SECURE TECHNOLOGY ALLIANCE

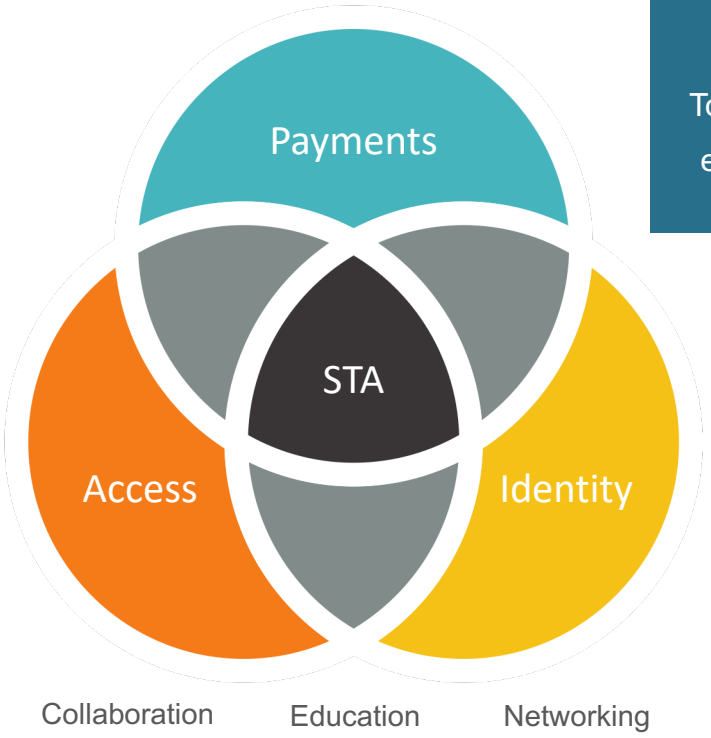
# The Future of Access Control (Part 2)

SECURE TECHNOLOGY ALLIANCE

# The Future of Access Control (Part 2)

The webinar will start momentarily.

# 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**

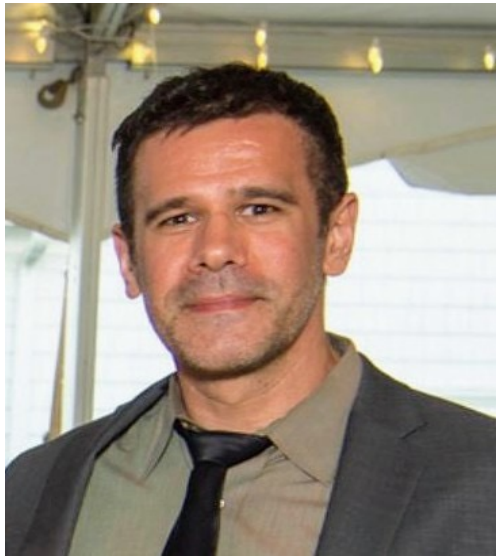
- Gerry Smith, NIST Certified TECHNICAL EXPERT for cryptographic and security technology, Sr. Consultant, High Assurance Identity Verification Solutions, ID Technology Partners
- David Ferraiolo, Computer Sciences Team Lead, National Institute of Standards and Technology
- Mark Dale, Sr. Systems Engineer – Mobility, Xtec
- Roger Roehr, Director, Identity Management - Integrated Security Technologies – ist
- Steve Rogers, CSCIP, President, IQ Devices, Inc.
- William Windsor, Sr. Director, ICAM Solutions, Public Security, Federal, Idemia

# Panelist – John Jacob

IDEMIA
augmented identity

- Executive Director (Federal Identity Solutions) – IDEMIA
- Impressive 30-year professional career in consulting, business development and management of computer related physical and logical security solutions
- Widely recognized as SME expert in the following:
  - High assurance credentials
  - ICAM, FICAM and cyber security
  - Expertise on ISO/ IEC and NIST published guidelines (mDL, ISO 18013, HSPD12 and FIPS 201-3)
- Key Council Member for the Secure Technology Alliance (Identity and Access Control Councils)

# Panelist – Colin Doniger



Homeland Security

- Program Lead - Enterprise PACS Modernization - DHS
- Recognized as a PACS SME in the commercial and federal markets
- Early career roles:
  - Began his security career as an MP in the US Army in 2000
  - Five years supporting federal contracts as an electronic security technician
- Joined DHS in 2009 where he held various roles; eventually served as Chief of the Physical Security Branch.
- BS in Organizational Security (University of Phoenix)
- Certifications
  - ASIS PSP
  - STA CSEIP
  - NSCA Electronic Systems Technician (Level 2)

Remarks by the speaker do not necessarily represent the views of DHS or the United States Government

SECURE TECHNOLOGY ALLIANCE

# 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-Present)
- 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

# Identity Management

A Discussion on Centralized vs. Decentralized Identity Credentials in the Mobile Identity world

