Corporate Identity Considerations for Cloud and ASP Application Vendors

Joe Bate
Senior Security Architect

OWASP Toronto Sept. 23rd, 2009

Disclaimer

- The points of view or opinions contained within this document are those of the author and do not necessarily represent the official view, position or policies of his employer.
- Diagrams provided are for discussion purposes and not technically accurate. Each of the processes and flows have an infinite number or variations

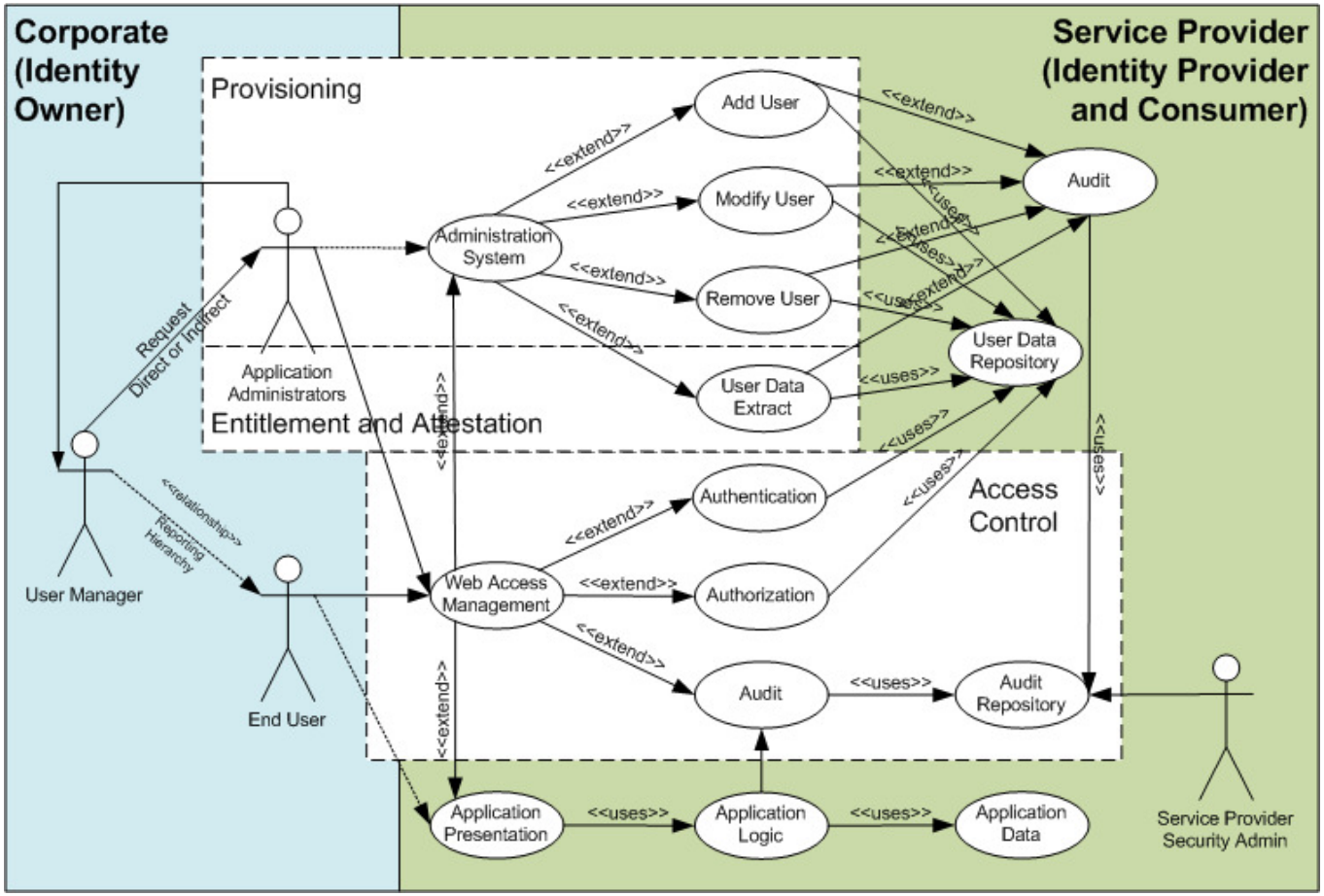
Background

- What is Cloud Computing?
  - **C**ommon
  - **L**ocation Independent
  - **O**nline
  - **U**tility
  - On-**D**emand
- What is an ASP Application?
  - A computer based service on the network
  - May or not be multi-tenanted
- What is a Cloud Application?
  - ASP application hosted in a Cloud
  - Multi-tenanted
  - a.k.a. Software As A Service (SaaS)

