BOEING

Engineering, Operations & Technology
Information Technology

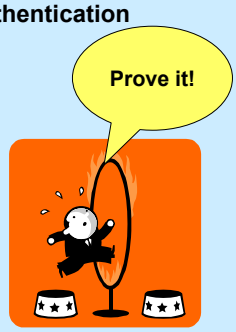
Identity Management in a Global Enterprise

Stephen T. Whitlock, Chief Architect
Information Protection & Assurance
The Boeing Company

Identification, Authentication & Authorization

Identification

Authentication



Authorization

The fine print:

- **Identification:** The presentation of an identifier so that the system can recognize and distinguish the presenter from other principals
- **Authentication:** The exchange of information in order to verify the claimed identity of a principal
- **Authorization:** The granting of rights, including access, to a principal, by the proper authority

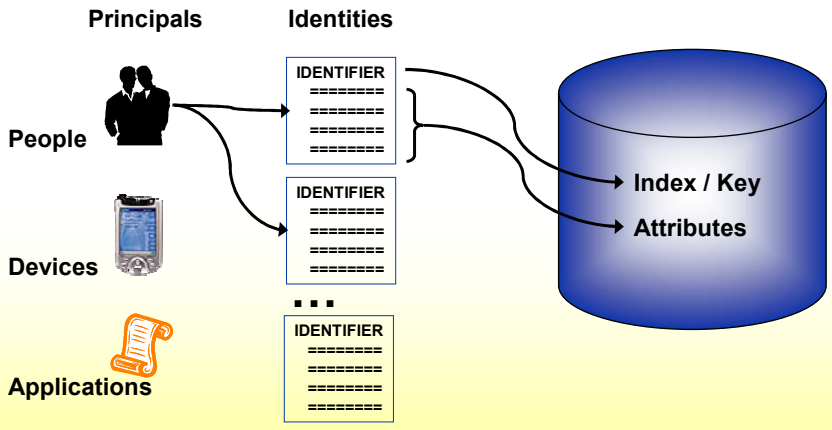
Principal: An entity (people, devices, applications, etc.) whose identity can be authenticated

Copyright © 2007 Boeing. All rights reserved.

Date: 5/11/2007

Identity Management Terminology

Engineering, Operations & Technology | **Information Technology** — **Information Protection & Assurance**



Copyright © 2007 Boeing. All rights reserved.

Date: 5/11/2007

Current State

Engineering, Operations & Technology | **Information Technology** — **Information Protection & Assurance**

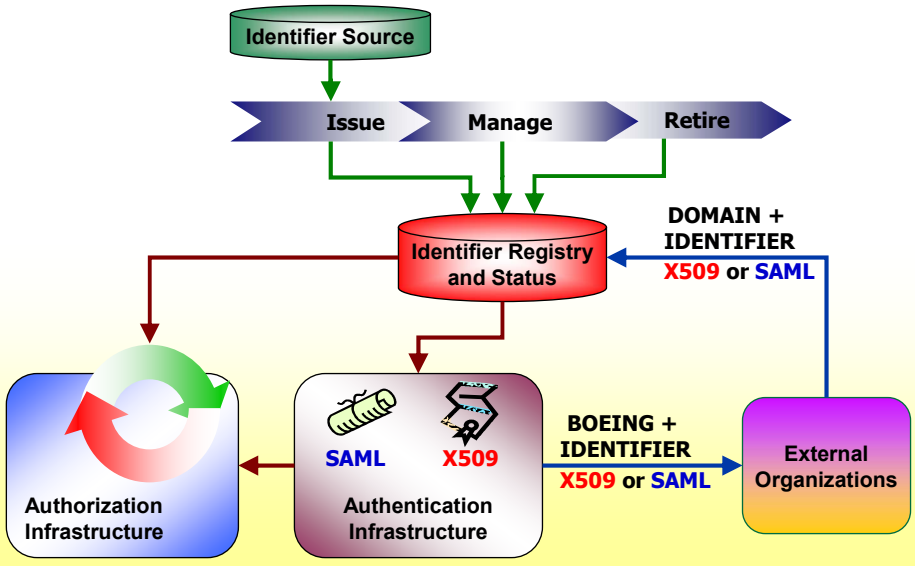
- **Boeing Electronic Messaging System ID (BEMSID) is the predominant identifier**
- **BEMSIDs provide a pervasive common identifier**
  - **In use for over 10 years**
  - **Mostly eliminated SSN use and associated risks**
  - **Never reused**
  - **Uses**
    - **Index into LDAP / Databases to look up attributes and roles**
      - **Used with authorization systems**
    - **Relative Distinguished Name in X.509 certificates**
      - **Stable RDN reduces certificate revocations**
    - **Used in SAML assertions**
- **Identifiers and attributes supported by a distributed, robust corporate electronic directory service that manages identities and supports applications**

Copyright © 2007 Boeing. All rights reserved.

Date: 5/11/2007

Identity Management Overview

Engineering, Operations & Technology | **Information Technology** — **Information Protection & Assurance**



Copyright © 2007 Boeing. All rights reserved.

Date: 5/11/2007

Challenges

Engineering, Operations & Technology | **Information Technology** — **Information Protection & Assurance**

- **BEMSID Challenges**
  - **BEMSID not meaningful outside of Boeing**
    - **BEMSID pool also includes non-Boeing employees - now about 160,000**
  - **Current identity systems are people focused**
    - **BEMSID pool also includes devices, applications, etc.**
      - **What is an application?**
      - **Device IDs still rely on proxy support from human**
- **General Challenges**
  - **It is a mistake to equate human identity to digital identity**
    - **If the principal is a human there is a relationship between the human identity and the digital identity, but that relationship can be many things and one does not necessarily identify the other (anonymity).**
  - **Global Regulatory Differences**
    - **In some jurisdictions companies cannot ask for citizenship**
    - **Some export decisions cannot be made without citizenship information**
  - **If one ID is used for all access what are the privacy and security risks from aggregation? Will this become another SSN?**
  - **Need identity assurance levels between enterprises**
    - **Significant work is required for managing identities for business partners without strong identity management practices**
  - **Blurring of identification, authentication, and authorization in products, protocols and ceremonies**
  - **If identity is central how do we offer services to those who cannot have identities in our systems?**

Copyright © 2007 Boeing. All rights reserved.

Date: 5/11/2007

Identity Management Strategy

- **Strategy**
  - **Deploy support for multiple identifiers from different sources across the extended enterprise**
- **Approach**
  - **Manage the complete life cycle of identifiers used to designate principals, including people, applications, devices and resources**
  - **Manage and federate the identity relationship between Boeing and external principals and organizations**
- **Current Activity**
  - **Augment the BEMSID, used for people, with new identifier types for applications, devices and resources**
    - **Backwards compatible with current people identifier**
  - **Adopt the OASIS XRI Framework for external identity needs**
    - **Collaborated with -**
      - **The Open Group, Network Applications Consortium and Distributed Management Task Force – produced a Core Identity Framework document**
      - **Transglobal Secure Collaboration Program**
    - **XRI simplifies our federation of identity management services**
    - **XRIs already generated for existing BEMSIDs**

Copyright © 2007 Boeing. All rights reserved.

BOEING

Copyright © 2007 Boeing. All rights reserved.