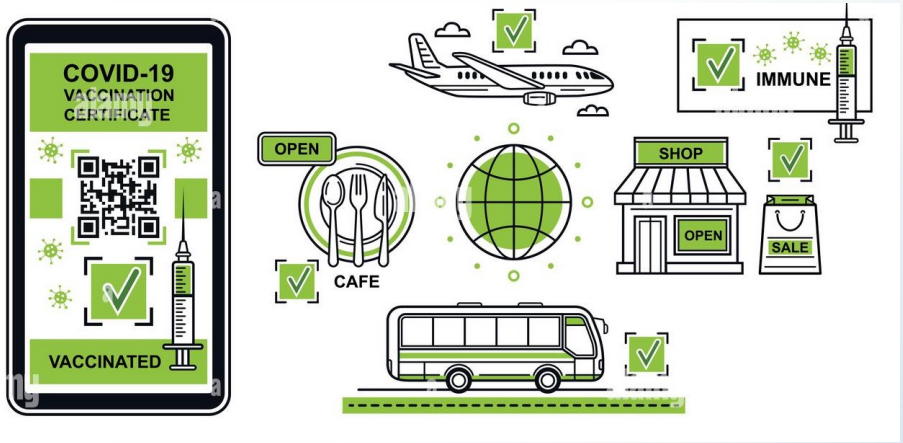
John Jacob

# Agenda

1. Overview of Centralized vs. Decentralized Mobile Credentials
2. Evaluation of Centralized / Standardized based Credentials
3. Discussion on Decentralized Identities or Verified Credentials
4. Consider Leveraging Both:
   A. Mobile DL (18013-5) Standards based
   B. Verified Credentials or Decentralized Identities DIDs using DLTs

# Identity Management
## Centralized vs. Decentralized Mobile Phone IDs

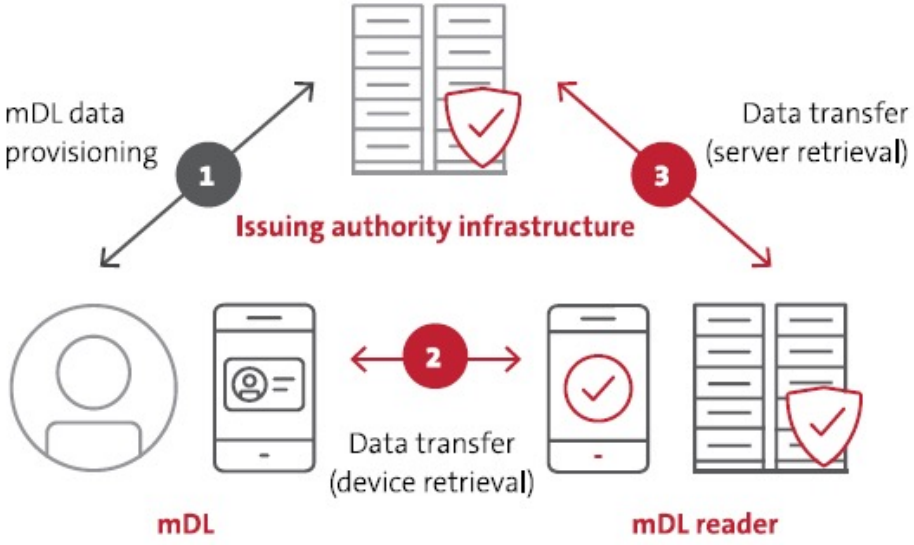
- **Identity Credentials**

# Centralized Identity Management – The Concept


- Digital Certs –which proves Identity of an entity and binds it to a public key
- PKI – System used to manage keys and Certificates
- CA – Trusted 3rd party – issues a signed certificate to an entity after verifying its identity
- Overall, provides a secure environment for online txns and e-commerce

# Example: Centralized Identity Management – State System of Record (SOR)




- Issuing authority (such as DMV)
- mDL – a digital representation of an individuals DL characteristics
- mDL Reader – Verifier that can interact with the mDL for attribute exchange as well as the issuing authority if required.

# Centralized Identity Management – FPKI and KYC

**Pros –**

- **Mature -** Many years of experience and implementation
  - The Federal PKI has shown to be a successful implementation for the HSPD2 PIV/CAC cards and digital representations of them known as derived credentials using centralized CA
  - PKI is also used for securing web sites, devices, and IOT

**Challenges -**

- Once compromised, all identities in the database are potentially exposed.
- Expensive to implement, manage and scale/expand
- Repetitive Registrations/KYC and shared personal information