Key Areas of Consideration in Corporate Identity Management

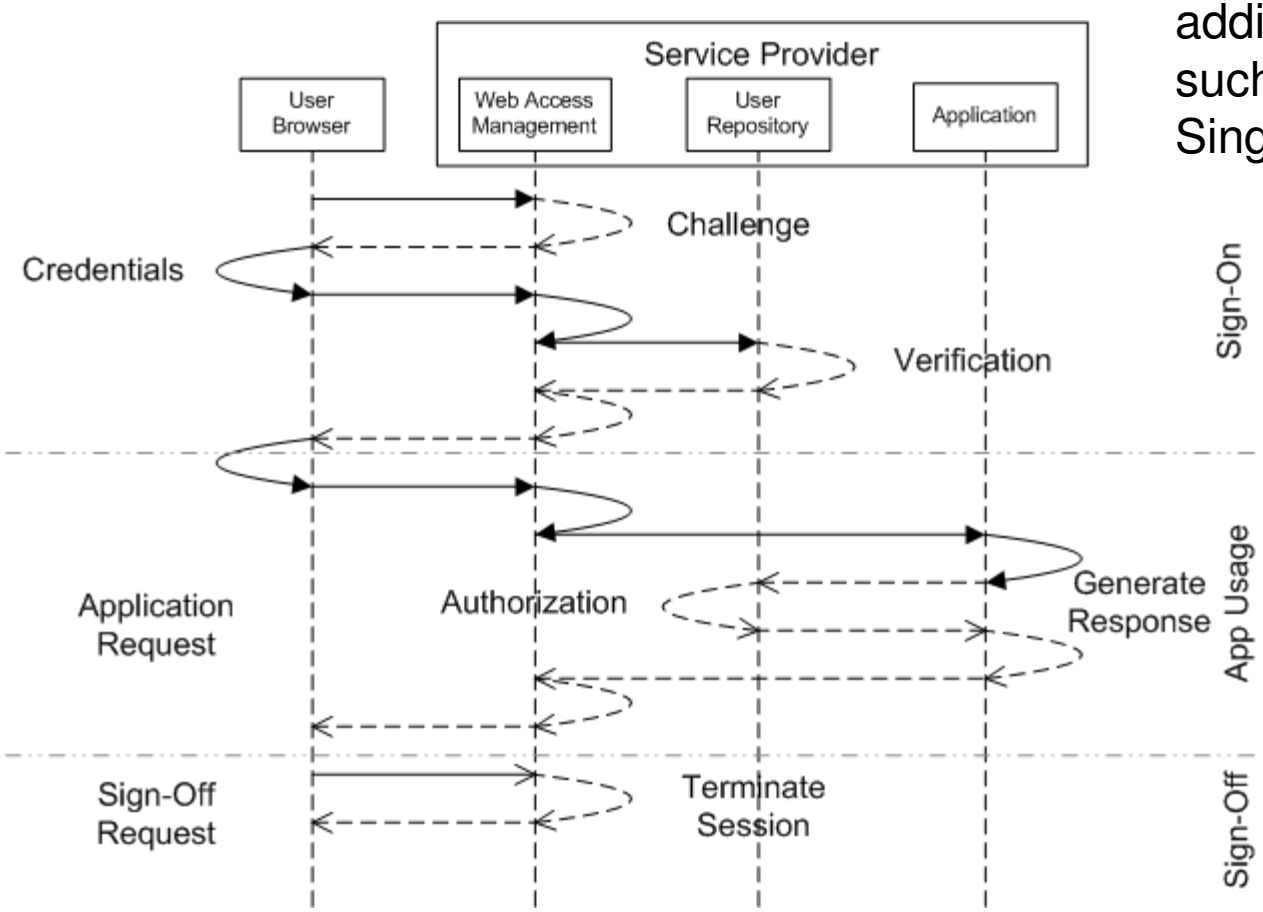
- Provisioning
  - Centralized management of user identity information, accounts and attributes.
  - May involve the creation, modification, deletion, suspension, restoration of a defined set or accounts, privileges and/or attributes.
  - May involve the execution of a defined business or system process.
- Entitlement and Attestation
  - Entitlement
    - What access the user has been granted
  - Attestation
    - Validation the access the user has been granted is what they should have for their role in the organization
  - Exceptions for Remediation
    - Delta between what access the user has been granted and actually have
- Access Control
  - Authentication
    - Single Sign On
    - Identity Assurance
  - Authorization

