

Identity Management: Key Technologies

Michael Huth
imperial.ac.uk/quads

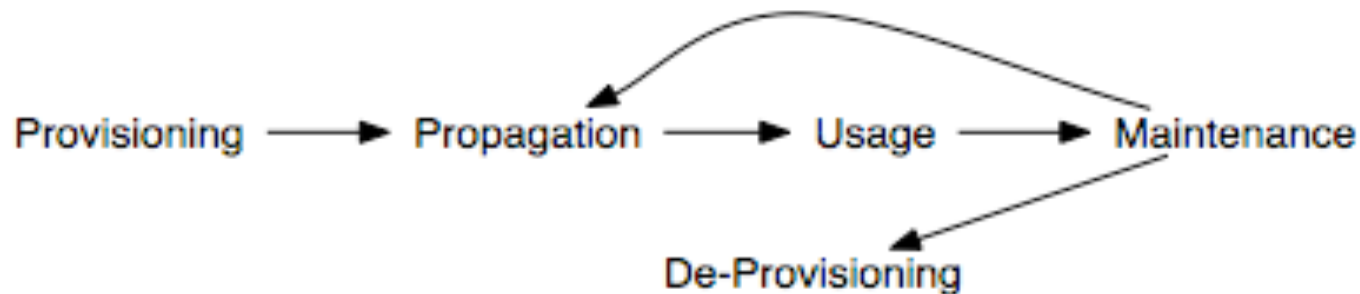


Key Concepts

- **Subjects:** agents that can request access to resources, e.g. *you or Microsoft Word*
- Subjects get access by claiming identities
- **Identities:** collate attributes or traits of subject
- **Traits:** *inherent* characteristics, e.g. *eye color*
- **Attributes:** *acquired and transient*, e.g. *visa status*
- **Credentials:** means of *laying claim to* an *identity*, e.g. *biometric*

Identity Management System (IMS) lifecycle

- **Provisioning:** creates/initializes identity records
- **Propagation:** stores/sends identity records to required locations/devices
- **Usage:** e.g. *authentication of finger print*
- **Maintenance:** *change management* of identity attributes and required resources
- **De-provisioning:** remove identities from IMS



Authentication & Authorization Technologies

- ***Authentication:*** process of checking validity of credentials, e.g. *passport*
- ***Authorization:*** process of mapping identities onto entitlements for access to resources
- Authorization Technologies have Authentication Technologies as vital components
- E.g. *check authenticity of passport before granting access to baggage claim area*

Biometrics

- Uses biological or behavioral traits to *uniquely identify* person or animal
- E.g. *signatures, voice, palm or finger prints*
- Its strength (uniqueness) also its weakness: e.g. *copies of finger prints “as good” as the real thing*
- Useful for *negative identification*, e.g. *detection of benefit fraud*
- *Enrollment*, e.g. *provisioning of biometrics in National Identity Registry*
- *Verification*, e.g. *authenticating iris scan against data stored securely in passport*

Two-Factor Authentication

- Authentication based on two credentials of different kind, *both must be approved*
- E.g. *ATM card (something you have) & PIN (something you know). Not username/password (both are something you know). One-time passwords for sensitive transactions.*
- Great scope in nature and interaction of two factors
- Two- and multi-factor authentication have *many future applications*, e.g. *fraud resistant train tickets, electronic voting, and exams*

Role-Based Access Control

- Systems that control access to resources *based on subject's role*, not their identity
- E.g. *company access policies*
- E.g. *role-based email: seniortutor@imperial.ac.uk*
- Offers *better change management*: only role attributes need to be updated; existing credentials then bind to new role
- Different roles may serve as different personas

Digital Rights Management Systems (DRM)

- Framework for *controlling circumstances* under which digital resource can be used
- Possibly dependent on usage history but independent of usage location
- E.g. *Fairplay (iTunes)*, *Zone Codes for DVDs*
- Of considerable interest for military and public section, e.g. *citizen-centric DRMs*
- Consumers need to see *cost/benefit value* in being under such contextual usage control