# Decentralized Identity Management – The Concept

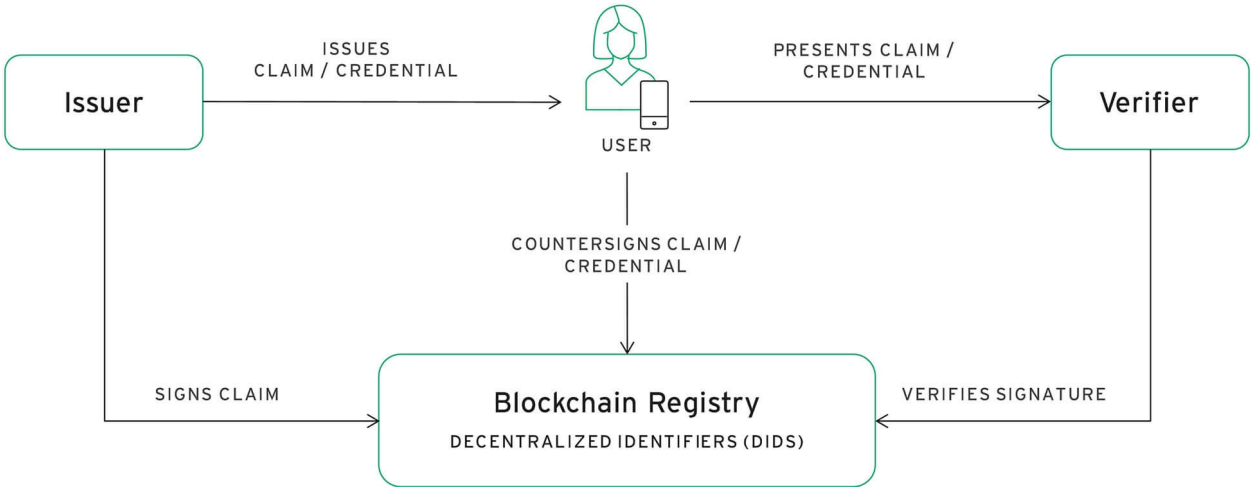
**Issuer**
Issue credentials

**User**
Stores credential in digital wallet

**Verifier**
Receives credential from user & verifies issuer via blockchain

**Registry**
Stores issuers & users identities on the blockchain

**Decentralized Identifier**
Unique identifier to prove identity ownership




- Digital Certs – continue to play a role, but in a distributed fashion using a Digital Ledger such a Blockchain, Ethereum or Holochain all using slightly different distributed ID management and authentication methodologies

# Examples of VC Use cases

# Leveraging the Best of Both Platforms

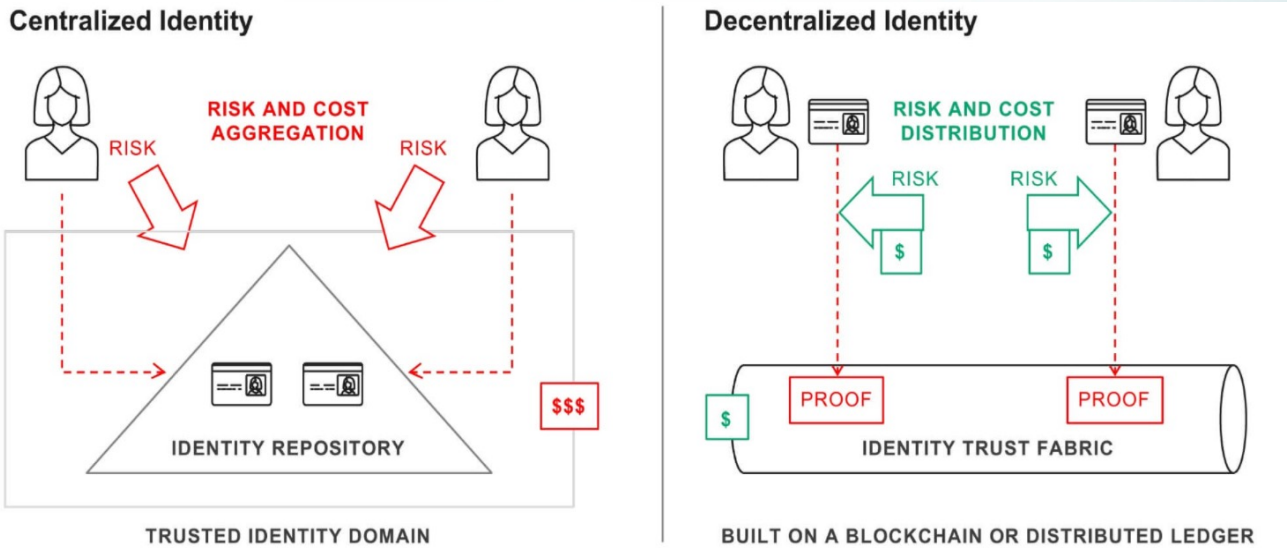



**Figure 6.** Decentralized identity systems shift the risk of data loss away from large central stores. Any single security breach will yield a much smaller haul of PII, thus changing the economics of a break-in attempt. Source: Gartner, 2017

SECURE TECHNOLOGY ALLIANCE

*“ISO/IEC 18013-5 can be a important road to a standards-based implementation of Verifiable Credentials”*

-- Underwriter Labs

SECURE TECHNOLOGY ALLIANCE

Thank you.

