of solutions for commercial, Federal, State and Local identity, credential, and access management (ICAM) requirements across multiple vertical markets
- Actively engaged with the HSPD-12 rollout since 2004
- Also directly engaged in the HSPD-12 Program Management Offices (PMOs) at DHS, Treasury, DOL and VA.

SECURE TECHNOLOGY ALLIANCE

Panelist – Roger Roehr

- Director / Identity Management - Integrated Security Technologies – ist
- Lead architect for the Pentagon Force Protection Agency - Identity Credential Access Management (ICAM) system.
- Participated / led the delivery the GSA's FIPS 201 shared service solution; GSA Approved Vendor List and TWIC card program
- Previously the Chair of the STA's Access Control Council and Board Member of the Smart Card Alliance
- Certifications:
  - CSCIP-G, CSEIP, CBP

Panelist – Lars Suneborn

ID TECHNOLOGY PARTNERS

- Sr. Consultant – ID Technology Partners
- Impressive 40-year career spans multiple organizations where he's become recognized as a Physical Access Control System and High Assurance Identity credentialing subject matter expert
- Led a variety of US, Canadian and British security agencies PACS deployments at high-risk facilities
- Two-term Chair of the Access Control Council of the STA (2007 – 2012; 2019-PresentS)
- Leads the CSEIP Certification Program, and is actively promoting Smart Card, biometric and PKI cryptographic technologies as vital components in overall system designs.

SECURE TECHNOLOGY ALLIANCE

SECURE
TECHNOLOGY
ALLIANCE

Trending Authentication Credentials and Devices

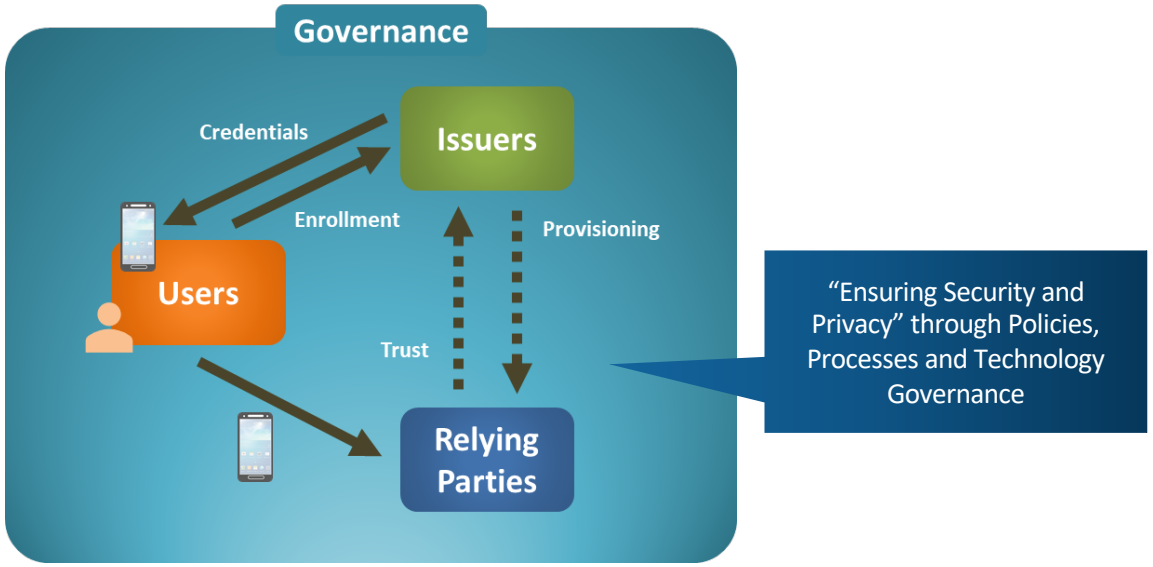
Agenda

- Security & Privacy Considerations for Trending Credentials
- Mobile devices will be leveraged for mobile ID's for both logical and physical access
- Trending credential examples
- Mobile IDs and biometrics use are expanding into new use cases
- Biometrics will be further expanded for specific use cases

SECURE TECHNOLOGY ALLIANCE

Security & Privacy First

Privacy & Security Focused Credentialing Trust Frameworks



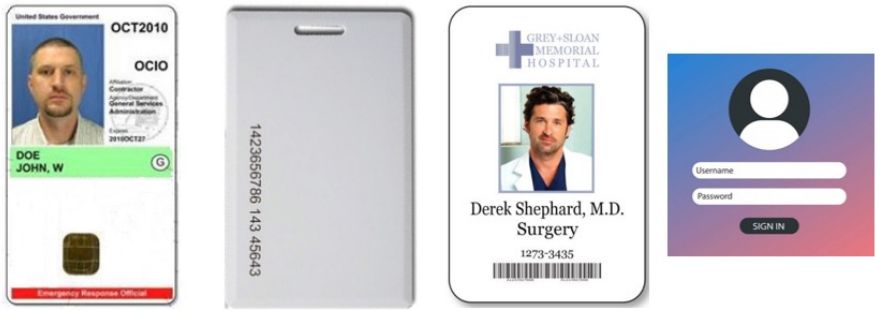
SECURE TECHNOLOGY ALLIANCE

SECURE TECHNOLOGY ALLIANCE

Trending Credential Devices

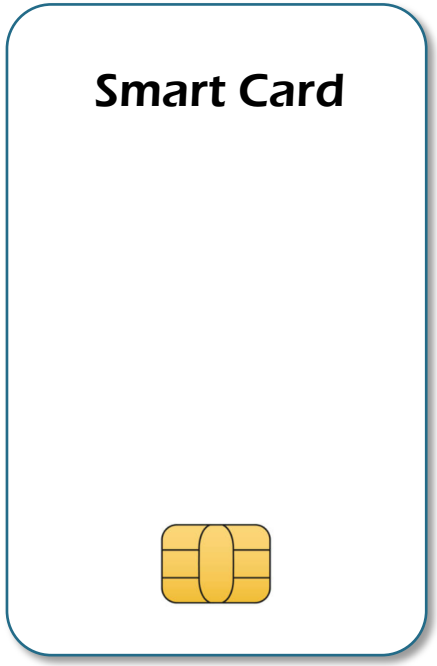
Traditional/Legacy Credentials

- Smartcards
- RFID Tags
- Flash Passes
- Driver's Licenses
- Username and Password



SECURE TECHNOLOGY ALLIANCE

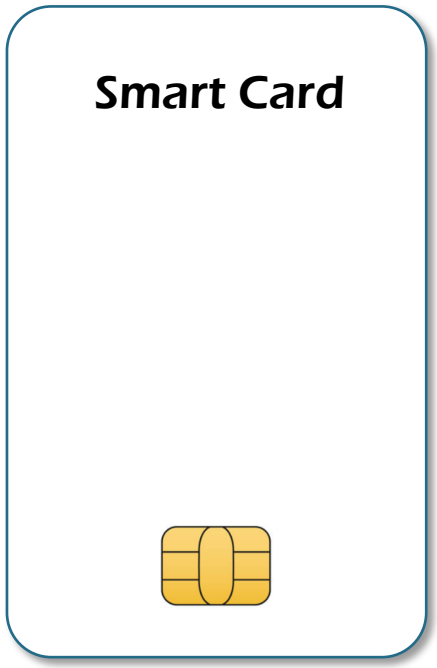
Smart Cards Exemplify Market Areas for Trend Changes



Smart Card Deployments

- Payments/Credit Cards
- Banking Cards
- Government IDs
- National IDs
- Company IDs
- University IDs
- Healthcare IDs
- ePassports
- Etc.

Mobile Device Credentials Are "Infringing" on Smart Card Markets



Smart Card Deployments

- Payments/Credit Cards ✓
- Banking Cards ✓
- Government IDs ✓
- National IDs ✓
- Company IDs ✓
- University IDs ✓
- Healthcare IDs
- ePassports
- Etc.

SECURE TECHNOLOGY ALLIANCE

Smart Mobile Device Value Proposition

Smart Phones

Tablets

Wearables

- Leverage Existing Devices
- Multiple Credentials on a Single Device
- Remote Credential Provisioning and Updates
- Provides Comparable Security Features to Smart Cards
- Support for Multi-Factor Authentication
- Unlimited Applications and Use Cases
- Increased Convenience, Accessibility & Expediency
- Etc.