Directories & their Meta and Virtual Versions

- **Directories:** centrally managed repositories for retrieving structured information to be supplied to distributed applications
- E.g. *Domain Name Server (DNS), X.509 Public-Key Infrastructure Standard, Lightweight Directory Access Protocol (LDAP)*
- **Meta Directory:** centrally managed, *needs to synchronize* with other directories of organization
- **Virtual Directory:** *no synchronization, presents single/integrated view* of data that reside in different directories

Identity Management Systems and Architectures

- ***IMS Architecture***: result of systematic analysis of how to conceive and carry out identity management in an IMS
- Comprises *process* architectures, *data* architectures, *policies*, and *interoperability frameworks*
- Architectural Patterns, Best Practices, *Capability & Maturity Models* will emerge

Federated Identity, Risk/Trust Management

- ***Federated Identity:*** Software architecture with *low coupling between heterogeneous IMSs*
- Coupling provides well defined & contained sharing of information
- E.g. *PingID & SXIP offer products*
- Increasingly important for *opportunistic federations in business and government*
- ***Risk/Trust Management Systems:*** automated risk assessment, risk revision; e.g. *in setup or negotiation of federations*

Anonymity, E-Cash, and E-Voting

- ***E-Cash***: (real or virtual) money exchanged in electronic form
- ***E-Voting***: provision, conduction or audit of election by electronic means
- ***Anonymity or Pseudonymity*** desired in E-Voting
- E-Cash versus Credit/Debit Cards
- Anonymity versus Traceable & Analyzable Customer Behavior
- Great potential of E-Cash and E-Voting in future

Interoperability Standards

- Specifications of *how data & processes should be implemented so that other systems can understand them*
- E.g. *Security Assertion Markup Language (SAML), Service Provisioning Markup Language (SPML), eXtensible Access Control Markup Language (XACML)*
- *Clear need for this, e.g. in federated IMSs*
- *XML key technology driver*

User-Friendly Solutions

- Solutions to Identity Management that are *easy to learn, easy to recover, etc.*
- E.g. *Single-Sign-On, Identity-Based Encryption, Self-Service Password Reset Service*
- *Free* Wide Area Wireless Network Access?
- *User empowerment great economic & societal enabler*

Regionally/Globally Unique Identifiers

- Means of *identifying subjects* or resources *uniquely within a region*, or globally
- E.g. *Oyster Card, Radio Frequency Identification Device (RFID), Universally Unique Identifier (UUID), The Digital Object Identifier System (DOI)*
- *Public perception and trust issues*
- Open standards and solutions (e.g. UUIDs) can be used within IMSs
- DRMs to control use of Unique Identifiers, e.g. *National Insurance Card?*

Pie-in-the-Sky Technologies

- **Quantum-based Digital Identities:** require scalable and stable quantum computers, which will make *past digital signatures insecure*, so hugely disruptive and trust-eroding technology
- **Adaptive Behavior:** *Ad hoc networks*, e.g. *Car Platooning*, and the emergent & evolving roles/identities of agents therein
- **Sensory Networks:** heterogeneous, ubiquitous tracking of activities, e.g. Microsoft's new Office Monitoring Tool; privacy issues
- **Computer Forensics:** *increased logging of identity-related information* for possible forensic activities; privacy issues

- **Nanotechnology:** creation of *unobtrusive and*

Not So Pie-in-the-Sky Technologies

- **Sensory Networks:** heterogeneous, ubiquitous tracking of activities
- E.g. as in The Times (online), 16 January 2008:
'The Times has seen a patent application filed by the company for a computer system that links workers to their computers via wireless sensors that measure their metabolism. [...] Microsoft submitted a patent application in the US for a "unique monitoring system" that could link workers to their computers. Wireless sensors could read "heart rate, galvanic skin response, EMG, brain signals, respiration rate, body temperature, movement facial movements, facial expressions and blood pressure", the application states.'

Recommended Reading

Philip J. Windley

Digital Identity

O'Reilly Media, Inc.

2005

