

PRIVARIS®

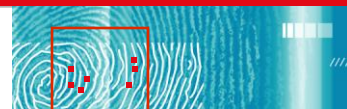


Moving To An Identity-Centric Model for Access Control

John Petze, President & CEO

Privaris, Inc.

Builconn 2007



Where We Use Identity

Entry



- Entry into secure buildings, rooms, vehicle gates

Computer



- Computer and network logon (local and remote) and access to data files, email, websites

Identity

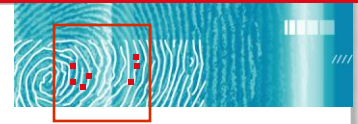


- Society/government – Identity information, such as driver licenses, passports, corporate, government or other credentials

Transactions

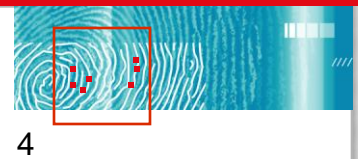


- Credit cards and other financial credentials for both online and point-of-sale transactions



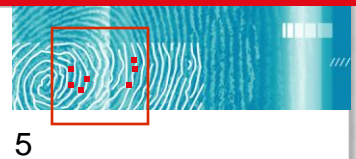
Moving to an Identity Centric Model

- Historically identity has been defined in respect to the requirements of individual systems: physical access control, IT
- As systems proliferate identity becomes fractured and duplicated
- Non-scalable, hard to manage, insecure, inefficient
- Systems are not “on top” anymore. Its not the control panel and its methods of recording identities and access privileges that matters now. This is a technical detail.
- Time to move from equipment centric view (readers, control panels) to an identity centric model.
- The identity of the person and the management of that identity through the lifecycle of the person’s involvement with the enterprise is the prime element:
- Identity authentication ➡ identity attributes ➡ transfer of credentials as appropriate for the service provider (recipient)



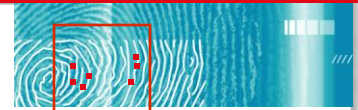
Convergence

- The move to identity-centricity is driven by the convergence of physical and logical access control
- Attributes of converged access control
 - Management of both functions by same C-level executive (Typically CSO, CIO)
 - Move to IP-backbone for all physical access control hardware
 - Single identity owns multiple credentials as needed for all access transactions:
 - Access card, usernames and passwords, smart card credential, one time password, etc.
 - Identity management middleware, or federation software is part of the IT environment



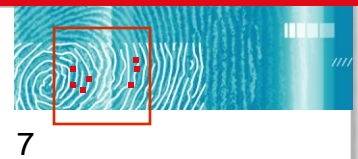
Physical or Logical?

- Use Case Example:
 - Laptop stolen from office
 - Contains sensitive corporate data
 - Is this a physical or logical security problem?
 - Who had access to facility? To office area?
 - How can access to PC be achieved? Simple password? Secure token? Is data encrypted?
 - *Who you gonna call?*



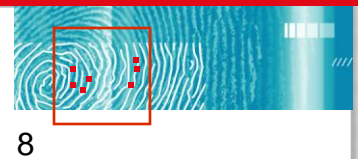
Identity Convergence Drivers

- Regulatory compliance
- Exposure to financial risk
- Cost of managing disparate systems
- “Federated Identity”



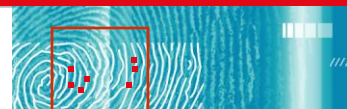
Identity Convergence Drivers

- Organizations need to reliably **verify every person** *without* excessive expense or the invasion of privacy
- **Reliable authentication:** passwords, cards, keys – something you know and have – are not enough (actually they are too much!!!)
- **Convergence of Systems and Responsibilities:** consolidation of physical and logical access devices and methods. Security is hampered by the proliferation of different passwords, cards, and credentials
- **Government requirements:** policies and standards to control physical and logical (computer) access (HSPD-12, FFIEC, SOX, PIV, HIPAA...)
- **Increasing privacy concerns:** databases with personal information continue to be compromised creating legal and financial risk for organizations holding that data