Smart Mobile Device Features

Smart Phones

Tablets

Wearables

Components
- CPU, GPU
- Memory
- Clock & Timers
- Display, Touchpad
- Microphone & Speakers

Security
- Crypto Modules (SW & HW)
- Keystores/Keychains
- TEE
- Secure Elements
- SIMs

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

Sensors
- Camera (Photo, Video)
- GPS
- Compass
- Accelerometer
- Gyro
- Proximity
- Fingerprint Scanner
- Barometer
- Iris & Retina Scanner
- Heart Rate
- Blood Pressure

Mobile Device Physical and Logical Access Interfaces

Mobile Device Interfaces

- Near Field Communication (NFC)
- Bluetooth 5.0, Bluetooth Low Energy (BLE)
- Camera
- Display
- WiFi
- Cellular Services
- Push Notifications

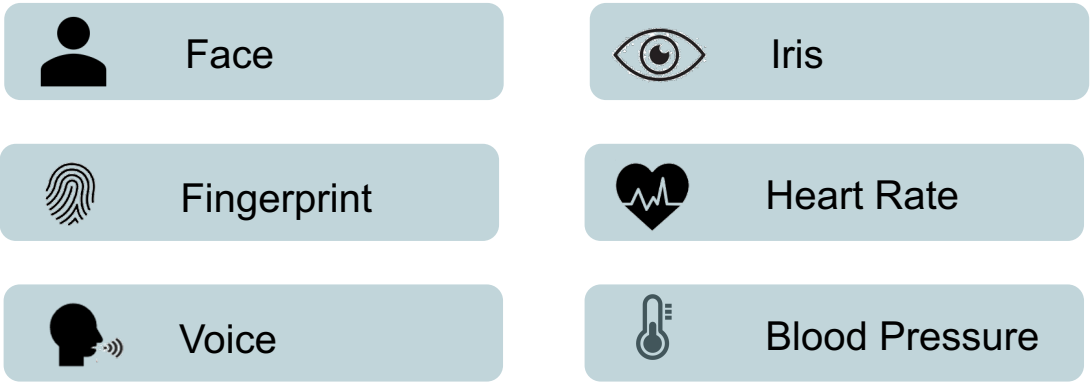
Local Authentication

Remote Authentication

Attended Authentication

SECURE TECHNOLOGY ALLIANCE

Example Mobile Device Biometric Capture Modalities



SECURE TECHNOLOGY ALLIANCE

Biometrics and the Traditional Multi-Factor Authentication (MFA) Model

Something You Have (Credential)
e.g., Digital Certificate, Public Key

Something You Know (Knowledge Based Authentication)
e.g., PIN, Passphrase, Personal information

Something You Are (Biometric)
e.g., Face, Fingerprint, Iris

Factors	Have	Know	Are	Assurance Level
Single Factor	✓			Low
Single Factor		✓		Low
Single Factor			✓	Low
2-Factor	✓	✓		Medium
2-Factor	✓		✓	Medium
2-Factor		✓	✓	Medium
3-Factor	✓	✓	✓	High

Mobile Devices Can Expand Authentication Factors

For example:

Presence Authentication - “Somewhere You Are”

GPS and proximity sensors can be used to confirm that a user is present at an authentication reader or has been verified to have been somewhere else in support of authentication.

Behavioral Authentication - “Something You Do”

Sensors, including gesture, gyro, accelerometer, pedometer, and proximity sensors, can be used to establish a behavioral profile.

Physiological Authentication - “How You Are”

Wearable heart rate, blood pressure and activity sensors can be exploited to establish a physiological biometric profile.

SECURE TECHNOLOGY ALLIANCE

Trending Credentials

Credentialing Frameworks

Enterprise/Dedicated – Vertical Markets

- Federal government credentials
  e.g., PIV, CAC, TWIC, Derived Credentials
- Corporate Credentials
  e.g., Corporate ID's, PIV-I

Universal – Horizontal Markets

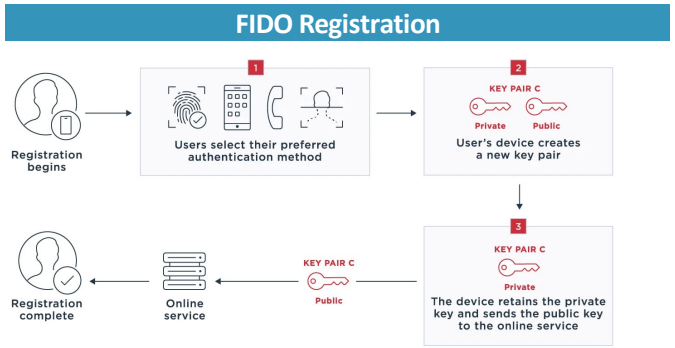
- Trending Credential can be used across markets
- E.g., FIDO, Verifiable Credentials, Mobile Driver's Licenses

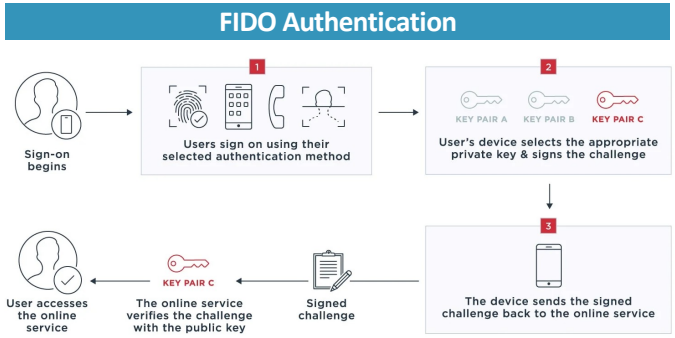
FIDO (Fast IDentity Online)

Widely Deployed

Features

- Based on RSA Key Pairs generated on client device
- Public key is used as an identifier and as an authenticator
- Decentralized credentials and authentication protocols based on asymmetric cryptographic key pairs generated on the mobile device
- Multifactor Authentication supported (e.g., biometric or PIN)
- FIDO governance is overseen by the FIDO Alliance – w/ Google, Apple, Amazon, VISA, etc.





Images from: "FIDO: Everything You Need to Know About Fast Identity Online" https://www.pingidentity.com/en/company/blog/posts/2021/fast-identity-online-fido.html

SECURE TECHNOLOGY ALLIANCE

Verifiable Credentials

Gaining Ground

Features

- Decentralized digitally signed credentials
- Issuer establishes decentralized data repositories accessible by Verifiers
- Verifiable data repository typically based on Blockchain Ledgers
- Verifiable Credential governance is overseen by the World Wide Web Consortium (W3C)

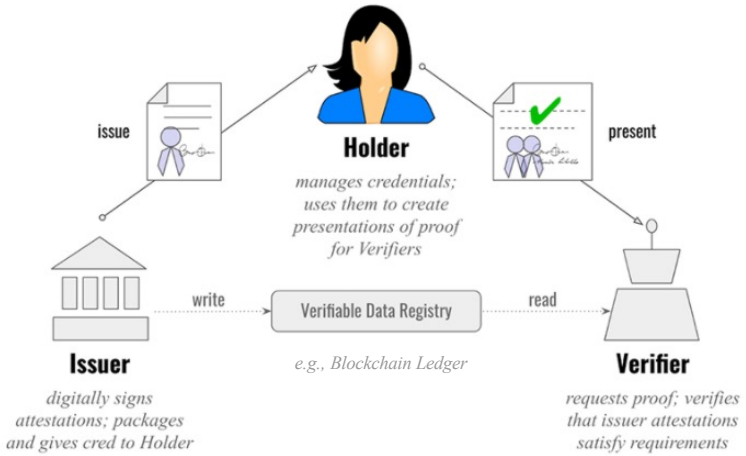


Image from: "A Gentle Introduction to Verifiable Credentials"
https://www.evernym.com/blog/gentle-introduction-verifiable-credentials/