John Jacob,  Idemia.
John.Jacob@us.idemia.com

SECURE TECHNOLOGY ALLIANCE

# Information Sharing

Colin Doniger,  CSEIP, Department of Homeland Security

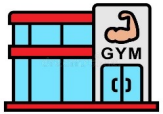
# Session 4 – Information Sharing Services



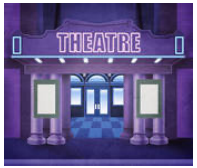
# Use Case Examples and Sharing

Where could we expect such environments to exists

- Medical Appointments
- Daycare Centers
- Entertainment Venues
  - Concert Halls
  - Theaters
  - Sports Stadiums / Arenas
- Hotel check in / check out
- Membership Driven Businesses
  - Fitness Centers
- Visitor Registration / Facility Check in
- Voter Registration / Balloting Processes
- Convenience Stores






*The key to operationalizing these examples are made possible through pre-registration processes, whereas the functional entity could perform ordinary vetting practices as a back-office function.*

Opportunities for shared services and infrastructures

- Gain efficiency through sharing information and infrastructures
  - Health based use cases (HIPPA constraints)
  - Entertainment use cases (season ticket holders, ecash / wallets)
  - Guest based services (hotel, membership)
  - Access control use cases (facility access, visitor registration)

# Common Attributes

What attributes might be included for identity and credential information

Core attributes

- Name (first, middle (if applicable), last name, prefix / suffix)
- Address (home / work)
- Association / affiliation (industry, government, private)
- Email address
- Home phone
- Mobile phone

Credential attributes

- Card / device / token type (presented for usage)
- PKI certificates (credential specific – PIVAuth & CAKAuth (PIV), OpenID)
- Authentication factor
- Registration date
- Registration entity
- Validity period

# Information Exchange

Today there are limited means to perform information exchange, leaving initial use cases bound to manually or individualized registration practices, the opportunity create such an exchange could be seen as a Greenfield / territory that remains untapped.

Considerations for building and growing it …….

- Driving factors
  - Use case specific data
  - Data protection
  - Secure transmission / exchange
  - Reliability
  - Convenience
  - Data accuracy
  - Ease of use
  - Incentives
- Diversity
  - Use of common data working for more than a single use case
  - Ease of enrollment into entity programs
  - Simple interface for opting in / out

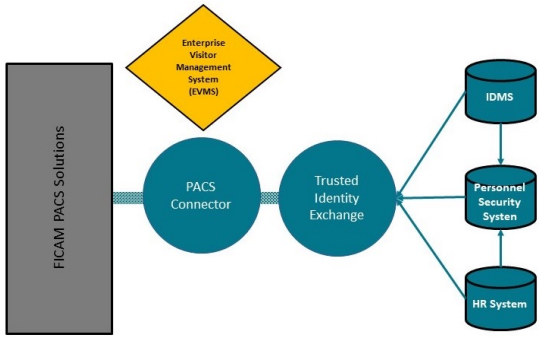
How it might work …….

- Mobile phone app – downloadable via common application stores
- Token readers could be positioned to read card / keyfobs / etc. type tokens
- Businesses could use a front page approach when connecting to wireless networks within the place of business to opt-in

# Federal Government Information Exchange

The federal government has developed a solution called “PACS Connector”, while this solution is designed specifically for access control needs, the theory could be adopted into shared services models in many different vertical markets such as health care, membership or access control

- The PACS Connector Application Programming Interface (API) bridges the gap between the trusted data source and the consuming PACS.
- It enhances interoperability through use of standard data elements.
- The API allows for integration at the product level.
- It enables data transfer without requiring physical presence to enroll into a local PACS
- Adds a layer of assurance through updated data being readily available aiding the deprovisioning process when the PIV certificates is revoked – in effect providing our Components the ability to automate the removal of the cardholder’s access in a near real time fashion



# What's the potential impact

Current FICAM PACS processes

- Registration & Provisioning to a local PACS requires each PIV Card to be enrolled in a "one off" manner
- Each PIV is authenticated during the card read process
- System solutions require the cardholder to enter their respective PIV Personal Identification Number (PIN) to read the PIV Authentication certificate
- Read information is bound to identity or cardholder record in the PACS, incorporating basic info such as name, card expiration, certificate info.
- PACS Administrator grants privilege based on local policies.

.....next customer, please.....

PACS Connector process

- Secure connection is established with Trusted Identity Exchange, TIE.
- TIE provides an agreed upon set of attributes to facilitate PACS registration for each cardholder in the system
  - Subsequent calls to TIE for updates to existing and new cardholder information
- Certificate authentication is performed during registration using the public key (no need for PIN entry)
- Registered users are ready for Provisioning as per local policies.

# How do we ensure “freshness” of data

## Who owns the data

- How is the info / attribute updated?
- How does updated data get disseminated?