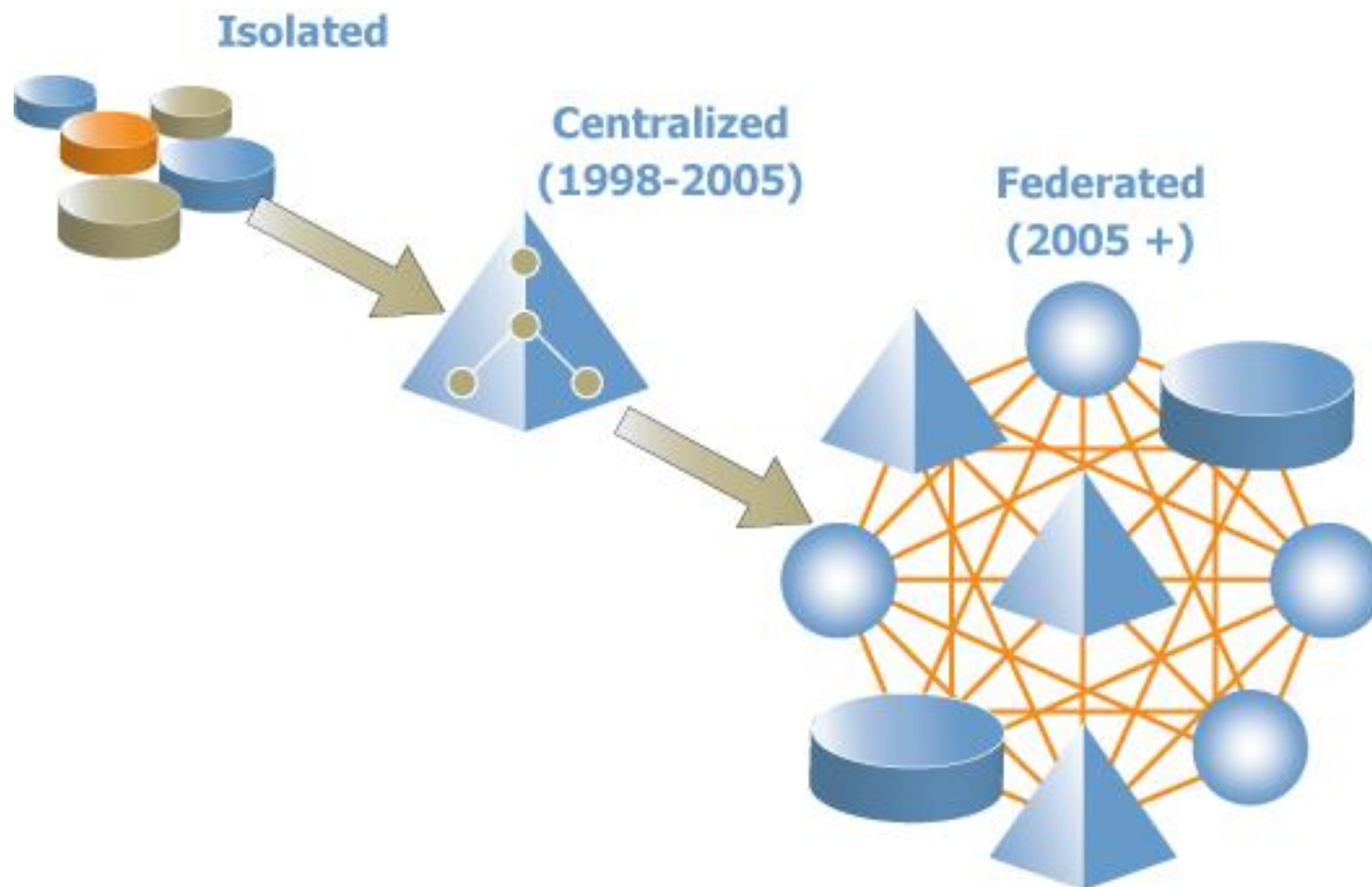


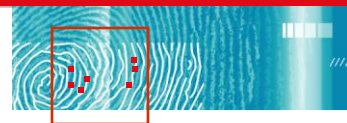
Federation of Identity

- The new trend – essential to Internet scalability and supply chain interoperability
- *Standards and technologies that make it possible to share identity information, and associated privileges, across different domains*
- Enables portability of identity information across boundaries – applications, enterprises – across networks and the Internet
- Goes beyond single sign on (SSO) middleware
- Based on SAML (Security Assertion Markup Language) and WS-* suite of specifications (an OASIS standard)