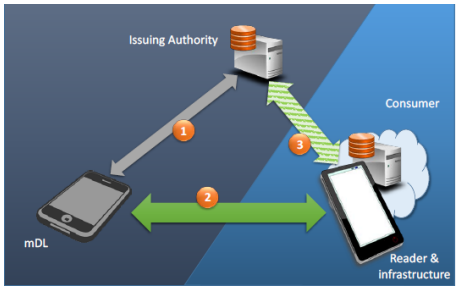
SECURE TECHNOLOGY ALLIANCE

Mobile Driver's License (mDL) & ISO 18013-5

Wide Adoption Pending

Features

- mDLs issued by State and International "DMVs"
- mDL standard allow for interoperability for a large range of Use Cases
- Consists of Signed Entities, Attributes, Keys and Digital Certificates
- mDL's are based on ISO international standards (e.g., ISO 18013-5)
- ISO 18013-5 can be applied to non-mDL Mobile Credentials
- mDL governance in the US is overseen by AAMVA, and in Europe by EReg



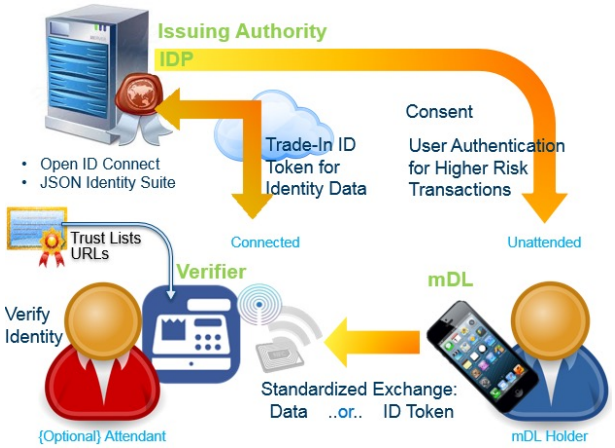


Image from: "The Mobile Driver's License (mDL) and Ecosystem"
https://www.securetechalliance.org/publications-the-mobile-drivers-license-mdl-and-ecosystem/

SECURE TECHNOLOGY ALLIANCE

SECURE TECHNOLOGY ALLIANCE

Summation

Future of Access Control Key Points

Devices

Mobile devices provide a rich feature set for a wide range of access applications

Sophisticated Wearables will have increased applicability (e.g., Smart Watches, Bands and Rings)

Credentials

Current credential types will see expanded use

Emerging credentials will gain wide adoption for both logical and physical access use cases (e.g., mobile driver's licenses)

New credentials types will be introduced (e.g., quantum computing-based credentials)

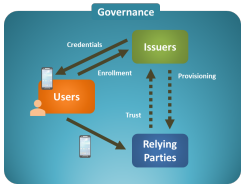
Biometrics

Biometrics will be employed for a variety of targeted use cases

Either as a single-factor mode, or in support of multi-factor authentication

Expanded Authentication Factors

Mobile devices support authentication factors beyond the traditional MFA Model, e.g., "Somewhere You Are", "Something You Do", and "How You Are"



SECURE TECHNOLOGY ALLIANCE

References

- STA “Using Mobile Devices for Physical Access” whitepaper https://www.securetechalliance.org/publications-using-mobile-devices-for-physical-access-control/
- The Mobile Driver’s License (mDL) and Ecosystem https://www.securetechalliance.org/publications-the-mobile-drivers-license-mdl-and-ecosystem/
- NSA “Selecting Secure Multi-factor Authentication Solutions” https://media.defense.gov/2020/Sep/22/2002502665/-1/-1/0/CSI_MULTIFACTOR_AUTHENTICATION_SOLUTIONS_UOO17091520.PDF

SECURE
TECHNOLOGY
ALLIANCE

Trending Authentication Credentials and Devices

The Context of the "Future" of Access Control

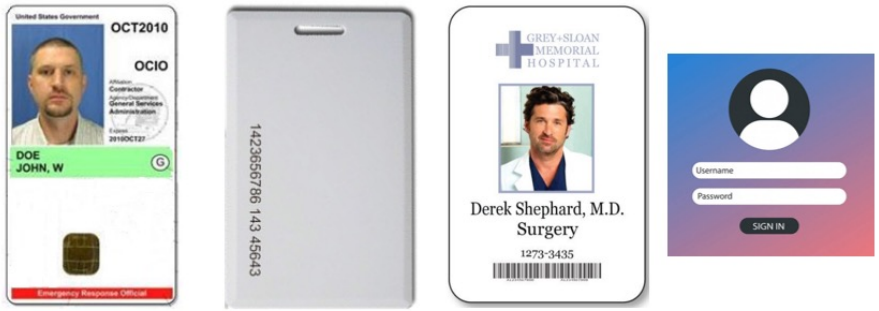
- ❑ Mobile devices will continue to be leveraged for both logical/online and physical access
- ❑ Mobile IDs and biometrics use are expanding into new areas
- ❑ Biometrics will be further expanded for specific use cases
- ❑ Trending credentials
  - Derived Credentials – (*Federal implementation that may be leveraged elsewhere)*
  - FIDO - *(widely used)*
  - Verifiable Credentials - *(gaining ground)*
  - Mobile driver's licenses - *(pending widespread adoption)*

SECURE TECHNOLOGY ALLIANCE

Trending Credential Devices

Traditional/Legacy Credentials

- Smartcards
- RFID Tags
- Flash Passes
- Credit Cards
- Driver's Licenses
- Username and Password



SECURE TECHNOLOGY ALLIANCE

Trending Credential Hosting Devices

Smart Phones

Tablets

Wearables

Benefits & Value Proposition

- Lower Costs
- Adaptable Security using Multifactor Authentication
- Increased
  - Convenience
  - Accessibility
  - Expediency

Smart Device Features

Smart Phones

Tablets

Wearables

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

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

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

Miscellaneous
- Visible Light Source
- IR Light Source
- Barcode/QR Code Scan/Display
- Physiology sensors, e.g., heart rate, motion, blood pressure

Mobile Device Physical Access Interfaces

Mobile Device Interfaces

- Near Field Communication (NFC)
- Bluetooth 5.0, Bluetooth Low Energy (BLE)
- Camera
- Display
- WiFi
- Cellular Services
- Push Notifications

Local Authentication

Remote Authentication

Attended Authentication

SECURE TECHNOLOGY ALLIANCE

Traditional Multi-Factor Authentication (MFA) Model

Something You Have (Credential)
e.g., Digital Certificate, Public Key

Something You Know (Knowledge Based Authentication)
e.g., PIN, Passphrase, Personal information

Something You Are (Biometric)
e.g., Face, Fingerprint, Iris

Factors	Have	Know	Are	Assurance Level
Single Factor	✓			Low
Single Factor		✓		Low
Single Factor			✓	Low
2-Factor	✓	✓		Medium
2-Factor	✓		✓	Medium
2-Factor		✓	✓	Medium
3-Factor	✓	✓	✓	High

Mobile Devices Can Expand Authentication Factors

For example:

Presence Authentication - “Somewhere You Are”

GPS can be used to confirm that a user is present at an authentication reader or has been verified to have been somewhere else that supports authentication.

Behavioral Authentication - “Something You Do”

Sensors, including gesture, gyro, accelerometer, pedometer, and proximity sensors, can be used to establish a behavioral profile.

Physiological Authentication - “How You Are”

Wearable heart rate, blood pressure and activity sensors can be exploited to establish a physiological biometric profile.

SECURE TECHNOLOGY ALLIANCE

Trending Credentials

Credential Issuance

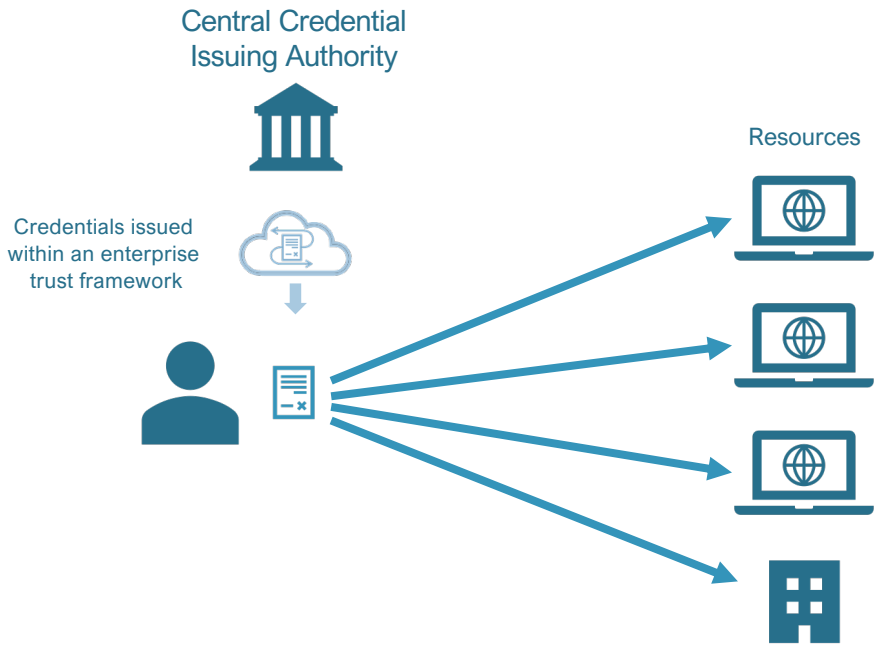
Centralized (Enterprise, Universal – Horizontal Markets)