Traditional – Use Case Model



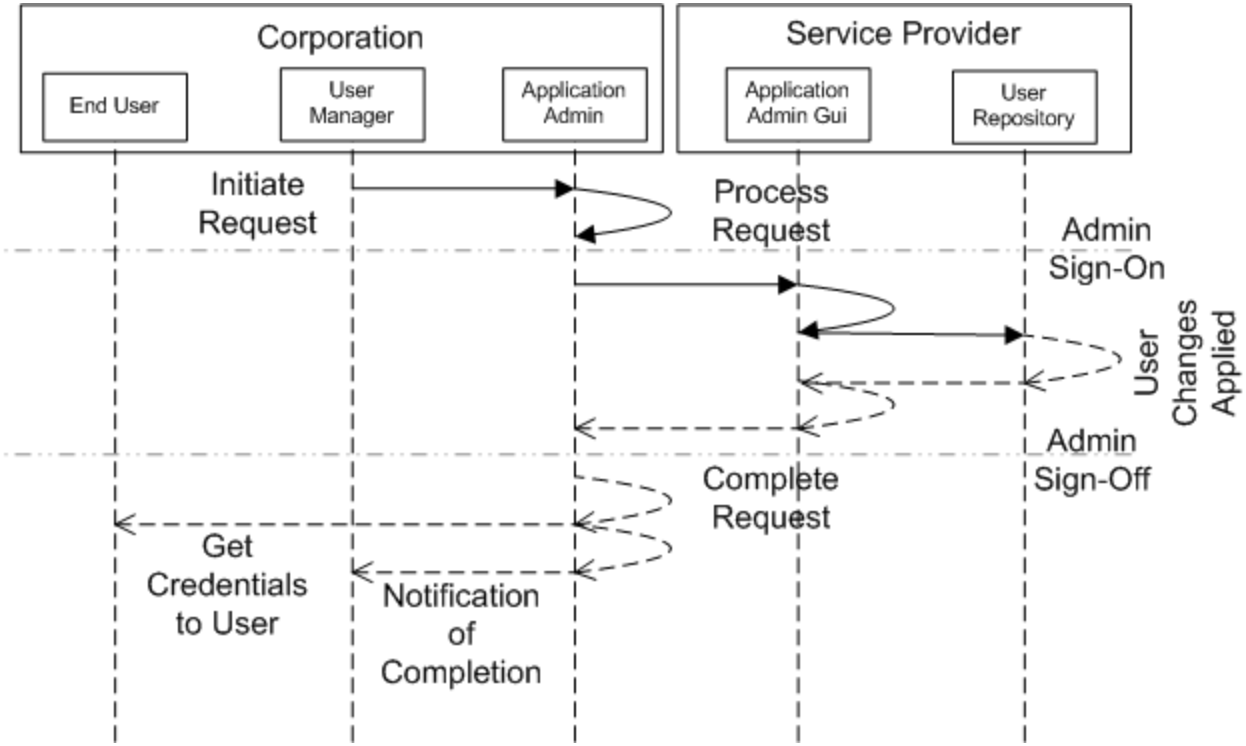
OWASP Toronto Sept. 23rd, 2009

Traditional - Sign-On

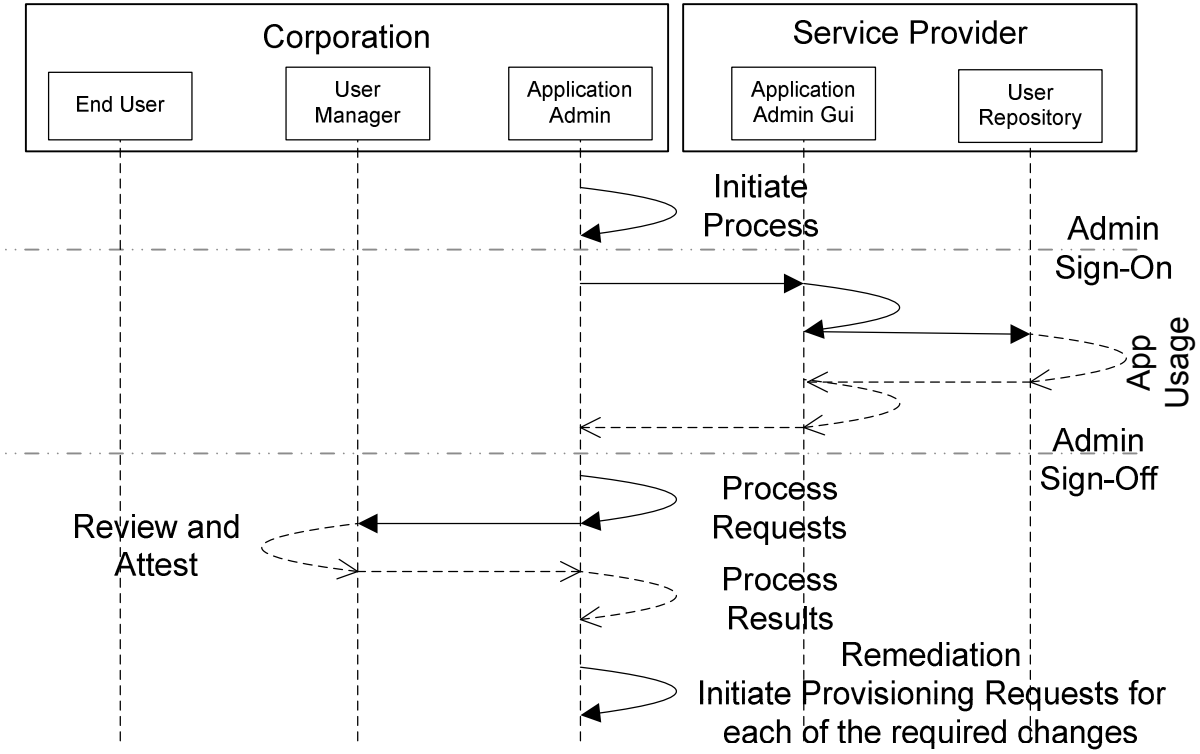


Requires additional tools such as ESSO for Singe Sign-On

Traditional - Provisioning

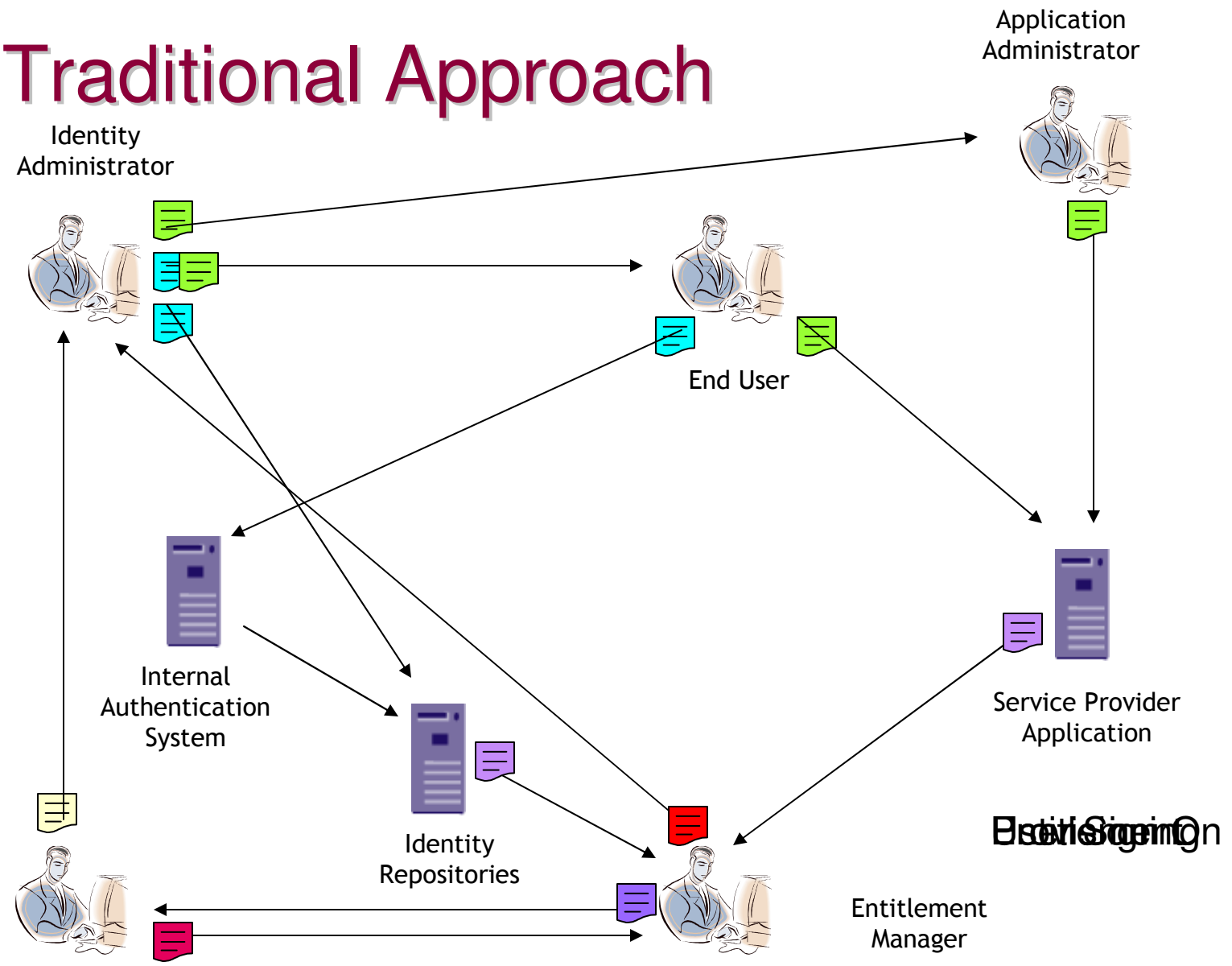


Traditional – Entitlement and Attestation Reporting



Often manual process

Traditional Approach



Issues with the Traditional Approach

- Usernames and Passwords present the follow challenges:
  - Cost:
    - Helpdesk calls for resets on infrequently used password
  - Risk:
    - Poor password handling, as user often write down the password
    - Weak password, so they are easy to remember
    - Reuse of passwords between internal and external systems, often creating an external weakest link
    - Password disclosure through credential sharing or social engineering
- Password complexity and strength is limited to remote system and the end user
- In many cases user may access user can access Internet ASP application external from corporate premises or assets.
  - This can lead to unauthorized use of resources, such as terminated employee still retaining access after leaving organization.
- Loss of productivity of business users due to time delays in accessing systems as the lookup or attempt to remember or have to have password reset.
- Delays in the suspension or termination of accounts can result in unauthorized access to systems and data.

