Virtual CONSULT

Presented By

security specifiers®

SIA
SECURITY INDUSTRY ASSOCIATION

securityspecifiers
CONSULT 2020
VIRTUAL TECHNICAL SECURITY SYMPOSIUM

securityspecifiers

CONSULT 2020

VIRTUAL TECHNICAL SECURITY SYMPOSIUM

Sponsors

Diamond Sponsor

Altronix®

Gold Sponsors

ACRE®

OPEN OPTIONS RS Technologies

VANDERBILT

intel®

LENEL:S2

SALIENT

Approvals

Bicsi®
CONTINUING EDUCATION
CREDIT PROVIDER

6 CEC's

ASIS INTERNATIONAL | Preferred CPE Provider

6 CPE's

Send Certificate Requests to Ray Coulombe
ray@securityspecifiers.com

Delivering Secure Identity

Sponsored By

ALLEGION™

securityspecifiers
CONSULT 2020
VIRTUAL TECHNICAL SECURITY SYMPOSIUM

Identification, Authentication, Authorization

- Steps in the access control process
- Who you are?
- What are you allowed to do?
- Levels of assurance (trust)
- Going to look at primarily the first two (identification and authentication)

Moderator

Sal D’Agostino
CEO, IDmachines

Panelists

Consuelo Bangs
Sr. Program Manager
IDEMIA

Hugo Wendling
CEO, WaveLynx

Pierre Bourgeix
CTO & Founder
ESI Convergent

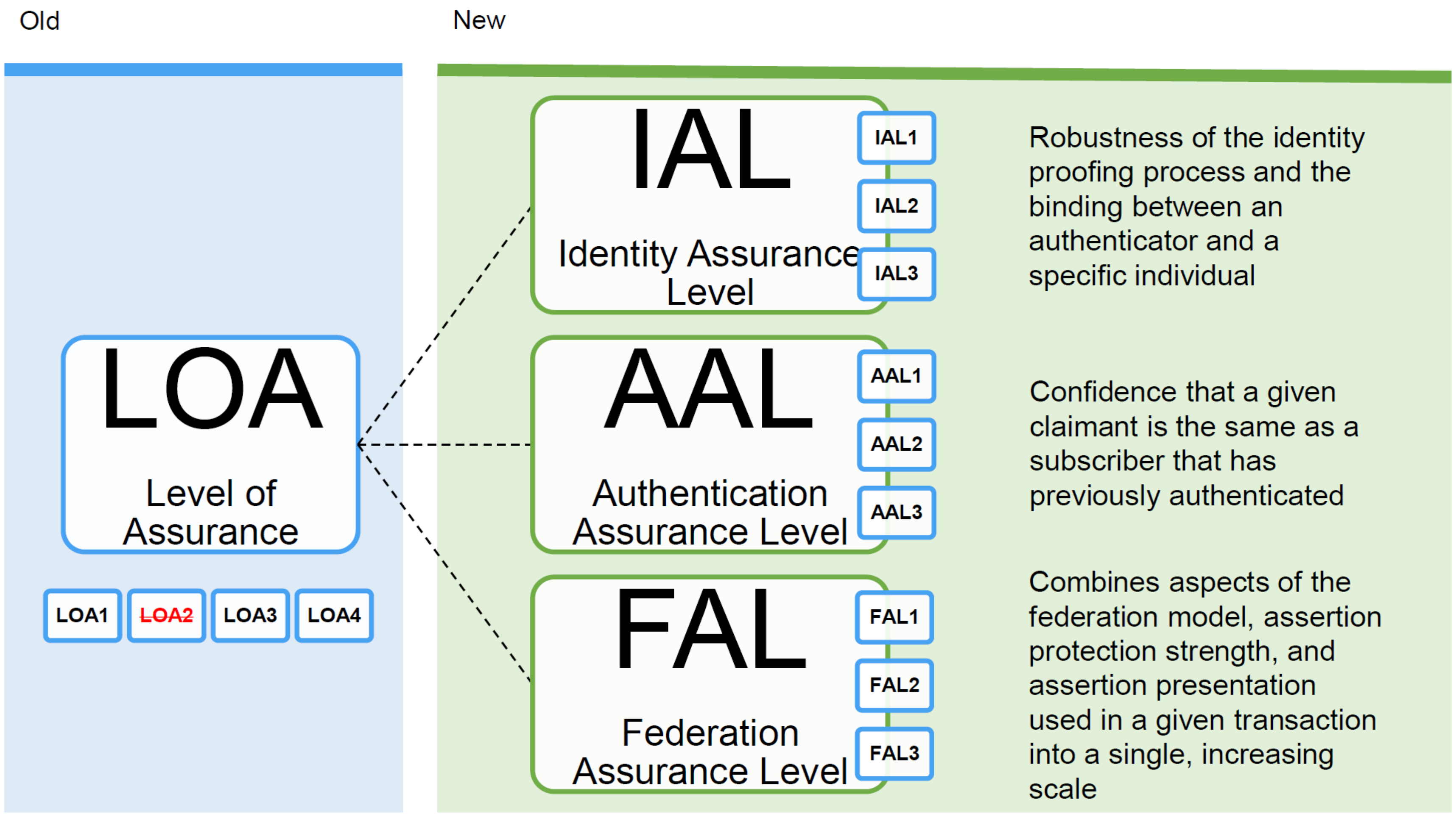
David York
VP & CISO
Allegion

What is secure identity?

- Something you would trust because of …
  - Identity assurance (IAL)
  - Authentication assurance (AAL)
  - Identifier uniqueness and control
  - Strength of credentials/tokens
  - Binding entities and credentials (IAL and AAL)
  - Ability to control identity and credential lifecycle (customer and individuals)
  - What does a specification include?

How do you specify a secure identity?

NIST 2017



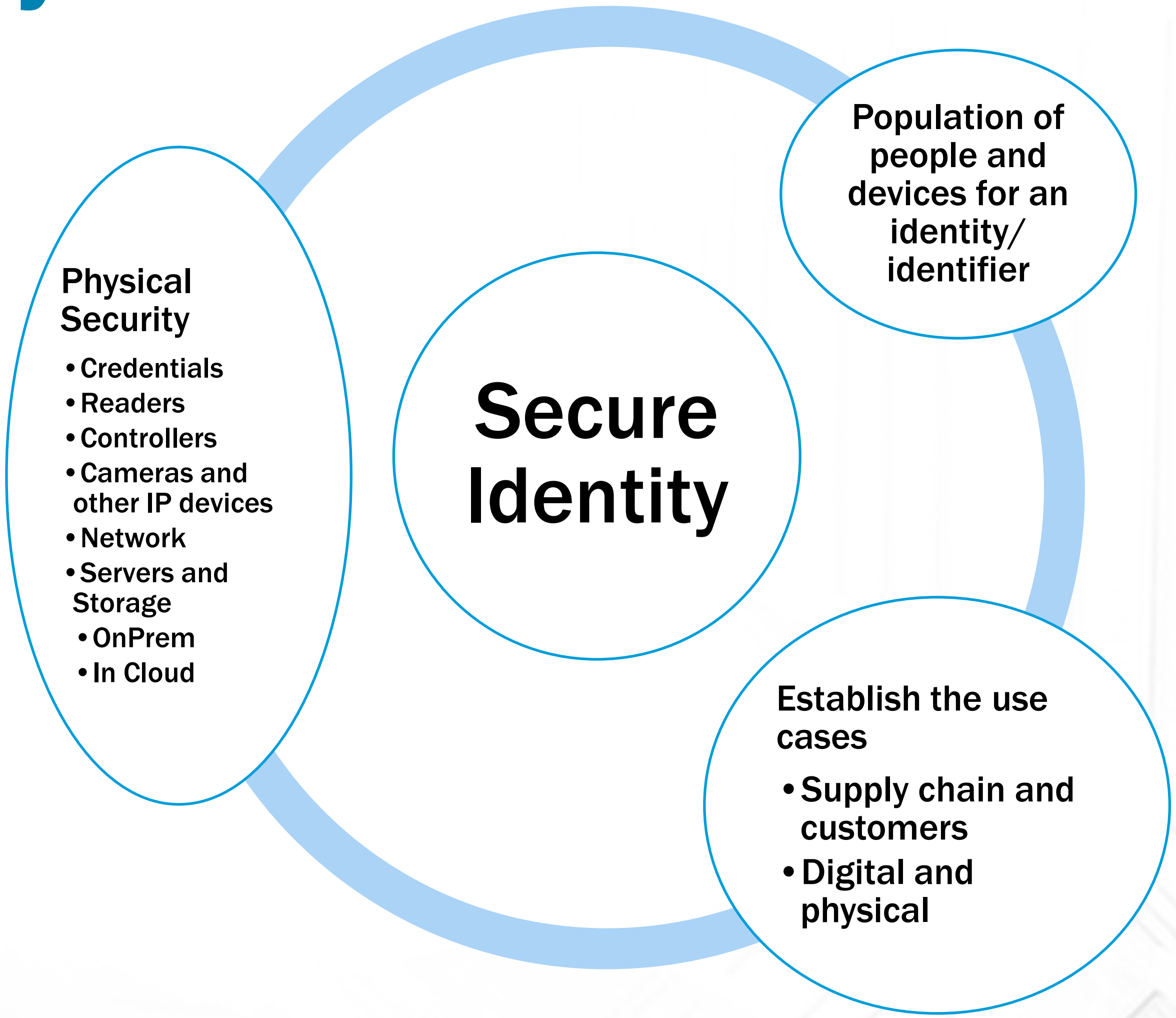
Robustness of the identity proofing process and the binding between an authenticator and a specific individual