- Federal government smartcard credentials
  (e.g., PIV, CAC & TWIC)
- Digital Certificates
- Derived Credentials

De-centralized (Local, Dedicated – Vertical Markets)

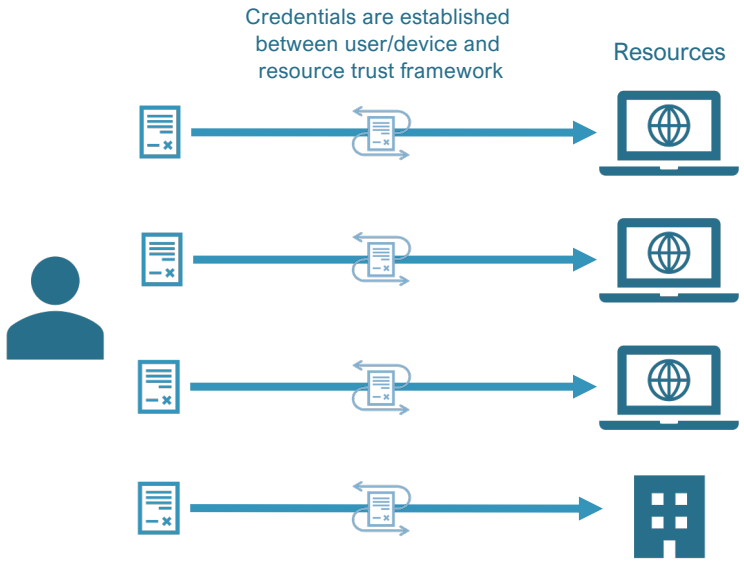
- FIDO
- Verifiable Credentials
- Mobile Driver's Licenses
- Username/Password + OTP & QR Codes

Centralized Credentials



SECURE
TECHNOLOGY
ALLIANCE

Decentralized Credentials



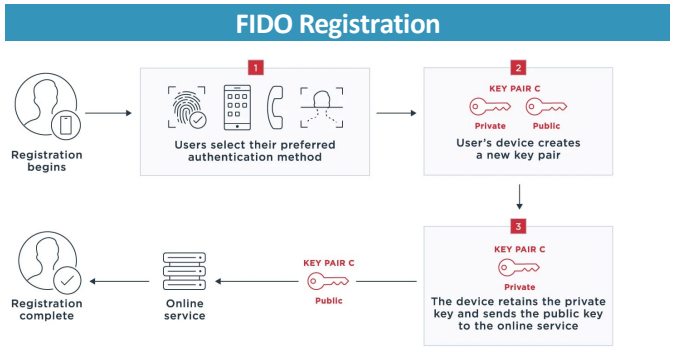
SECURE TECHNOLOGY ALLIANCE

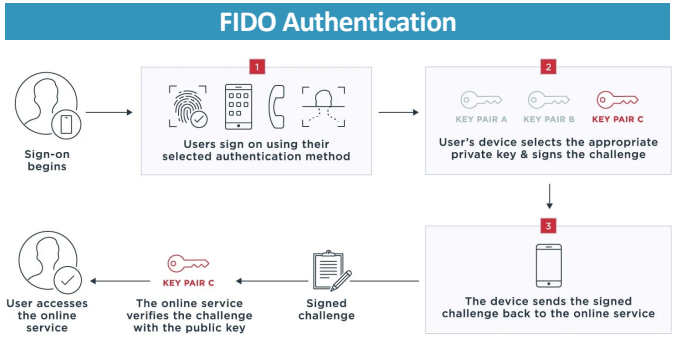
FIDO (Fast IDentity Online)

Widely Deployed

Features

- Based on RSA Key Pairs generated on client device
- Public key is used as an identifier and as an authenticator
- Decentralized credentials and authentication protocols based on asymmetric cryptographic key pairs generated on the mobile device
- Multifactor Authentication supported (e.g., biometric or PIN)
- FIDO governance is overseen by the FIDO Alliance – w/ Google, Apple, Amazon, VISA, etc.





Images from: "FIDO: Everything You Need to Know About Fast Identity Online" https://www.pingidentity.com/en/company/blog/posts/2021/fast-identity-online-fido.html

SECURE TECHNOLOGY ALLIANCE

Verifiable Credentials

Gaining Ground

Features

- Decentralized digitally signed credentials
- Issuer establishes decentralized data repositories accessible by Verifiers
- Verifiable data repository typically based on Blockchain Ledgers
- Verifiable Credential governance is overseen by the World Wide Web Consortium (W3C)

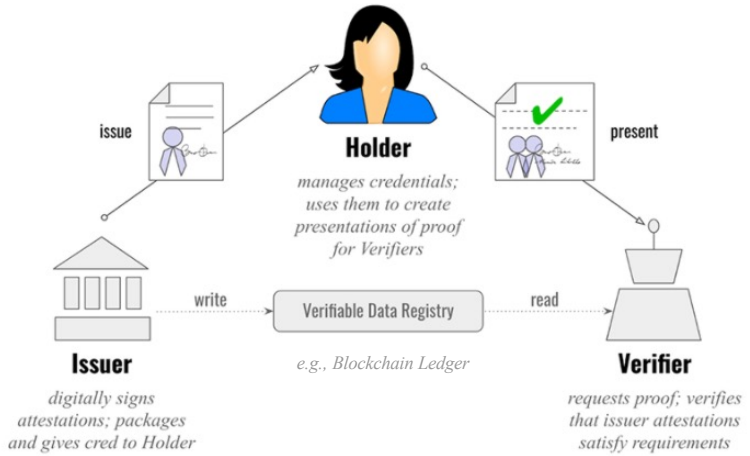


Image from: "A Gentle Introduction to Verifiable Credentials"
https://www.evernym.com/blog/gentle-introduction-verifiable-credentials/

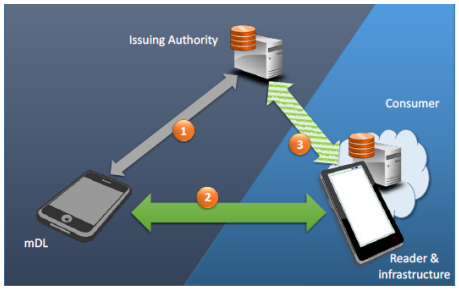
SECURE TECHNOLOGY ALLIANCE

Mobile Driver's License (mDL)

Wide Adoption Pending

Features

- Consists of Attributes and Digital Certificates provisioned to mobile devices
- mDLs issued by State DMVs
- mDL standards allow for interoperability for a large range of Use Cases that are not governed by a central Trust Framework
- mDL's are based on ISO international standards (e.g., ISO 18013-5)
- mDL governance in the US is overseen by AAMVA, and in Europe by EReg



