THE INTEROPERATION BETWEEN CASIDP AND InCommon etc.

JIWU JING
OUTLINE

- Introduction of CASIDP (CAS’s IDP)
- Concerns on the CASIDP’s Interoperability
- An Approach of Interoperation Project
CASIDP System

- Identity Management System
  - In the future (100+ institutes, 100,000+ users)

- Single sign on
  - Now (100+ applications, public services and private applications)

- Authentication and authorization
  - Security Policies

- X.509 Certificate Support
  - Provide certification services
  - Accept third party certificates
CASIDP Characteristics

- Using Chinese cryptographic algorithms, include SM2, SM3 and SM4
  - No DES, Sha1 and AES
  - RSA are used sometimes
- A light-weighted single-sign-on protocol is implemented
  - Simpler than SAML
- Light-weighted Tree-based system managing users and applications
  - Simpler than LDAP
- Privacy preserve mechanisms
  - CASIDP don't provide user information to applications without user’s permission, include the organization he belongs
**Typical Authentication Flow**

1. User Access an Application
2. Redirect to IDP agent for Authentication
3. User Log in to CASIDP
4. The Agent provide a Handle and some user attributes to the Application

The Agent connect to CASIDP for Synchronization
OUTLINE

- Introduction of CAS’s IDP (CASIDP)
- Concerns on the interoperability with other IDP
- An approach of interoperation project
Concerns on Interoperability

- Algorithm
- Protocol
- Security concern
- Service configuration
PROBLEM1: ALGORITHM

- CASIDP uses Chinese Standard Cryptographic Algorithm:
  - SM2(signature algorithm)
  - SM3(Hash algorithm)
  - SM4(Block cypher algorithm) and
  - RSA is used sometimes

- Other IDPs and service providers use RSA, SHA1 and AES.

- For certificate, we do not use VeriSign etc. as root.

- Key exchange with other IDP needed
- A Gateway may be used to interpret different algorithm
PROBLEM2: PROTOCOL

- CASIDP uses a light weighted protocol
  - Comparing with SAML, we have less delay and less processing time.
- Other IDP uses standard protocol: SAML

- A Gateway may be needed for transformation of protocol data
Problem 3: Security Policies

- CASIDP provide several security policies for different login method and terminal environment
  - User’s Rank
  - USB key with digital certificate (SM2 algorithms)
  - Mobile Authentication Pin Code
  - User name and Password

- Policies can be:
  - Used by CASIDP for Application Authentication
  - Used by Application for authorization

- Are the policies interoperable?
Problem 4: Service Configuration

- CASIDP allows application to select its users from the directory
  - Not all the users are permitted
- CASIDP allows application to select security policies
  - Depends on the user's rank, login method, etc.
- CASIDP sent user's attributes to application for its authorization when permitted by the user
  - E.g., Student or faculty?
OUTLINE

- Introduction of CASIDP (CAS’s IDP)
- Concerns on the CASIDP’s Interoperability
- An Approach of Interoperation Project
To be successful

- We should let people know that the interoperation is very secure and their privacy are well preserved
  - Applications will not compromise
  - User information are under control
- We shall provide capabilities to the SPs and users
  - More configuration items
  - Audit all cross domain authentication
  - Easy to Disconnect
AN APPROACH FOR INTEROPERATION

Identity Federation Gateway

InCommon

CAS

CAS APP

CAS APP

CAS APP
IDENTITY FEDERATION GATEWAY

- View from the side of Incommon
  - Act as an IDP
  - Support SAML
  - Use RAS and SHA1 or SHA2
  - Use policies in InCommon

- View from the CAS side
  - Act as a sub tree of users and applications
  - Support CAS light-weight protocol
  - Use SM2/SM3 algorithm
  - Support security policy of CAS

- Other functions
  - Provide detailed identity federation audit
INTEROPERATION FLOW (e.g. CAS USER ACCESS IN COMMON SP)

1. User Log in to CAS IDP
2. User Access InCommon SP
3. Redirect the request to the gateway
4. The Gateway get a token CAS IDP which provide the user’s Identity and attributes
5. The Gateway provide a Handle to SP
6. The SP request user Attributes from the gateway

Identity Federation Gateway

Handle

Attribute
INTEROPERATION FLOW (E.G. INCOMMON USER ACCESS CAS APP)

1. User Access CAS APP
2. Redirect The request to CAS IDP
3. The Gateway act as SP and use the standard InCommon procedure to get the handle and attribute of the user
4. The Gateway generate a Identity federation token To CAS IDP
5. The CASIDP generate A token to app, which Will open the access to The user

APP

The Gateway act as SP and use the standard InCommon procedure to get the handle and attribute of the user.
THANK YOU