Issues with the Traditional Approach

"The dark ages before Identity Management"*

- Isolated directories and databases containing same information about people within and external to the company
- Every application has own user management and every additional application compounds the problem
- Linkage of accounts and users becomes extremely hard to manage
- Redundancy of data and administration means high costs
- Process for provisioning accounts very slow
- User often get access to resource to late
- Even worse user keeps access after leaving the job
- There's no real security in chaos

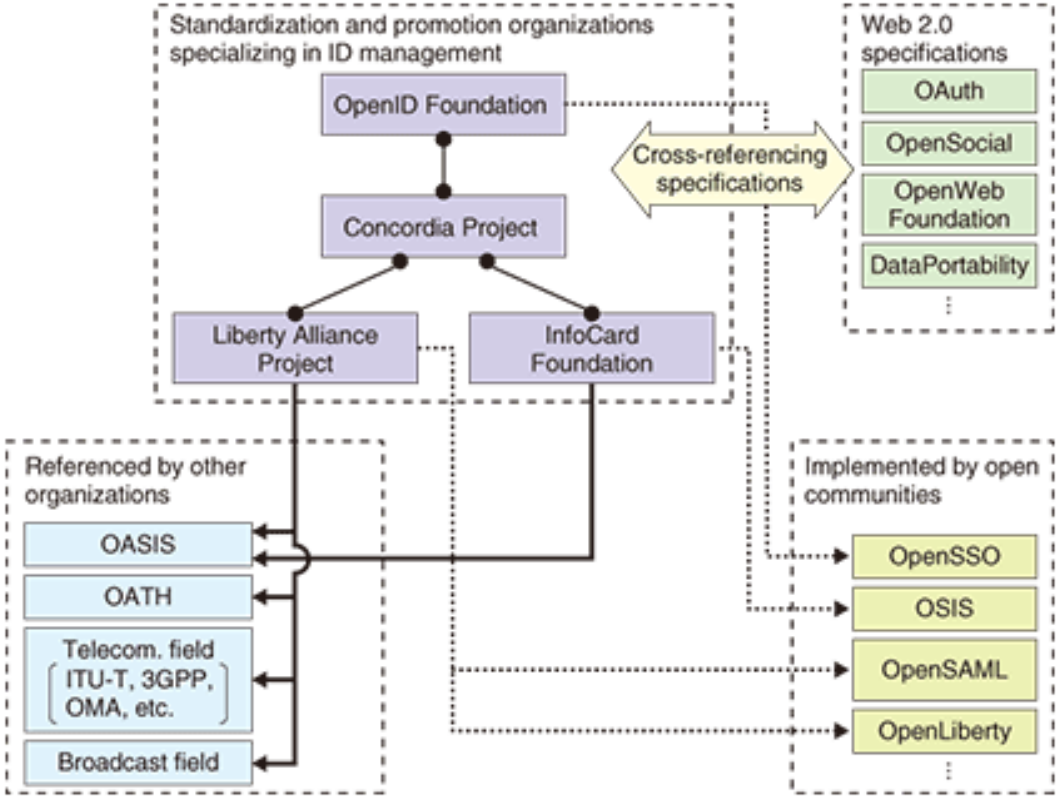
OWASP Toronto Sept. 23rd, 2009

* Unknown author

Industry Trends

- Trending towards more outsourcing technology through use of Cloud and ASP Applications, this will become more prevalent once Privacy, Data Residency and Security concerns are overcome.
- As the number of web applications increases, users are having to set up with more and more online digital identities, driving changes to the way Corporation need to handle their user identities.
- Regulatory compliance is driving better protection user security and privacy, through careful management of user identities, throughout their life cycles from creation to termination.
- Advances in IdM Industry Standardization and Alignment
- Advances IdM Technology/Industry Interoperability

Industry Standardization



Main SSO Technologies:
- SAML
- OpenID
- InfoCard

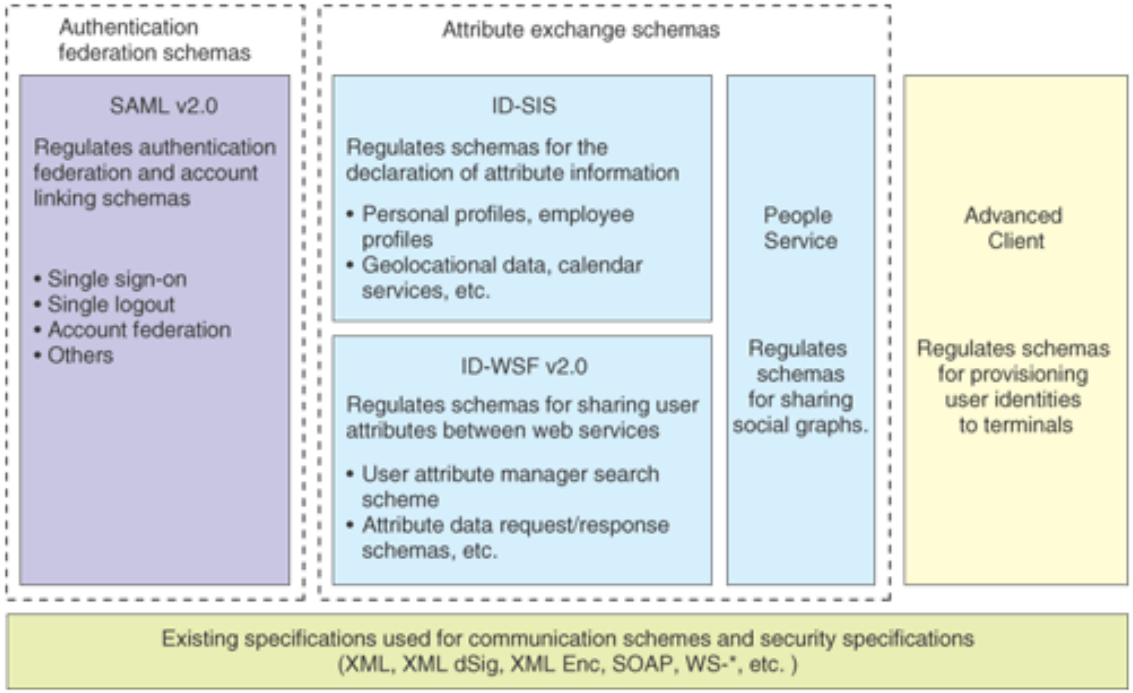
Web Application Targeted

Industry groups
- specifications
- encourage use

Main attribute exchange technology
- ID-WSF

* Standardization Trends in Identity Management Technologies

Industry Alignment



Liberty Alliance ID FF has developed into SAML v2.0, which is now regulated by (OASIS).