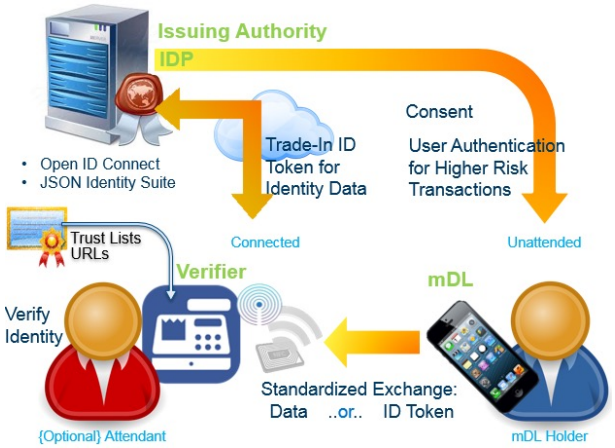


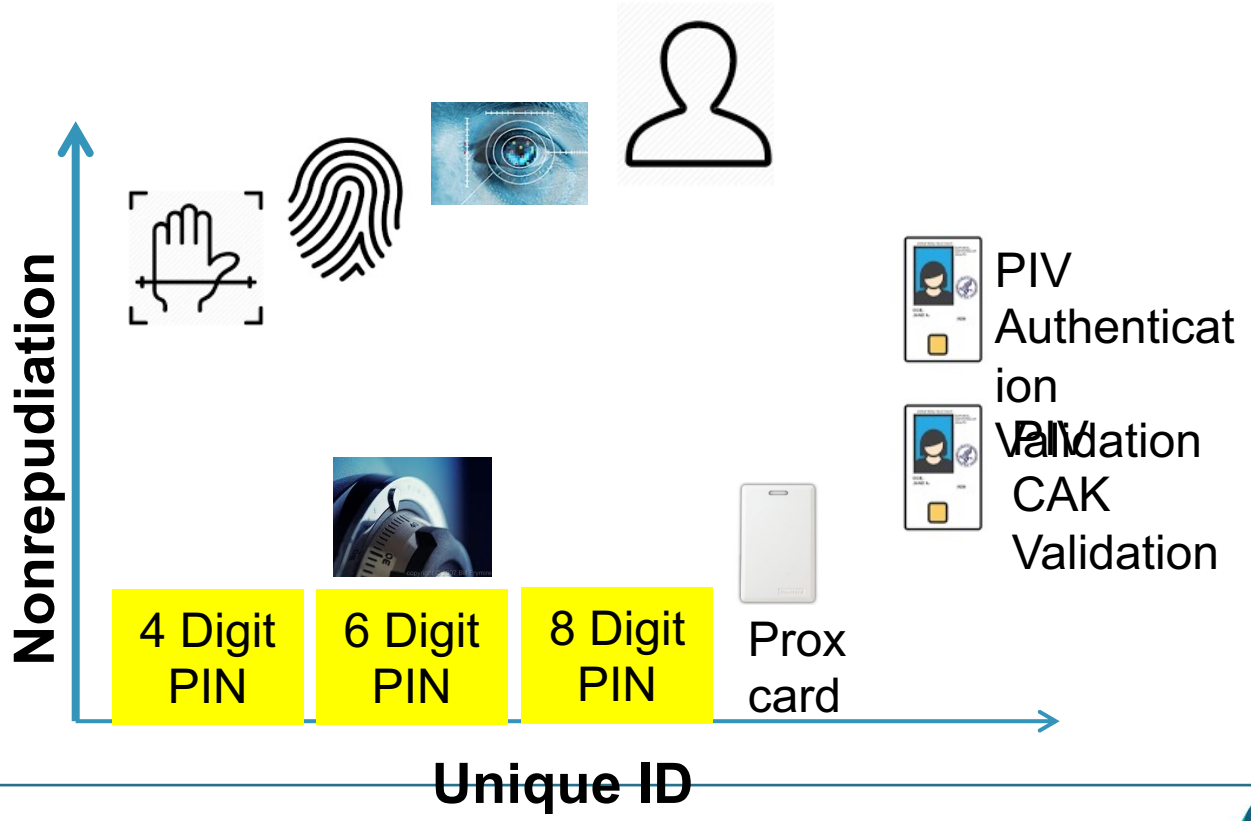
Image from: "The Mobile Driver's License (mDL) and Ecosystem"
https://www.securetechalliance.org/publications-the-mobile-drivers-license-mdl-and-ecosystem/

SECURE TECHNOLOGY ALLIANCE

SECURE TECHNOLOGY ALLIANCE

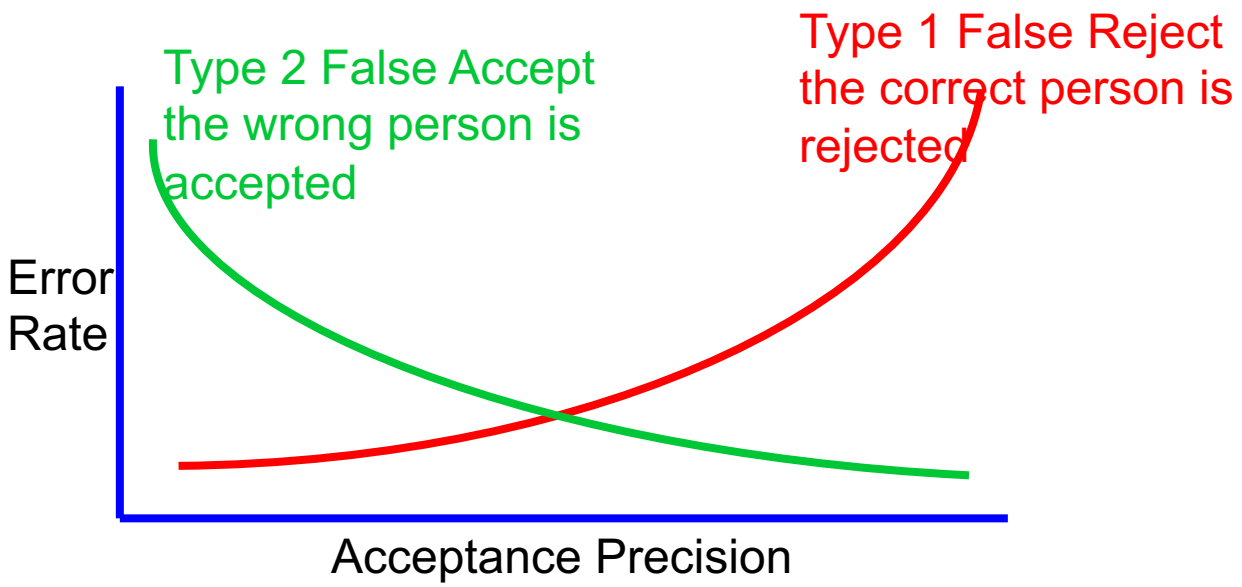
Trending Biometric Usage

How Biometric fit in with other Identity Factors



SECURE TECHNOLOGY ALLIANCE

Biometrics unlike the other factor are not absolute! They are only a measure of relationship of the Probe to the Refence biometric. The higher accuracy setting the more likely you will be falsely rejected.

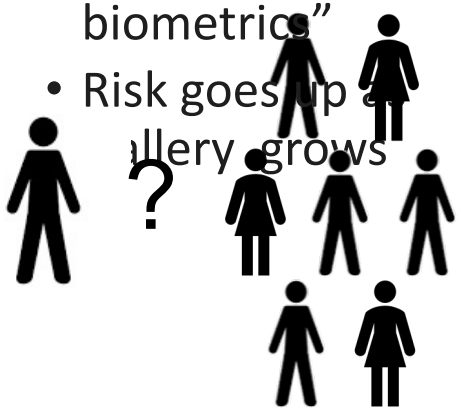


SECURE TECHNOLOGY ALLIANCE

Biometric Matching

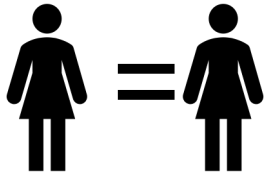
Identification

- One-to-many (1-N)
- Match to a gallery of "reference biometrics"
- Risk goes up as gallery grows

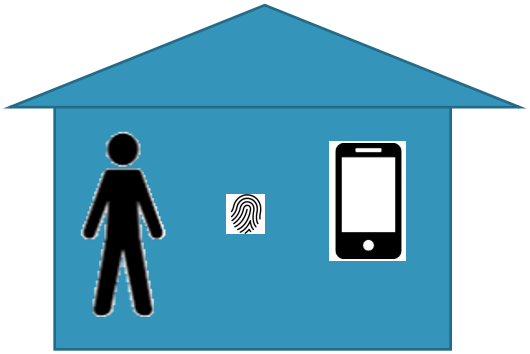


Verification

- One-to-one (1-1)
- Match to single "reference biometric"
- Risk stay the same regardless of the size of the Gallery