## Risk-based factors

- Each vertical market may have different “views” on risks
- Common data may need to be minimized to remove theoretical risks

## What rules need to be applied?

- Establish rules for dormant data
  - Establish time / date-based dormancy rules.
  - 90 days or less

## Create a mechanism / portal for individual data management

- Self service driven
- Offer remove / cancellation feature
- Provide an updating capability
- Subscription management

# Thank you!

Colin Doniger

Colin.Doniger@hq.dhs.gov

SECURE TECHNOLOGY ALLIANCE

# Attribute Based Access Control

## A Discussion on future Physical and Logical Access Provisioning using Enterprise Attributes & Local Policies

Lars R. Suneborn, CSCIP/G, CSEIP , Sr. Consultant, Identification Technology Partners

# Identities & attributes – Center of authorization



# Attributes and Privileges: PACS & LACS combined

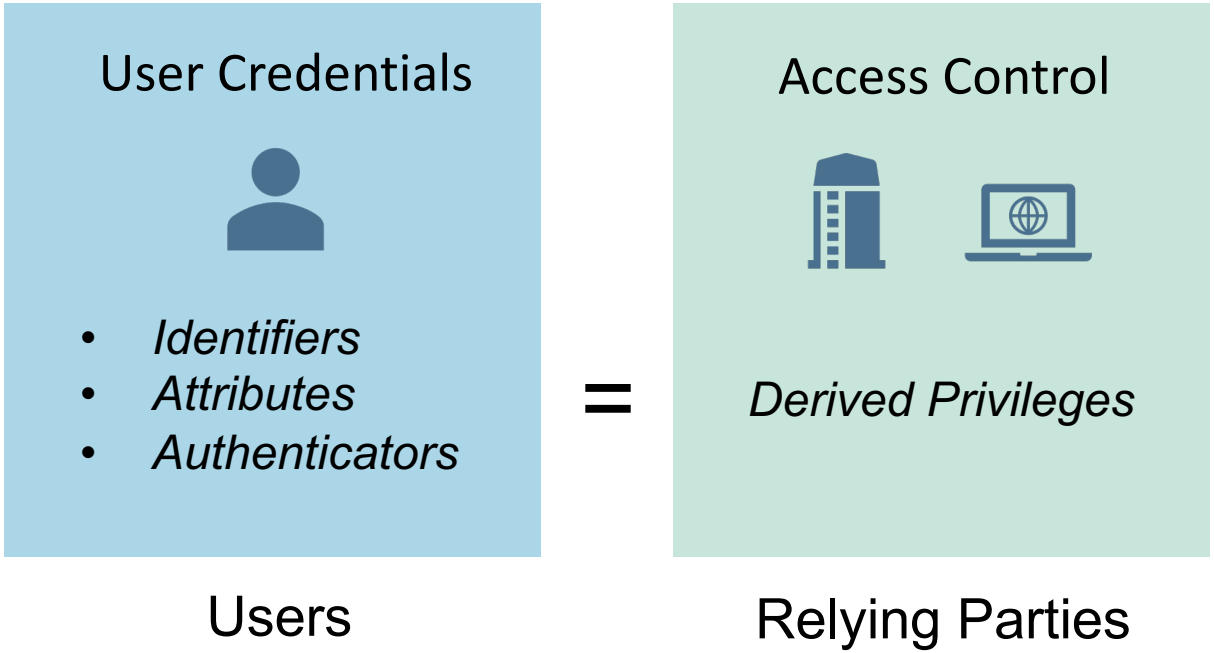
Assigning proper access privileges (Authorization) often become a complex task, especially in large sites where there may be several hundred, or thousand of access control readers and groups of people. Many members of a group often need some exception to include additional, or fewer access points.

Logical provisioning can become just as complex when considering what files and records are restricted to what level and determine who can access, edit, or create records. Location at time of access request also impact what files may be accessed.

Provisioning individuals who travels between multiple large Corporate or Agency locations add significant complexities to the problem

What if, in addition to a basic employee data record, a separate set of Enterprise wide attribute tables could be created and distributed to each site of an enterprise. As an employee visit other agency locations, the basic employee record could be linked to the specific attribute table at each site. Each site would have their own locally defined privileges instantly provisioned . This could make provisioning privileges more precise as well as a much less complex task

# User Credentials and Privileges



# Identity and attributes for access control purposes

Definition of an **Attribute:**

"*a quality or feature regarded as a characteristic* or inherent part of someone or something"

**An Attribute** is often a justification for Authorization to enjoy a Privilege

**Authorization**: Assigning privilege to access specific resources

We will take a look at a generic framework to distribute identity and attributes to be provisioned as per site specific (Local Environment) policy for two different organizations. Chemical engineering and Medical center.

# Identity and attributes for access control purposes

Each individual has an Attribute that is associated to a site specific privilege, making the process of assigning physical and logical privileges dependent on local environment policies for each group or individual.