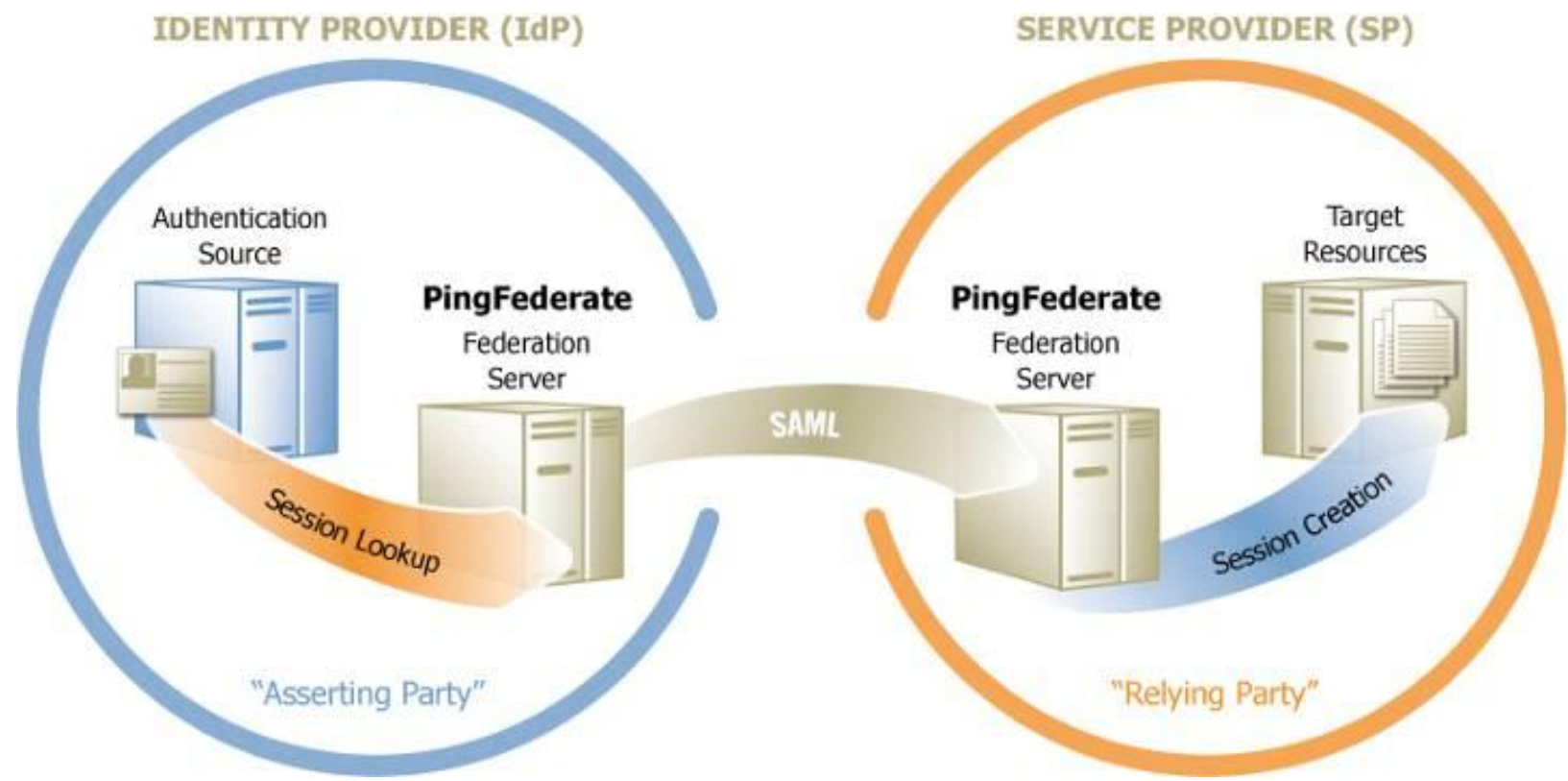


Identity Federation Continuum

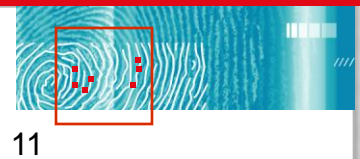




Federation



Application Security Evolution



11

Centralized

- Provisioning
- Policy
- Access Mgmt



Federated

Isolated

ERP

CRM

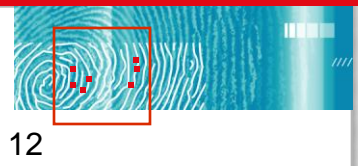
Windows

VPN

Citrix

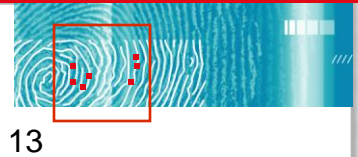
Mainframe

Custom



Supporting identity convergence

- **Unified solution** for both physical and logical access
- **Compatible** with existing security systems to minimize impact and cost
- **Biometrics** for accurate verification
- Ensure and protect individual **privacy**



Supporting identity convergence

You need compatibility with all major industry standards

- **125kHz** proximity card - common door readers
- **13.56MHz RFID** contactless smart card readers - doors and computers (ISO14443A/B, 15693 & NFC) for access control and financial transactions (contactless payment)
- **2.45GHz Bluetooth™** to access computers and networks
- **USB** for “tethered access” to computers and networks
- **One-time-password** delivery for remote access to computers and networks and “air gap” requirements

PRIVARIS®