Security Requirement and Implementation Solution for e-Gov System

Chuan Liu
liuchuan@tongtech.com

TongTech Co., Ltd
2006-11
Agenda

• Introduction of E-Gov (Platform)
• Requirement of Identity Management & Authorization
• Implementation Solution
The Functions of e-Gov platform

- Objects
  - Service support for e-Gov application

- Functions——Support Data Sharing and Exchanging
  - Data Exchanging
  - Uniform Portal
  - Basic business services: Authentication & Authorization & Resource navigation
  - Connect to Sharing Database, Database of Government Agencies, and Application System

- Two-level Structure of Municipal and County

- Service Platform compliant with SOA
  - Single business services
  - Composite services
  - Business process services
E-Gov Service Platform Architecture

- Portal
  - Authentication
  - Authorization
  - Navigation

- Data Exchange Platform
  - WS-Gateway
  - Service
  - Service
  - Service

- Other Platform

- Application
  - Share Database
  - Database
  - Application

- Consumer
  - Provider
Existing Foundation for Security

- Releasing certification from uniform CA centre, providing authorization service
- Security functions in existing applications
  - No Uniform Security Solutions
  - Providing Username/Password authorization
  - Providing Role-based Right Management
Requirements of Authentication & Authorization

- Existing Security Management Services should be integrated into the Service Platform
  - Personal certification released by Authentication center
  - Adopt existing Authentication & Authorization Mechanism

- **Single Sign-On (SSO)**
  - Log in Only Once on Portal
  - Log in with Certification or Username/Password
  - Same Log-in Mechanism for County and Municipal Level Platform

- Providing Organization Structure Management and Role Management

- Providing Federal Authentication Management
  - Access authorization service once when log-in
  - Authorization information used by different service provider
Functions Implemented

• Base on SAML standards
• Realize uniform log-in management and authorization management services
  – Support SSO, simplifying authentication and authorization management.
• Supporting Dual Username/Password and Digital Certification Identity Management Mechanism
  – Digital Certification Signed and Authorized by authentication Centre
  – Cross authorization based on digital certification for IM in two-level Security Zone
• Mapping uniform authorization to existing right management information, supporting Right Management in Legacy system
Features of SAML

• XML-based framework
  – Describing and exchanging security information between on-line business partners.
  – Security information is expressed in the form of portable SAML assertions that applications working across security domain boundaries can trust.
  – The OASIS SAML standard defines precise syntax and rules for requesting, creating, communicating, and using these SAML assertions.
SAML usage scenario

• Single Sign-On
  – Within platform
  – Between platform

• Federated identity
  – Single service in platform
  – Process in platform
  – Services between platforms
Key of the Implementation

• Different implementations for in a platform and between platforms/partners
  – A SAML-like (simplified) approach to address the requirements – SSO and Federal Authentication in the platform.
  – Real SAML compliant implementation to support the Authentication & Authorization across platforms and/or partners.

• No Authorization decision statement in SAML.
  – Just authentication assertions involved in current (primary) phase.
  – Artifact Resolution Protocol not supported.
The Architecture
The Architecture

1. Portal
   - Login & authorization

2. Data Exchange Platform
   - Authenticating
   - Authorization

3. Service
   - Verify signature
   - Information translate
   - Access check
   - Service

4. WS-Gateway
   - Other Platform
   - HTTP/SOAP
Preliminary Preparing

• Service defines open and limited roles and right information

• Release security certificate to officials and platform

• Mutual authorization between county and municipal platform (exchange public key)

• Definition of role and right information on platform
  – Simplify right management
  – Objects includes single service and process service

• Authorization for officials
Scenario 1

- Officials/enterprise users in county platform use services in the platform
Scenario 1

- Officials/enterprise users in county platform use services in the platform
Scenario 1

- Officials/enterprise users in county platform use services in the platform
Scenario 1

- Officials/enterprise users in county platform use services in the platform
Scenario 2

- Authentication information be transferred by process service automatically
Scenario 3

- Usage of services in different platforms

![Diagram showing the flow of services and data between different platforms and services.]

1. Portal
2. SAML MSG + DATA
3. DEP
4. SAML MSG  + DATA
5. WS-Gateway

Service 1
- Verify signature
- Information translate
- AUTH MSG + DATA
- Access check
- Business Service 1

Service 2

Other Platform

Partner's Web Service
Thanks