Attributes may be accumulated, i.e. being an employee at an organization, being is a chemical engineer and have a PhD and have a security clearance, but no safety training. Both access and visitor Escort privileges could depend on current Safety Training, an attribute with conditional privilege(s)

The individual accumulation of attributes can become quite complex.

An automated Attribute based policy processor could accomplish this efficiently to individuals, of entire group of individuals.

# Identity record

## ANATA Attribute Table: Attributes for NATional Access

In his company employee database, a portion of Bob's Identity record includes his full name, DoB and a Universally Unique Identifier, UUID.

| No. | Attribute Name | Attribute Value |
|---|---|---|
| 01 | First Name | Bob |
| 02 | Last Name | Bigbang |
| 03 | DoB | July 04 1990 |
| 04 | Unique Identifier | B7aab8f-2b40-4573-a604-221b9e4068d5 |

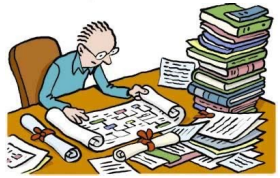
# Identity and attributes for access control purposes

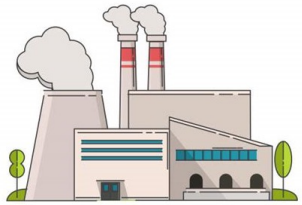
Attribute is a specific accreditation that may be eligible to a specific privilege. Examples:

- Being an employee of an organization may be associated with basic access privileges at each of his organization sites.
- Safety training may be required to access specific areas & escort visitors
- A Security Clearance of x level may be associated with physical & logic access privileges.
- Inside the Secure area of HQ, full access to research data

# Identity record and attributes for access control purposes

| No. | Attribute Name | Attribute Value |
|---|---|---|
| 01 | First Name | Bob |
| 02 | Last Name | Bigbang |
| 03 | DoB | July 04 1990 |
| 04 | Unique Identifier | B7aab8f-2b40-4573-a604-221b9e4068d5 |
| 05 | Engineer PhD | Chemical |
| 06 | Security Clearance | Q |
| 07 | Safety Training Expires | Dec 31, 2021 |
| 08 | Escort Privilege | Yes with current Safety Training |





# ANATA Attributes Table

Let us take a look  at the same table framework in a different type of organization

Alice work in an Health Care organization, Health & Healthy, with locations in several cities and states.

# Identity record + attributes

A portion of Alice's Identity record includes Alices full name, DoB and a Universally Unique Identifier, UUID.

These details may be linked with a local set of specific attributes that applies to her both as an individual and as a part of a groups of individuals.

| | Attribute Name | Attribute Value |
|---|---|---|
| 01 | First Name | Alice |
| 02 | Last Name | Anderson |
| 03 | DoB | July 04, 1980 |
| 04 | Unique Identifier | a3c85b8f-2b40-4573-a604-221b9e4068d5 |

# Identity record + attributes

A local attribute table that applies to groups of individuals.

Attribute that relate to a function such as Dr. This Attribute can then be combined with other attributes that are also defined locally, such a Oncology.

Example of Alice's  Dr. attributes within her licensed regions

| | Attribute Name | Attribute Value |
|---|---|---|
| 05 | Medical | Dr. |
| 06 | Category | Oncology |
| 07 | Specialty | Lung & Throat |
| 08 | Radiation Cert. Expiration Date | Dec.31 2022 |
| 09 | Region | MD., VA. |
| 10 | License Expiration Date | June 01, 2023 |
| 11 | Staff | Department Administrator |
| 12 | | |

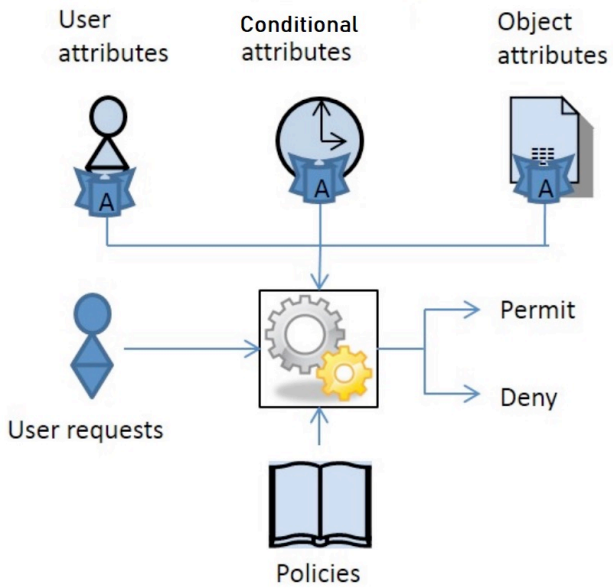
# Identity record + attributes

Alices initial Identity record may be linked with a local attribute table that applies to groups of individuals. Each attribute Description is associated with a locally defined Physical and Logical privileges. Example of Alice's Dr. attributes within her licensed region

| No. | Attribute Name | Attribute Value |
|---|---|---|
| 01 | First Name | Alice |
| 02 | Last Name | Anderson |
| 03 | DoB | July 04, 1980 |
| 04 | Unique Identifier | a3c85b8f-2b40-4573-a604-221b9e4068d5 |
| 05 | Medical | Dr |
| 06 | Specialty | Oncology |
| 07 | License Expiration Date | June 01, 2023 |
| 08 | Specialty | Lung & Throat |
| 09 | Radiation Cert. Expiration Date | Dec 31, 2022 |
| 10 | Region | VA. MD. |
| 11 | Staff | Administrator |
| 12 | | |
| 13 | | |