SAML v2.0 is also referenced by ITU-T. In the form of Recommendation X.1141

Limited SAML 2.0 supported with release of Microsoft Geneva (ADFS)

* Standardization Trends in Identity Management Technologies

Telecom Industry

ID management recommendations (including drafts) in Q10/17 (as of Feb. 2009)

Recommendation No.	Recommendation name	Scheduled agreement date	Editor (affiliation & country)
Y.2720	NGN identity management framework	Approved (Jan. 2009)	Richard Brackney (DoD, USA), Takashi Egawa (NEC, Japan)
Y.NGN IdM Requirements (draft)	NGN identity management requirements	May 2009	Martin Dolly (AT&T, USA) Enhui Liu (Huawei, China) Anthony Rutkowski (Verisign, USA) Ray Singh (Telcordia, USA)
Y.NGN IdM Mechanisms (draft)	NGN identity management mechanisms	Sep. 2009	Takashi Egawa (NEC, Japan) Zachary Zeltsan (Alcatel-Lucent, USA)
Y.NGN IdM Use-cases (Technical Report) (draft)	NGN identity management use cases	May 2009	Martin Dolly (AT&T, USA) Paul Knight (Nortel, USA) Ray Singh (Telcordia, USA)

ID management recommendations (including drafts) in Q10/17 (as of Feb. 2009)

Recommendation No.	Recommendation name	Scheduled agreement date	Editor (affiliation & country)
X.1250 (draft)	Capabilities for enhanced global identity management trust and interoperability	2009 (Reconsideration to gain approval in May 2008 and redetermined in Feb. 2009)	Anthony Rutkowski (Verisign, USA), Jiwei Wei (Huawei, China)
X.1251 (draft)	A framework for user control of digital identity	2009 (redetermined in Feb. 2009)	Sangrae Cho, Seung-Hun Jin, Michael McIntosh (ETRI, South Korea)
X.eaa (draft)	Entity authentication assurance	2010	Richard Brackney (DoD, USA)
X.idm-dm (draft)	Common identity data model	Oct. 2009	Anthony Nadalin (IBM, USA) , Paul Knight (Nortel, USA)

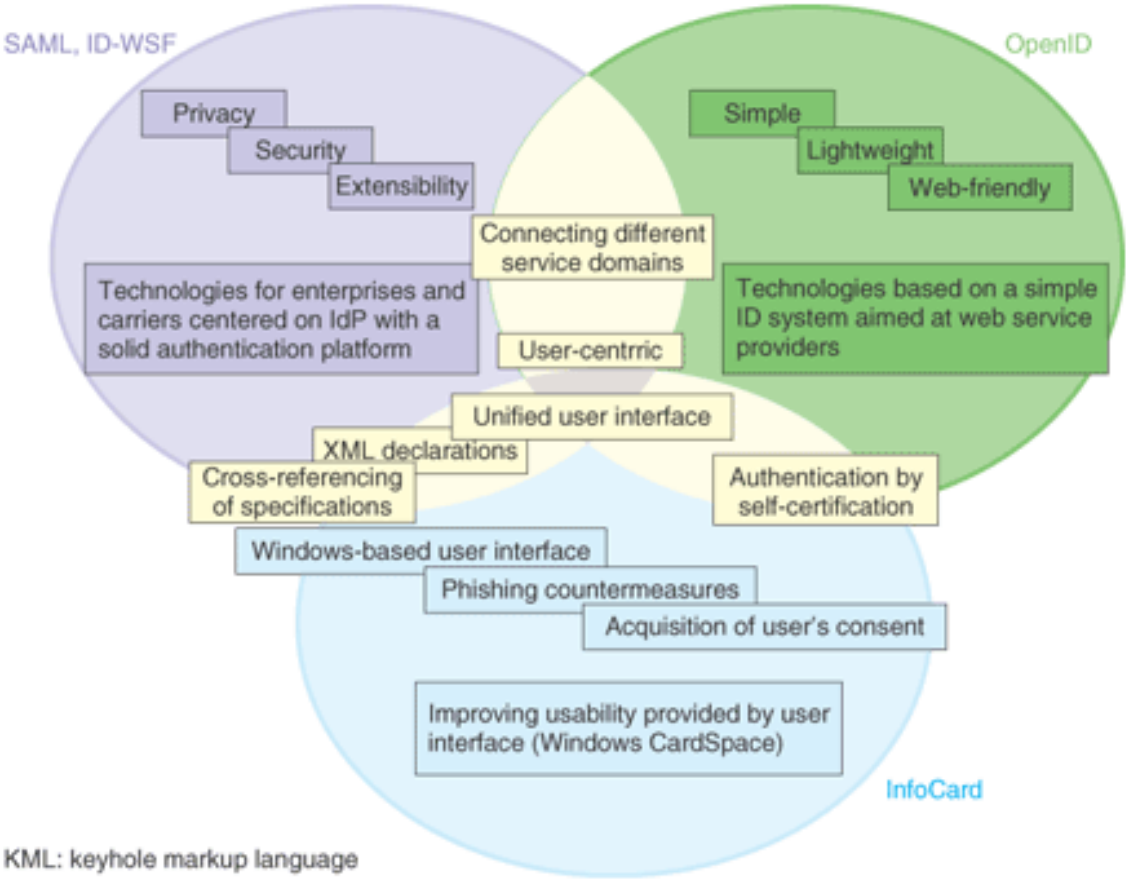
* Standardization Trends in Identity Management Technologies

Q16/13 which is investigating security and IdM in future networks including Next Generation Networks (NGNs)

Jan 2009 Y.2720 was approved by ITU-T as first stage of recommendations

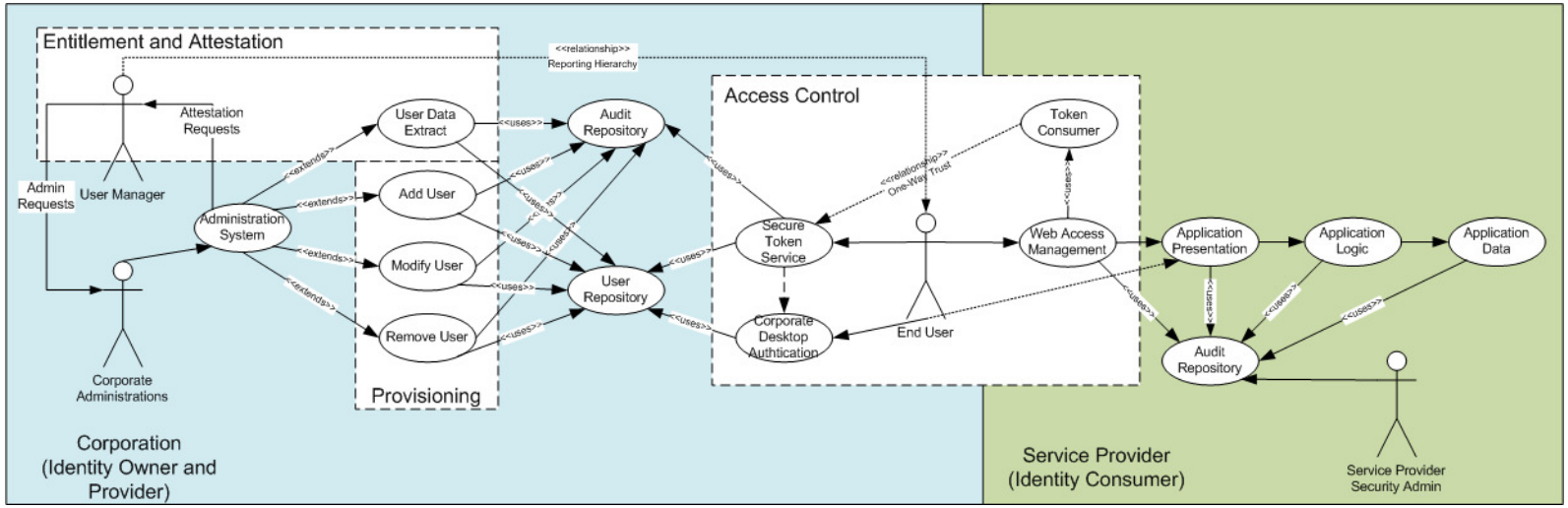
Q10/17 which is investigating IdM architectures and security mechanisms. mobile networks