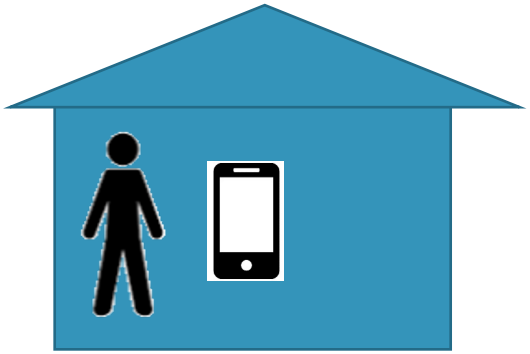


New Age Multi factor



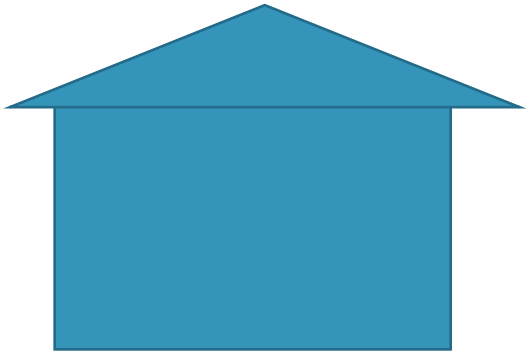
SECURE TECHNOLOGY ALLIANCE

New Age Multi factor



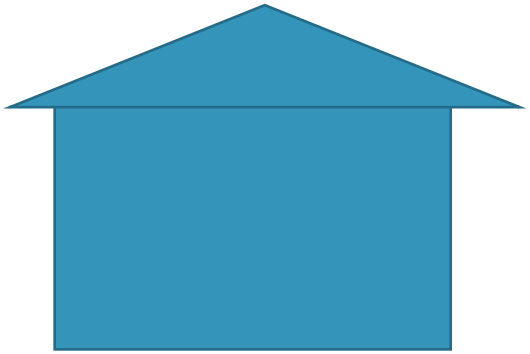
SECURE TECHNOLOGY ALLIANCE

New Age Multi factor

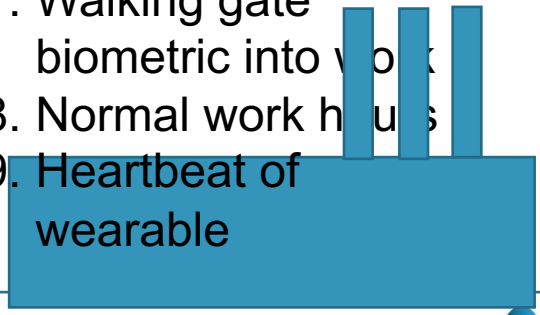


SECURE TECHNOLOGY ALLIANCE

New Age Multi factor

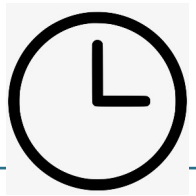


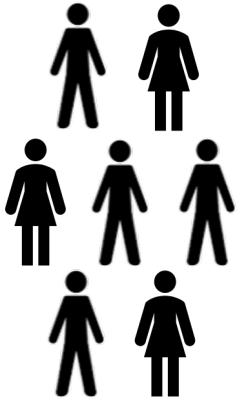
1. Phone
2. Fingerprint
3. Home WiFi
4. Walking time between home and car
5. Bluetooth of same car
6. Uses Waze navigation
7. Walking gate biometric into work
8. Normal work hours
9. Heartbeat of wearable

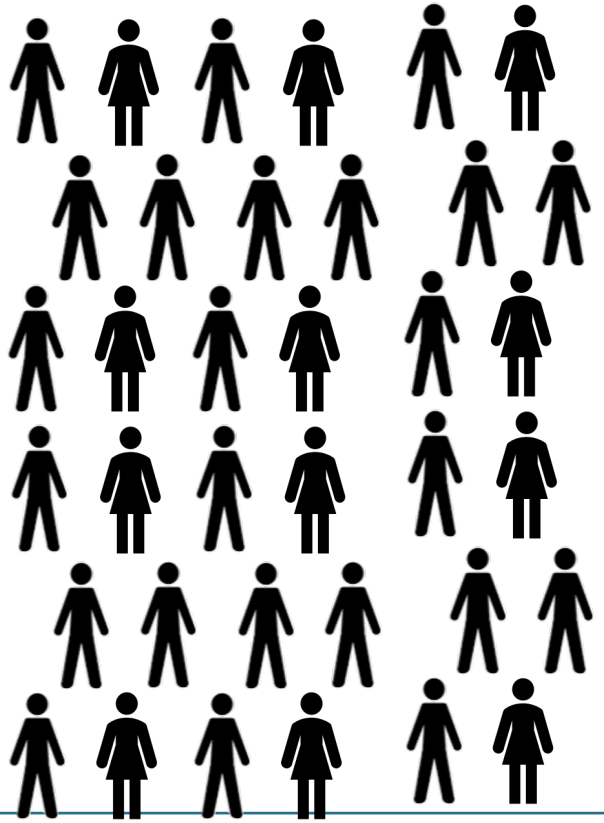


SECURE TECHNOLOGY ALLIANCE

Controlling the Gallery for 1N







SECURE TECHNOLOGY ALLIANCE

SECURE TECHNOLOGY ALLIANCE

Single-Factor Biometric Use Cases

Single-Factor Biometric

- Disadvantages
  - High Error Rate compared to other biometrics
  - COVID-related mask wearing
- Advantages
  - Low-cost equipment/cameras
  - Low cost to implement
  - Convenient
  - Expeditious
- Suitability
  - Low-risk use cases
  - Leverages “Small” biometric reference pool
  - Managed and controlled populations

Biometrics and the Traditional Multi-Factor Authentication (MFA) Model

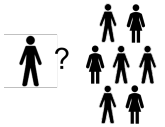
Something You Have (Credential)
e.g., Digital Certificate, Public Key
Something You Know (Knowledge Based Authentication)
e.g., PIN, Passphrase, Personal information
Something You Are (Biometric)
e.g., Face, Fingerprint, Iris

Factors	Have	Know	Are	Assurance Level
Single Factor	✓			Low
Single Factor		✓		Low
Single Factor			✓	Low
2-Factor	✓	✓		Medium
2-Factor	✓		✓	Medium
2-Factor		✓	✓	Medium
3-Factor	✓	✓	✓	High

Single-Factor Facial Recognition Sample Use Cases

Cruise Ships

- Boarding
- Room Entry
- Dining Areas
- Bars
- Access to Entertainment Venues
- Onboard Purchases



Fitness Centers

- Facility Entry
- Locker Rooms
- Purchases
- Special Equipment Use
- Fitness Tracking

Adoption Factors

- Low risk environments
- Low cost
- Fast authentication
- Small biometric reference pools
- Convenience
- Expediency

SECURE TECHNOLOGY ALLIANCE

SECURE TECHNOLOGY ALLIANCE

Summation

Future of Access Control Key Points

Devices

- Mobile devices provide a reach feature set for a wide range of access applications
- Sophisticated Wearables will have increased applicability (e.g., Smart Watches, Bands and Rings)

Credentials

- Current credential types will see expanded use
- Emerging credentials will gain wide adoption for both logical and physical access use cases (e.g., mobile driver's licenses)
- New credentials types will be introduced (e.g., quantum computing-based credentials)

Biometrics

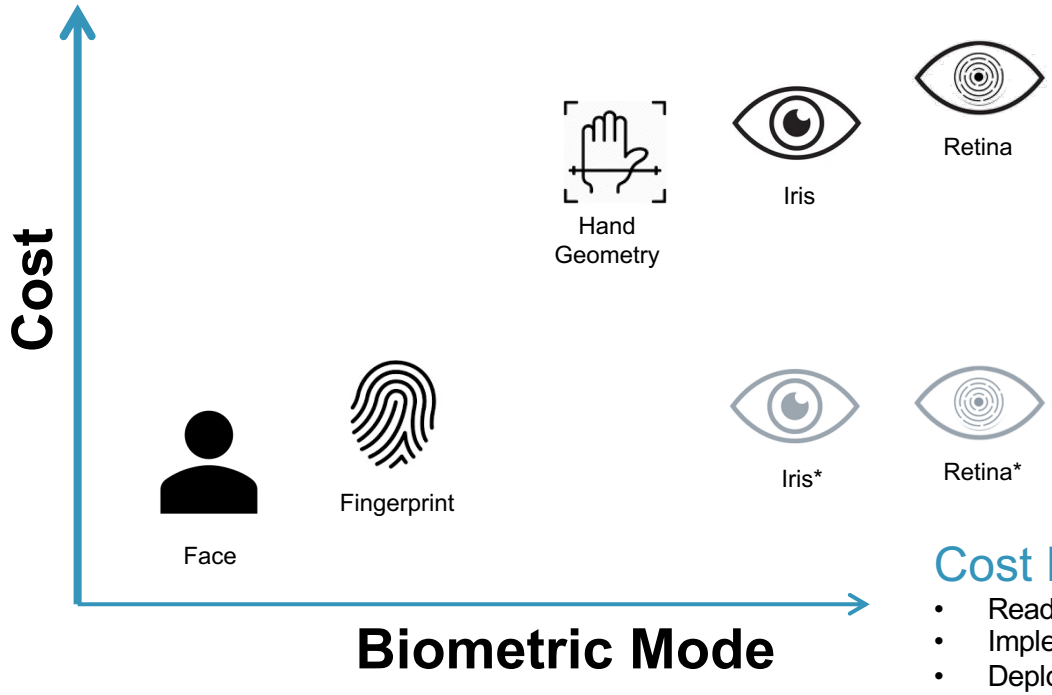
- Biometrics will be employed for a variety of targeted use cases
- Either as a single-factor mode, or in support of multi-factor authentication