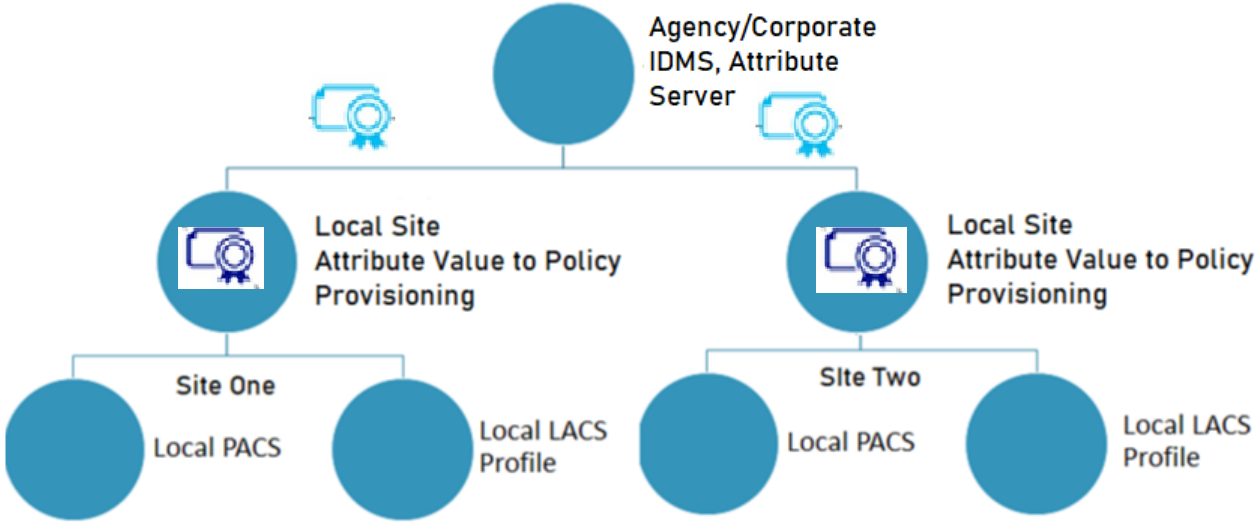
# Attribute Value connect with locally defined privilege

Employee Attribute Value connect with locally defined privilege as per site policy for each attribute value for the requested resource.



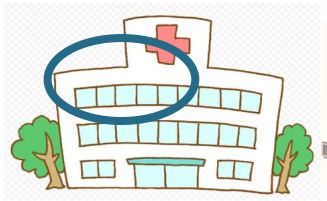
# Attribute Value connect with local defined privilege

Employee identity and Attribute Value data may be shared using a method such as an Enterprise Trusted Identity Exchange, described in the previous session to connect with locally defined privilege as per site policy for each attribute value.

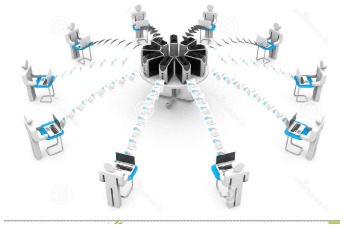


# Dr. Alice local PACS & LACS Attribute based Privileges

PACS privileges:
- Employee access to VA. & MD. centers
- Dr. Oncology, Lung & Throat
  Physical access to special areas
- In VA., M.D.'s enjoy Parking Privileges



LACS Privileges:
- At each center, access is restricted to Oncology records of her staff's patients. See, create, edit, save, share, write prescriptions, and print their patients records
- Staff Administrator, privileged account with privileges to create other Oncology accounts for her staff



| No. | Attribute Name | Attribute Value |
|---|---|---|
| 01 | First Name | Bob |
| 02 | Last Name | Bigbang |
| 03 | DoB | July 04 1990 |
| 04 | Unique Identifier | B7aab8f-2b40-4573-a604-221b9e4068d5 |

| No. | Attribute Name | Attribute Value |
|---|---|---|
| 05 | | |
| 06 | | |
| 07 | | |
| 08 | | |
| 09 | | |
| 10 | | |
| 11 | | |
| 12 | | |

| No. | Attribute Name | Attribute Value |
|---|---|---|
| 05 | | |
| 06 | | |
| 07 | | |
| 08 | | |
| 09 | | |
| 10 | | |
| 11 | | |
| 12 | | |
| 13 | | |
| 14 | | |
| 15 | | |