Industry Interoperability



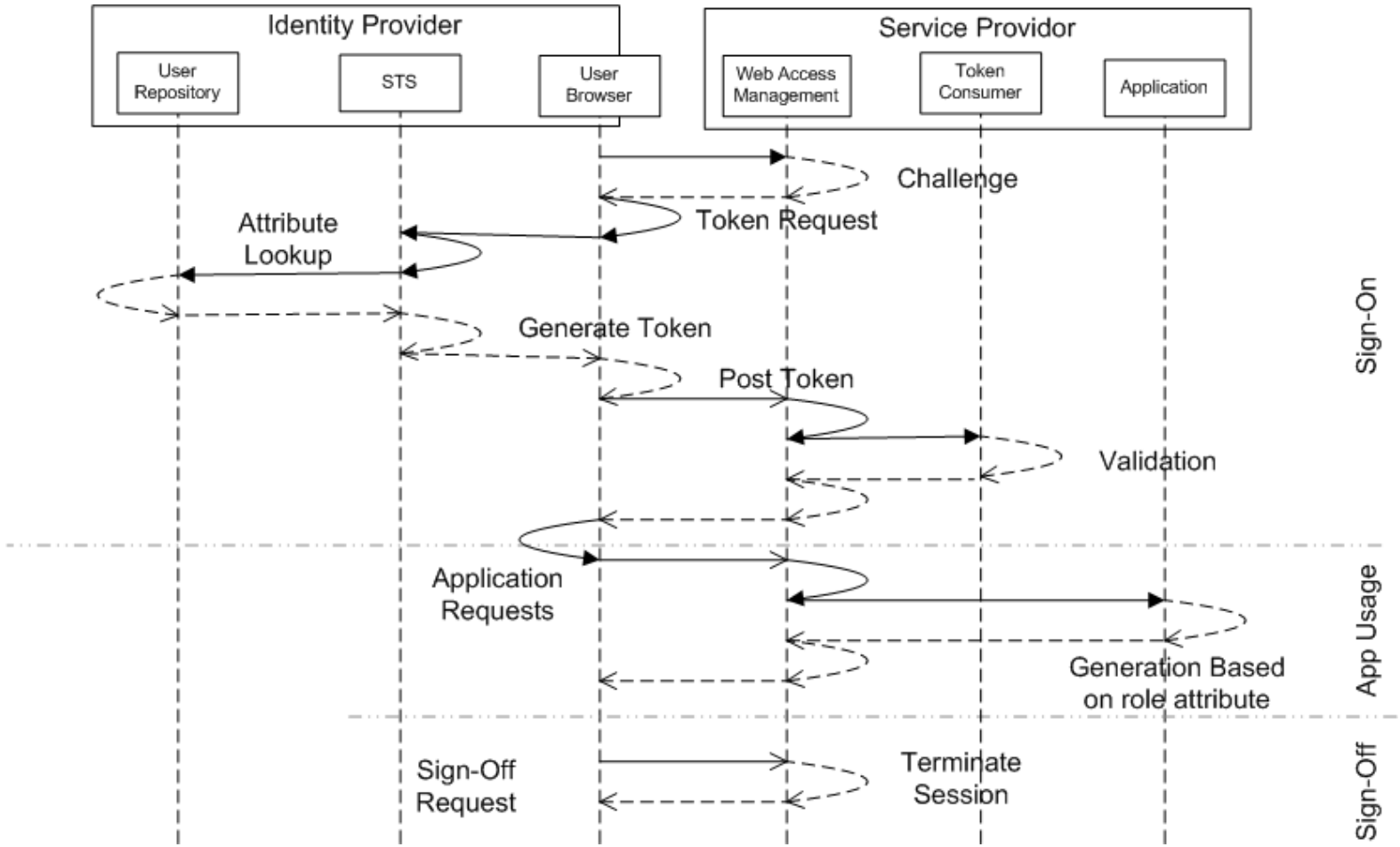
* Standardization Trends in Identity Management Technologies

