Single Sign-On: Reviewing the Field

Michael Grundmann   Erhard Pointl

Johannes Kepler University Linz

January 16, 2009

1. Introduction
   - Why Single Sign-On?
2. Single Sign-On Architectures
   - Pseudo SSO Systems
   - Centralized SSO Systems
   - Federated SSO Systems
3. Comparison
   - Criteria
   - Categorization
4. Products
   - Overview
   - shibboleth
5. Conclusion

Why Single Sign-On?

- more Services

Why Single Sign-On?

- more Services
- more (Different) Passwords

Why Single Sign-On?

- more Services
- more (Different) Passwords
- Main Idea: One Logon Procedure for All Services

Pseudo SSO Systems

- Encrypted Credential Database

Pseudo SSO Systems

- Encrypted Credential Database
- Authentication Proxy

Pseudo SSO Systems

- Encrypted Credential Database
- Authentication Proxy
- Strong Password Dilemma

Pseudo SSO Systems

- Encrypted Credential Database
- Authentication Proxy
- Strong Password Dilemma
- Where to Store the credentials?

Pseudo SSO Systems

- Encrypted Credential Database
- Authentication Proxy
- Strong Password Dilemma
- Where to Store the credentials?
- But: Multiple Authentications are still happening

Centralized SSO Systems

- Centralized Authentication Site

Centralized SSO Systems

- Centralized Authentication Site
- Centralized User Database

Centralized SSO Systems

- Centralized Authentication Site
- Centralized User Database
- Definitions

Centralized SSO Systems

- Centralized Authentication Site
- Centralized User Database
- Definitions
    - Service Provider (SP)

Centralized SSO Systems

- Centralized Authentication Site
- Centralized User Database
- Definitions
  - Service Provider (SP)
  - Trusted Third Party (TTP)

Centralized SSO Systems

- Centralized Authentication Site
- Centralized User Database
- Definitions
    - Service Provider (SP)
    - Trusted Third Party (TTP)
- Users and SP have to trust TTP

Token Based SSO

1. User Authenticated with TTP

Token Based SSO

1. User Authenticated with TTP
2. Software Token is Cached Locally

Token Based SSO

1. User Authenticated with TTP
2. Software Token is Cached Locally
3. Each SP Verifies the Token

PKI Based SSO

1. User Generates Asymetric Key Pair

PKI Based SSO

1. User Generates Asymetric Key Pair
2. ... Sends the Public Key to CA

PKI Based SSO

1. User Generates Asymetric Key Pair
2. … Sends the Public Key to CA
3. … Authenticates Himself with CA

PKI Based SSO

1. User Generates Asymetric Key Pair
2. ... Sends the Public Key to CA
3. ... Authenticates Himself with CA
4. ... Receives a Certificate Signed by CA

PKI Based SSO

1. User Generates Asymetric Key Pair
2. ... Sends the Public Key to CA
3. ... Authenticates Himself with CA
4. ... Receives a Certificate Signed by CA
5. SP Verifies the Certificate

Federated SSO Systems

- Centralized SSO are Limited to a Single Environment

Federated SSO Systems

- Centralized SSO are Limited to a Single Environment
- Main Idea: Local Credentials Should be Accepted by a Foreign Domain

Federated SSO Systems

- Centralized SSO are Limited to a Single Environment
- Main Idea: Local Credentials Should be Accepted by a Foreign Domain
- How to Esstablish a Trust Relationship?

Circle of Trust

- Service Providers Have to Trust Each Other

Circle of Trust

- Service Providers Have to Trust Each Other
- Technical Implementation

Circle of Trust

- Service Providers Have to Trust Each Other
- Technical Implementation
- Business Contracts

Identity Provider

- Central Identity Management within a Domain

Identity Provider

- Central Identity Management within a Domain
- or Use Serveral IP Each Trusting Each Other

Identity Provider

- Central Identity Management within a Domain
- or Use Serveral IP Each Trusting Each Other
- Similar to Circle of Trust

Identity Federation

- A Users Identity is Managed by an IP

Identity Federation

- A Users Identity is Managed by an IP
- Protection of Private Data

Identity Federation

- A Users Identity is Managed by an IP
- Protection of Private Data
- Federated Identity

Definition of criteria

- Usability

Definition of criteria

- Usability
- Security

Definition of criteria

- Usability
- Security
- Performance

Definition of criteria

- Usability
- Security
- Performance
- Scalability

Definition of criteria

- Usability
- Security
- Performance
- Scalability
- Compatibility

Definition of criteria

- Usability
- Security
- Performance
- Scalability
- Compatibility
- Maintenance

Definition of criteria

- Usability
- Security
- Performance
- Scalability
- Compatibility
- Maintenance
- Deployment

Categorization of single sign-on systems

	Pseudo SSO	Centralized SSO	Federated SSO
Usability	-	○	+
Security	○	+	○
Performance	-	○	○
Scalability	-	+	+
Compatibility	-	*	*
Maintenance	-	○	+
Deployment	+	-	-

Table: Categorization of single sign-on systems

Overview of single sign-on products

- Kerberos

Overview of single sign-on products

- Kerberos
- PKI Based SSO

Overview of single sign-on products

- Kerberos
- PKI Based SSO
- shibboleth

Overview of single sign-on products

- Kerberos
- PKI Based SSO
- shibboleth
- Microsoft Passport

shibboleth

- federated single sign-on system

shibboleth

- federated single sign-on system
- open source

shibboleth

- federated single sign-on system
- open source
- based on SAML

Components of shibboleth

- identity provider

Components of shibboleth

- identity provider
- service provider

Components of shibboleth

- identity provider
- service provider
- WAYF

Conclusion

- no "winner"

Conclusion

- no "winner"
- find the right system

Questions?

Thank you for your attention!