| No. | Attribute Name | Attribute Value |
|---|---|---|
| 01 | First Name | Bob |
| 02 | Last Name | Bigbang |
| 03 | DoB | July 04 1990 |
| 04 | Unique Identifier | B7aab8f-2b40-4573-a604-221b9e4068d5 |

| No. | Attribute Name | Attribute Value |
|---|---|---|
| 05 | | |
| 06 | | |
| 07 | | |
| 08 | | |
| 09 | | |
| 10 | | |
| 11 | | |
| 12 | | |

| No. | Attribute Name | Attribute Value |
|---|---|---|
| 05 | Medical | |
| 06 | Specialty | |
| 07 | License Expiration Date | |
| 08 | Specialty | |
| 09 | Radiation Cert. Expiration Date | |
| 10 | Region | |
| 11 | Staff | |
| 12 | | |
| 13 | | |
| 14 | | |
| 15 | | |

| No. | Attribute Name | Attribute Value |
|---|---|---|
| 01 | First Name | Bob |
| 02 | Last Name | Bigbang |
| 03 | DoB | July 04 1990 |
| 04 | Unique Identifier | B7aab8f-2b40-4573-a604-221b9e4068d5 |

| No. | Attribute Name | Attribute Value |
|---|---|---|
| 05 | | |
| 06 | | |
| 07 | | |
| 08 | | |
| 09 | | |
| 10 | | |
| 11 | | |
| 12 | | |

| No. | Attribute Name | Attribute Value |
|---|---|---|
| 05 | Medical | Dr |
| 06 | Specialty | Oncology |
| 07 | License Expiration Date | June 01, 2023 |
| 08 | Specialty | Lung & Throat |
| 09 | Radiation Cert. Expiration Date | Dec 31, 2022 |
| 10 | Region | VA. MD. |
| 11 | Staff | Administrator |
| 12 | | |
| 13 | | |
| 14 | | |
| 15 | | |

| No. | Attribute Name | Attribute Value |
|---|---|---|
| 01 | First Name | Bob |
| 02 | Last Name | Bigbang |
| 03 | DoB | July 04 1990 |
| 04 | Unique Identifier | B7aab8f-2b40-4573-a604-221b9e4068d5 |

| No. | Attribute Name | Attribute Value |
|---|---|---|
| 05 | Engineer PhD | Chemical |
| 06 | Security Clearance | Q |
| 07 | Safety Training Expires | Dec 31, 2021 |
| 08 | Escort Privilege | Yes with current Safety Training |
| 09 | | |
| 10 | | |
| 11 | | |
| 12 | | |

| No. | Attribute Name | Attribute Value |
|---|---|---|
| 05 | Medical | Dr |
| 06 | Specialty | Oncology |
| 07 | License Expiration Date | June 01, 2023 |
| 08 | Specialty | Lung & Throat |
| 09 | Radiation Cert. Expiration Date | Dec 31, 2022 |
| 10 | Region | VA. MD. |
| 11 | Staff | Administrator |
| 12 | | |
| 13 | | |
| 14 | | |
| 15 | | |

# Information Sharing & Summary

In these conceptual examples of generic set of EXCEL type tables to cerate Corporate Attribute tables and Values to simplify the Authorization process.

- Basic Identity records
- Additional Attribute Tables with corporate Attribute Names and Values
- Define PACS “Door Groups” and other PACS policy based access details for each Attribute Value
- Define LACS Profiles (Accounts) with detailed Privileges for each relevant Attribute Value
- May be extended to visitors from other corporations
- XML schemas and location based attribute/policy authorization documentation available from NIST
- Benefit: Greatly simplified Provisioning Process

# RBAC and ABAC for access control purposes (Gerry)

Further Reading:

**National Institute of Standards and Technology (NIST)**

NIST SP 800-178 “A Comparison of Attribute Based Access (ABAC) Standards and Data Services”

**Excellent White Paper (Ferraiolo)**

“On the Unification of Access Control and Data Services“
https://csrc.nist.rip/pm/documents/ir2014_ferraiolo_final.pdf

**National Standards Efforts**

ANSI/INCITS 499-2013/2018 Next Generation Access Control (NGAC) Functional Architecture (FA)

ANSI/INCITS 565-2020 – Information technology – Next Generation Access Control (NGAC)

**Academia (Syracuse) for RBAC**

tmp/RBAC.dvi (syr.edu) OR
https://web.ecs.syr.edu/~wedu/Teaching/cis643/LectureNotes_New/RBAC.pdf

# Thank you!

Lars Suneborn, CSCIP/G, CSEIP.
Lsuneborn@idtp.com

# Q/A Session

Contact information:

John Jacob, john.jacob@us.idemia.com

Colin Doniger, Colin.Doniger@hq.dhs.gov

Lars Suneborn, Lsuneborn@idtp.com

SECURE
TECHNOLOGY
ALLIANCE

# Thank You For Attending!