Federation - Use Case Model



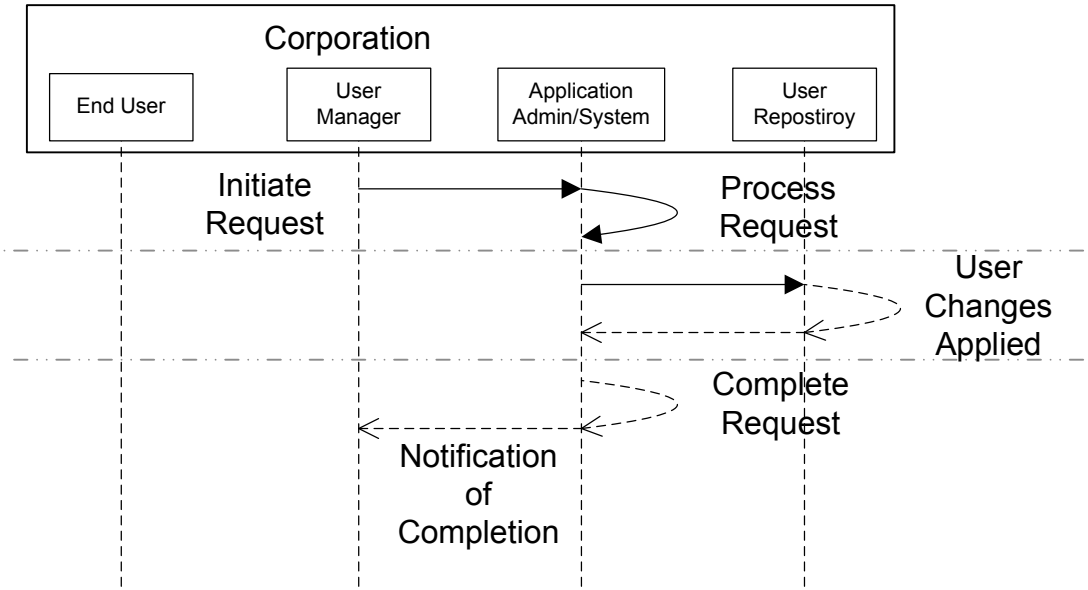
Federation - Sign-On

Example Based on
Fully Trust Model



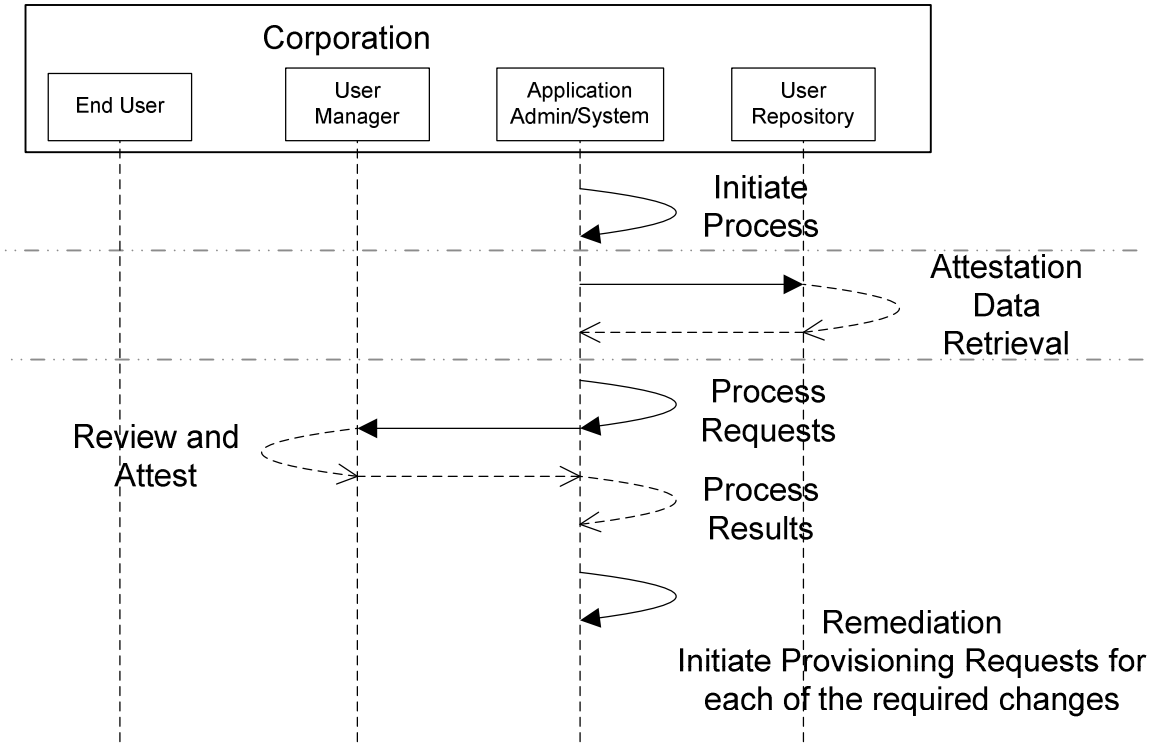
OWASP Toronto Sept. 23rd, 2009

Federation - Provisioning



If persistent tokens are used Application Admin/ System may also be required push data to Service Provider either through traditional or other method such as SPML automation

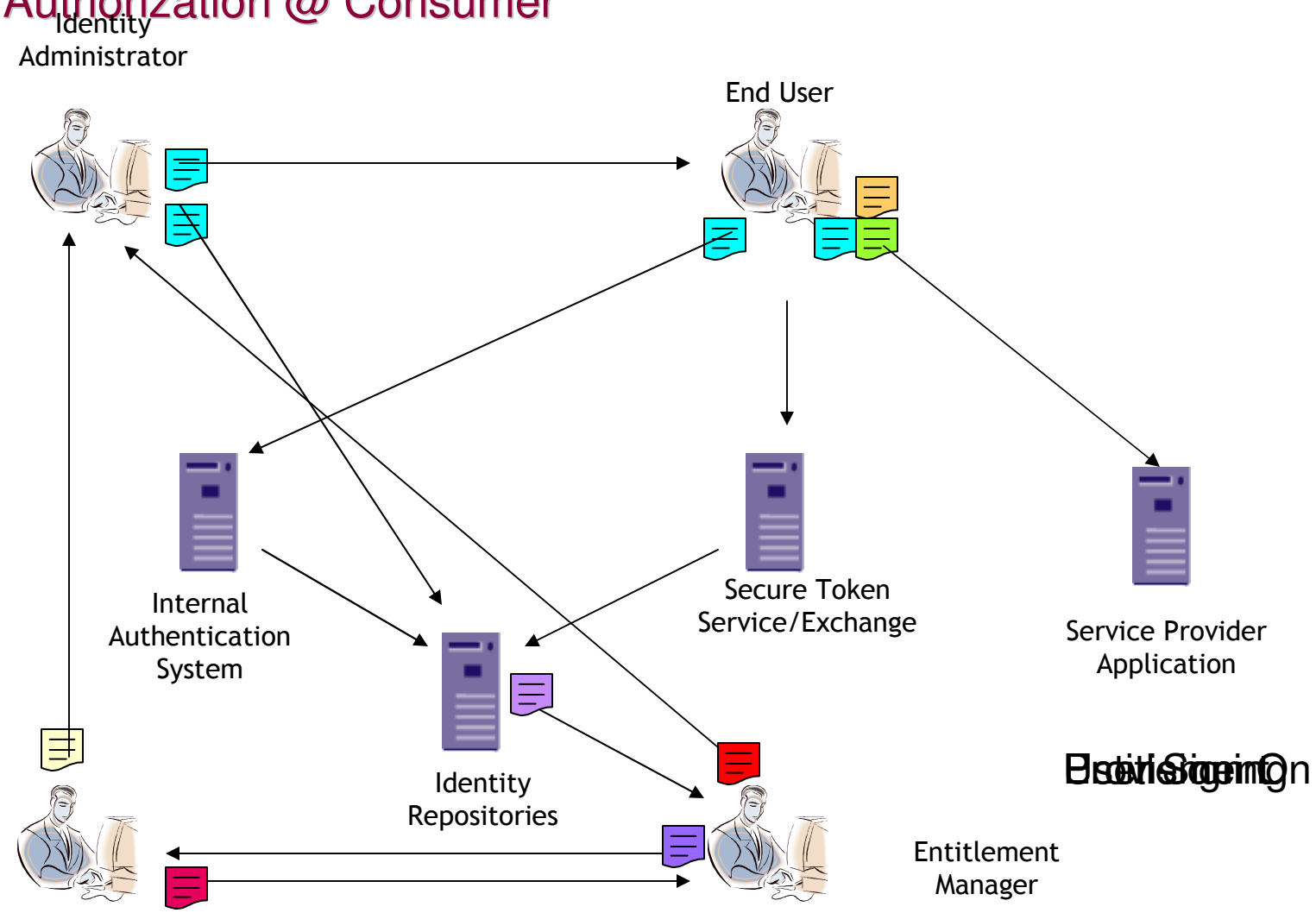
Federation – Entitlement and Attestation