Confidence that a given claimant is the same as a subscriber that has previously authenticated

Combines aspects of the federation model, assertion protection strength, and assertion presentation used in a given transaction into a single, increasing scale

How do you specify a secure identity?

- Need to narrow the question.
- Leverage existing specifications and standards.
- Look to supply chain and industry for best in class and practice.



Secure Identity

Physical Security

- Credentials
- Readers
- Controllers
- Cameras and other IP devices
- Network
- Servers and Storage
  - OnPrem
  - In Cloud

Population of people and devices for an identity/ identifier

Establish the use cases

- Supply chain and customers
- Digital and physical

Identity Assurance

- Sponsor/Application (HR policy)
- Background Check (Identity, Qualifications, Disqualifications)
- Breeder Documents
  - I9 or equivalent typically
- Enrollment
  - “Registration Authority”
- Issuance (Identifier)

Identifier and Authentication Assurance

- Uniqueness
  - Namespace
    - Constraints (128 bits?)
    - Collisions (Corporate 1000… redux)
- Multiple Identifiers
  - Global (GUID, UUID)
  - Application
  - Credential (Certificate, Private Key)
  - Keys (Base Key, Symmetric, Asymmetric)

Identifier and Authentication Assurance

- Modern standards-based cryptography
  - Symmetric
  - Asymmetric
- Strongest practical key protection
  - Hardware based secure element
  - Root key(s) and key management
- Strong binding of the keys (and certificates) to people of a given identity assurance.

Baseline Requirements

Component	**Cards**	**Mobile**	**Readers - Peripheral Devices**	**Controllers, Cameras, IP Intercom, etc.**	**Switches**	**Servers and Workstations**
Standards - Requirements	Modern Standards Based Cryptography • AES 128-256 • ECC (note: ECC varieties) • RSA 2048 (dependent on processing speed)	• Bluetooth Low Energy vs. NFC • Approved App • Multi-Factor • Trusted platform	Strong Device Credential Authentication and Secure Bi-Directional Communications • TLS 1.2/3 for IP devices • Secure OSDP profile • Supports OSDP File Transfer	Secure Device Authentication and Secure Communication • TLS 1.2/3 • Secure OSDP profile • Supports OSDP File Transfer	Secure Device Authentication and Secure Communication • TLS 1.2/3	Secure Device Authentication and Secure Communication • TLS 1.2/3 Leverage other IT Security and Privacy Standards

Logical vs. Physical

- Physical access and accessing web pages are different.
  - Convergence is only partially here.
  - Multifactor Authentication (MFA, 2FA)
- Web and logical access “tokens”
  - PKI or FIDO (asymmetric keys)
  - OAuth and OpenID Connect (JOSE)
  - Username and Password
  - Biometrics
  - Adaptive

What about biometrics?

- Existing law in IL, LA, TX, MA, CA, WA, OR, NY and municipalities (e.g. facial recognition bans).
- Not the same as privacy laws which also require important consideration.
- OSDP Biometric Profile (Secure Channel)
- Introduces requirements for managing identity/privacy assurance risks, vs. authentication/security risk.
- Encryption in motion and at rest, and other controls

Mobile drivers license (something new..)

- Opportunity to combine strong IAL and AAL.
- ISO Standard
- Could include biometric information?
- Introduces 3rd party identity providers (FAL)

References and Links

- NIST Digital Identity Guideline SP-800-63-3, A,B, C, 4
- NIST Frameworks
  - SP 800-53 Security and Privacy Controls
  - Cybersecurity Framework
  - Privacy Framework
- NIST INCITS Standardized Biometric Data
- NIST Post Quantum Crypto
- European Data Protection Board Processing of personal data through video device.
- Mobile Drivers License ISO/IEC DIS 18013-5