Authentication Factors

- Mobile devices support authentication factors beyond the traditional MFA Model, e.g., "Somewhere You Are", "Something You Do", and "How You Are"

SECURE
TECHNOLOGY
ALLIANCE

Relative Comparison of Biometric Reader Costs

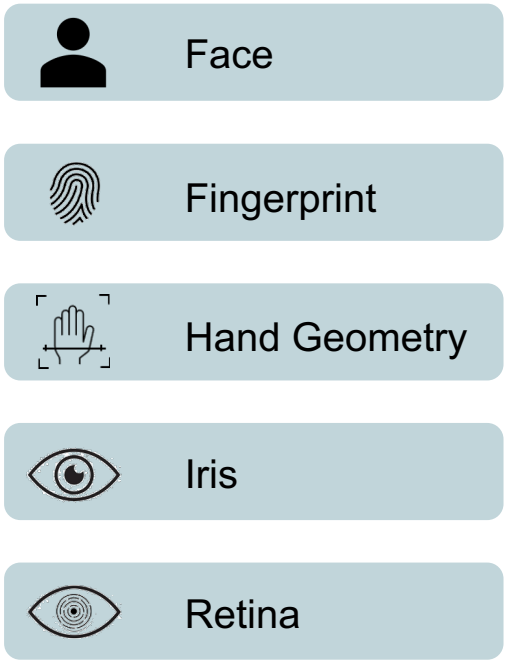


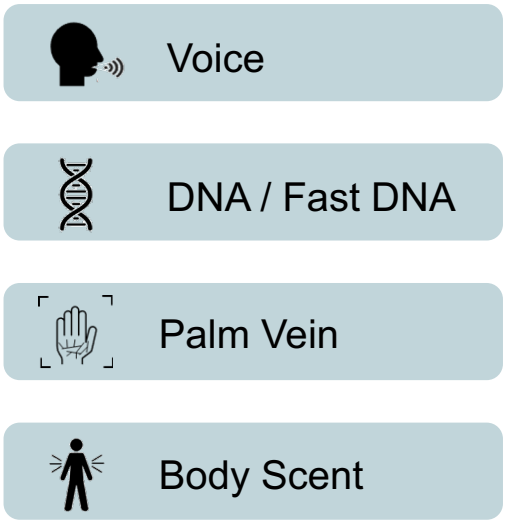
Cost Factors

- Reader pricing
- Implementation costs
- Deployment base
- Liveliness Detection

SECURE TECHNOLOGY ALLIANCE

Biometric Authentication Mode Examples





SECURE TECHNOLOGY ALLIANCE

SECURE
TECHNOLOGY
ALLIANCE

Developing Apps for Access Control on Mobile Devices

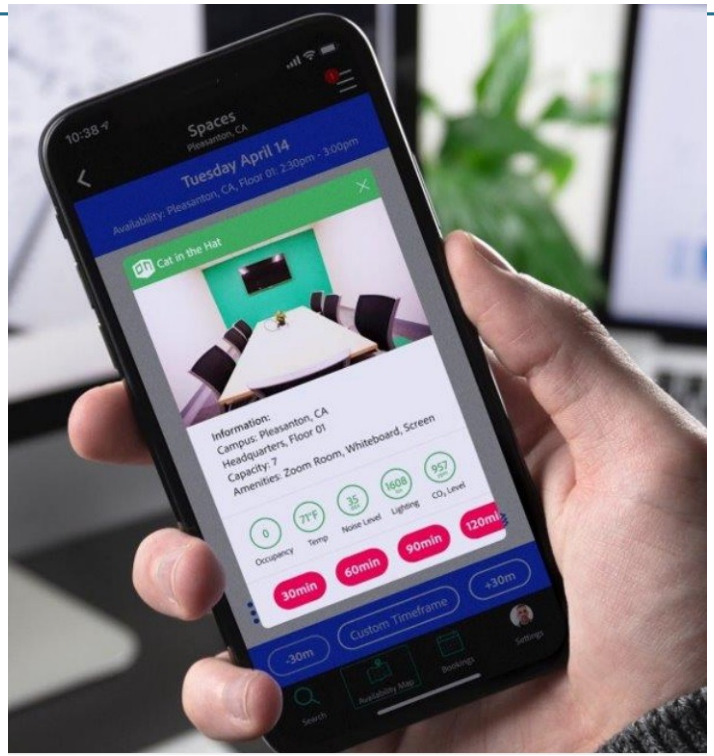
Mobile devices use in access control

Way finder app to reserve an office, or meeting room space

SECURE TECHNOLOGY ALLIANCE

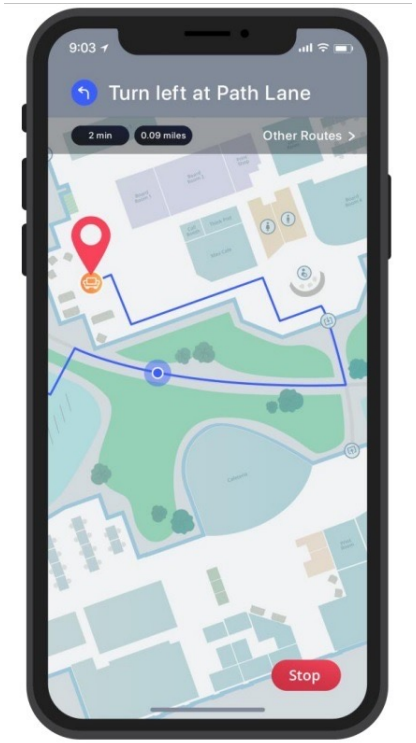
Mobile devices use in access control

Way finder app to reserve an office, or meeting room space



SECURE TECHNOLOGY ALLIANCE

Mobile devices use in access control

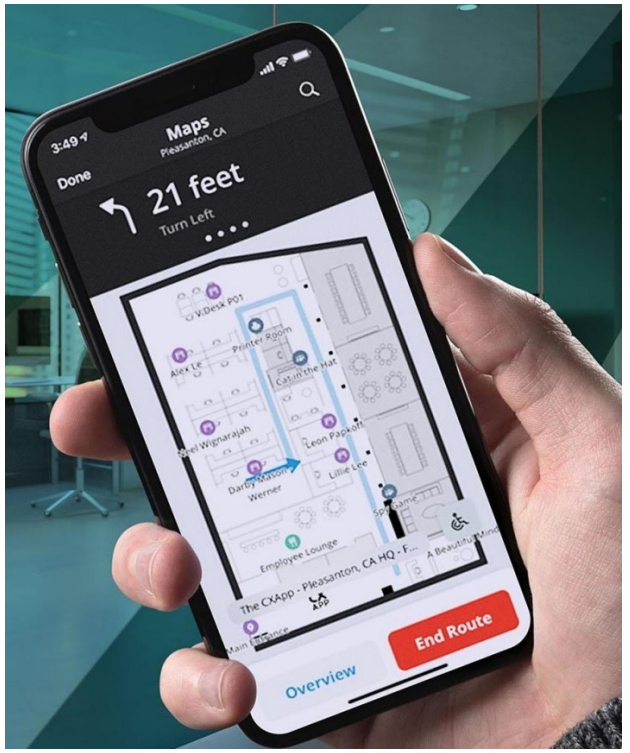


Way finder app show path to correct building

SECURE TECHNOLOGY ALLIANCE

Mobile devices use in access control

Way finder app show path to correct desk inside correct building



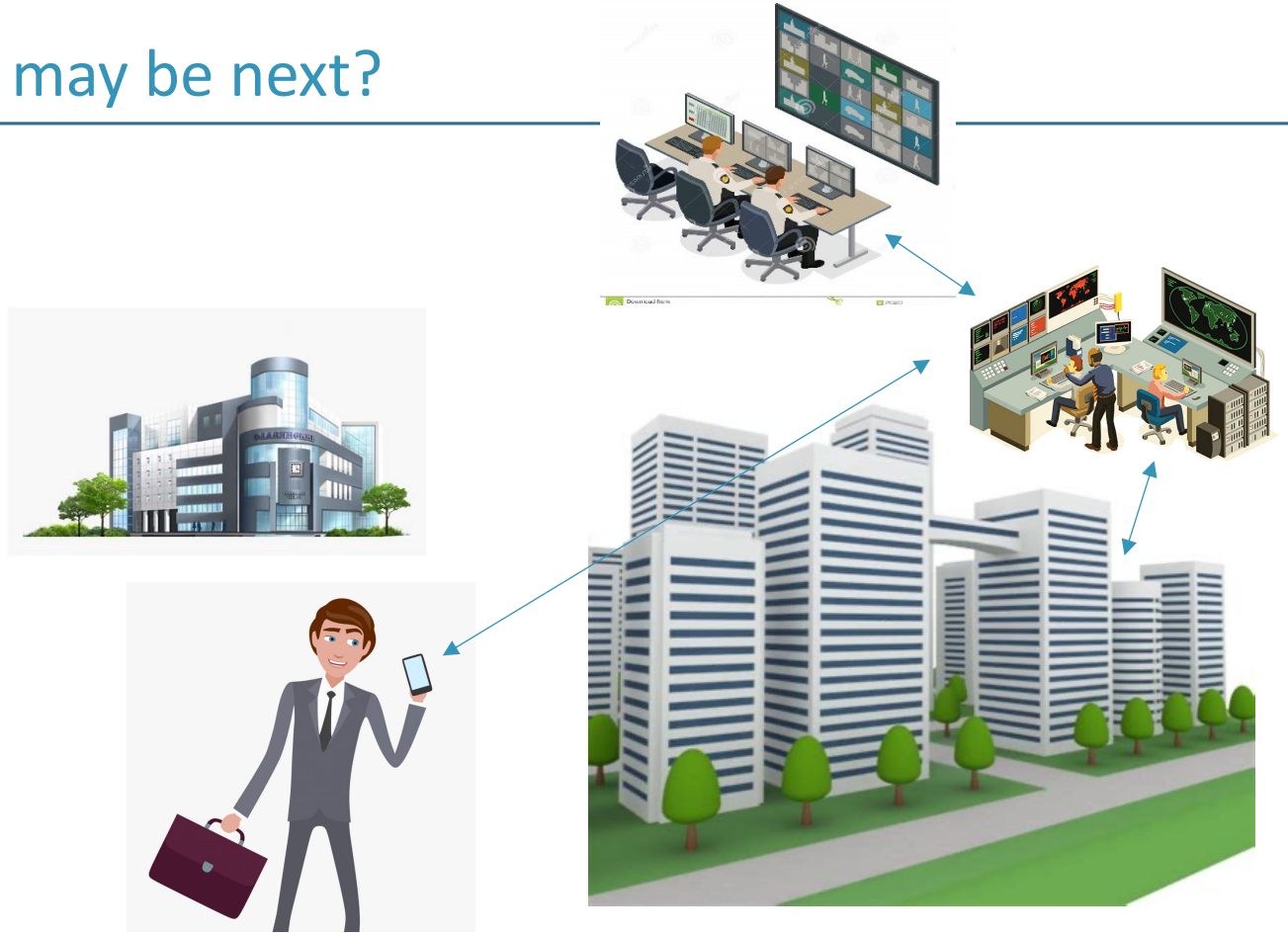
SECURE TECHNOLOGY ALLIANCE

What if:

What if:

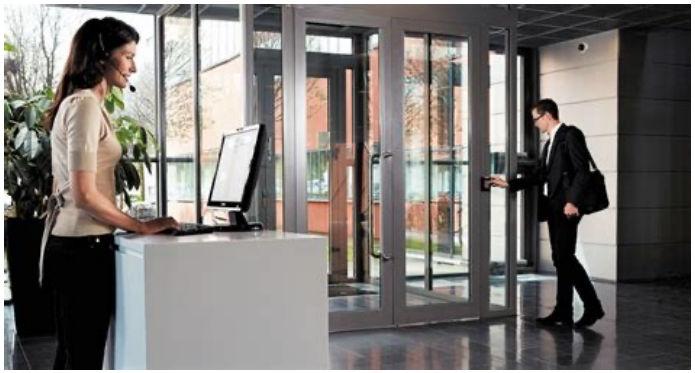
- The Office Reservation system was integrated with a Way Finder
- The Way Finder was integrated with a PACS
- The host site could send credential to the visitor phone