If persistent tokens are used Application Admin/ System must also pull data from Service Provider and due Exception handling

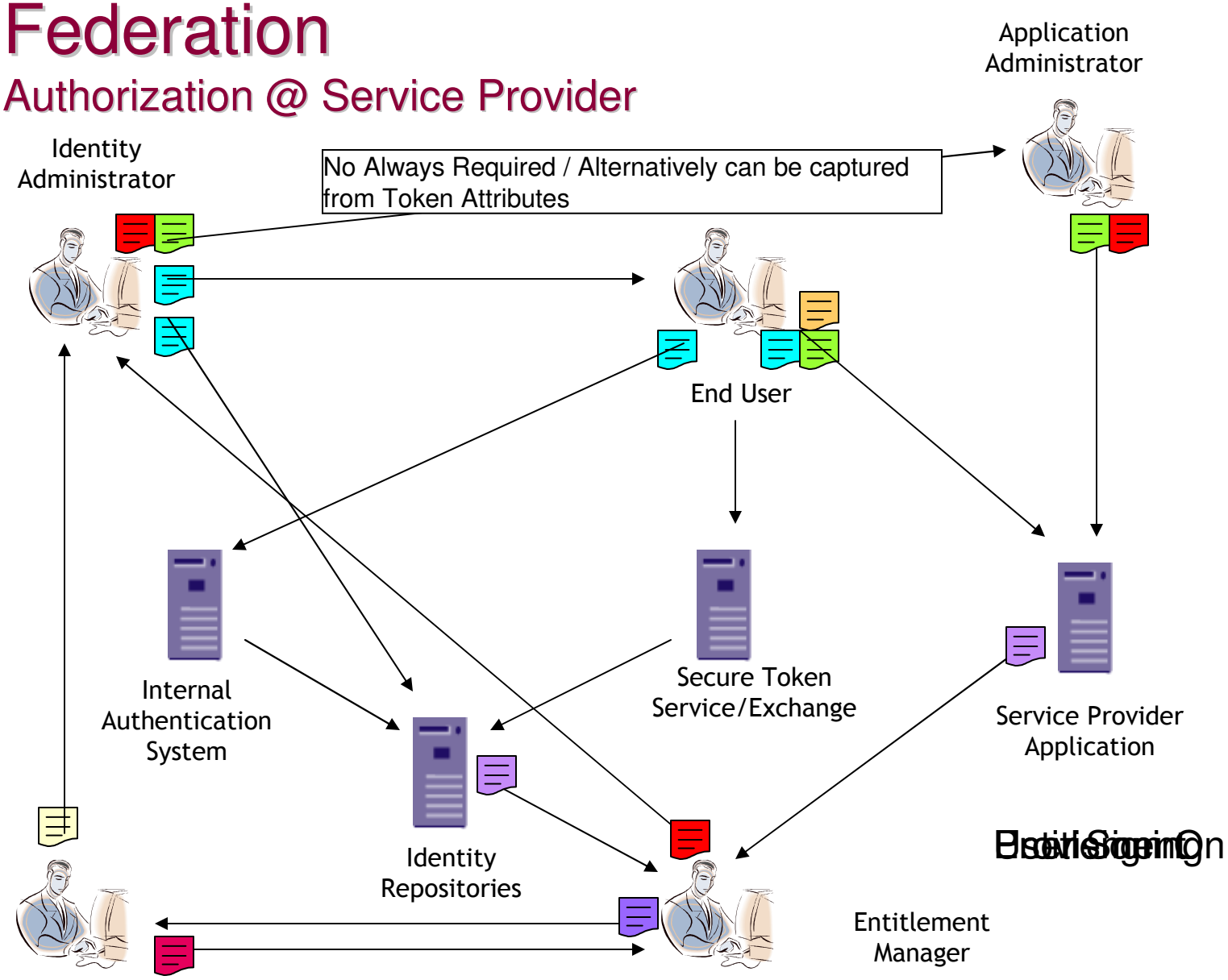
Federation

Authorization @ Consumer



Federation

Authorization @ Service Provider



Cloud and ASP Application Design Considerations

- Applications should be designed with externalized Identity Management in mind
  - Removing silo Identity Management from the application should allow changes to occur without application design impact.
  - Expect SAML 2.0 to be the Token of preference for the next few years
  - Expect SAML HTTP Post to be preference over Artifact Resolution
  - Avoid the use of persistent tokens where possible
- Applications should be designed using role based access control
  - Design application role complexity should be at service consumer discretion where possible
- Applications should be designed expecting minimal user attributes
- Applications should be designed expecting that they will no longer have or require a local user repository
- Applications should be designed expecting an increasing demand for a usage based licensing model
- Applications should always be designed with Privacy, Data Residency and Security in mind.

References and Useful Links

- http://saml.xml.org/ - Online Community for SAML OASIS Standard
- https://www.ntt-review.jp/ - NTT Technical Review
  - Standardization Activities of the Liberty Alliance
  - Standardization Trends in Identity Management Technologies
  - Recent NGN Security Standardization Trends
- http://informationcard.net/ - The Information Card Ecosystem
- http://www.projectliberty.org/ - Liberty Alliance Project
- http://www.oasis-open.org/ - OASIS
- http://www.cio.gov/ - Federal Chief Information Officers Council
  - EAuthFederationArchitectureInterfaceSpec
- http://www.xmlgrrl.com/ - Eve Maler's Blog – Pushing String
  - The Venn of identity

- http://www.ipc.on.ca/ - Office of the Information and Privacy Commissioner/Ontario
- http://www.identityblog.com/ - Kim Cameron's Identity Weblog
- http://www.idtrail.org/ - Lessons from the Identity Trail

- http://www.openid.org/ - OpenID Identity Provider
- http://www.ssocircle.com/ - SSOCircle Identity Provider
- http://www.tricipher.com/ - TRICipher Identity Provider

Contact

joe.bate@gmail.com

OWASP
Toronto
Sept.
23rd,
2009