- The phone credential could be provisioned in the PACS to relevant access control points

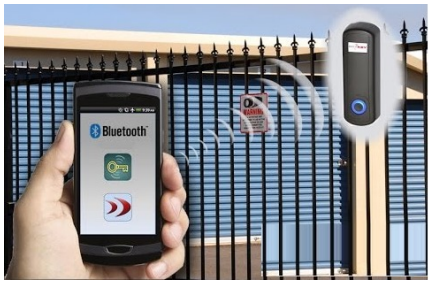
What may be next?

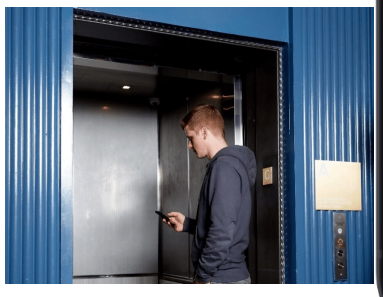


Way finder app show path to correct VA HQ building

What may be next?



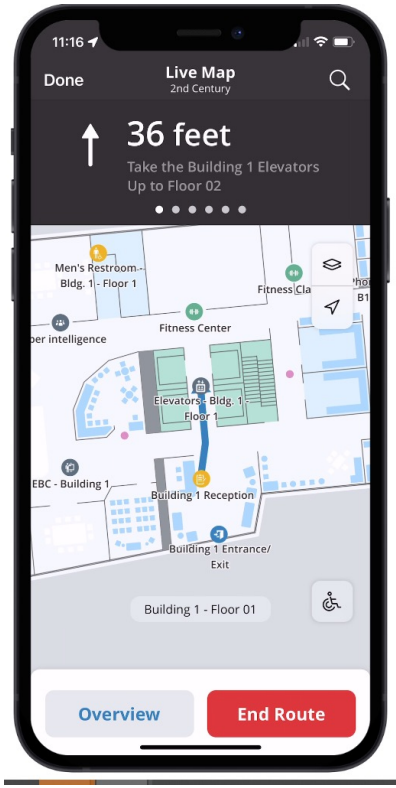




Way finder app show path from parking to correct building

SECURE TECHNOLOGY ALLIANCE

What may be next?



SECURE TECHNOLOGY ALLIANCE

What may be next

Summary

- Mobile phones are universally accepted
- Increasing processing power, memory capacity
- Rapidly increasing Apps for all mobile device OS
- We are beginning to see developers taking advantage of the powerful platforms mobile devices offer that are beyond the traditional multifactor model of Something you Have, Know and Are.
- Offer convenience and expedience.
- Be aware of any Privacy law that may be applicable.
- Anyone else who may want to take a guess, or make a suggestion for what may be next?

THANK YOU

SECURE TECHNOLOGY ALLIANCE

This is a 'big thought' slide – place for a provocative quote, a theme for a section or whole presentation. Mainly useful for point in a presentation when you will be talking over the slide for a long period of time and so something attractive but visually a little quiet is on screen.

Copyright 2021 IDTP

SECURE
TECHNOLOGY
ALLIANCE

Q&A

Contact Information

- Jason Bohrer, jbohrer@securetechalliance.org
- Mark Dale, mdale@xtec.com
- Roger Roehr, rroehr@istonline.com
- Lars Suneborn, lsuneborn@idtp.com