Security/VO Management
– Interim report of PKI deployment in 7 Computing Centers –

Toyokazu Akiyama*, Yuuichi Teranishi, Shinji Shimojo*
{akiyama, teranisi, shimojo} @cmc.osaka-u.ac.jp

Cybermedia Center, Osaka University
NICT Osaka JGN2 Research Center*

National Institute of Advanced Industrial Science and Technology
Yoshio Tanaka
yoshio.tanaka @ aist.go.jp

Ubiquitous Software Development Division, NEC
Ayako Komatsu
a-komatsu @ ay.jp.nec.com
Background

- 7 Computing Centers in Japan

- Cooperative activities
  - Authentication Workshop
    - Considering Campus-Wide authentication infrastructure
  - Grid Computing Workshop
    - Considering computing service federation among Computing Centers

- NAREGI and National Institute of Informatics (NII)
  - Support activities of 7 Computing Centers from technical and budgetary aspects
Wireless LAN and information wall socket roaming service

Security and dependable federation infrastructure

Web and e-learning contents sharing and students’ credit transfer service

Federation of device base authentication infrastructure

PKI base authentication infrastructure must be deployed as a replacement of password base authentication infrastructure

Computing center federation using Grid Technologies

Secure and dependable federation infrastructure

Communications Center

Osaka Univ. Cybermedia Center

Hokkaido Univ. Information Initiative Center

Tohoku Univ. Information Synergy Center

Nagoya Univ. Information Technology Center

National Institute of Informatics

Computing center federation using Grid Technologies
Today’s contents

• Current status report on the consideration for PKI deployment
  – Relation to the VO Management considered in Grid Community
  – PKI management
    • Private CA management
    • CA federation
  – Current consideration for the implementation of PKI base authentication and authorization system
Assumption (1/2)

- Current situation
  - Private CA is becoming common in enterprise authentication infrastructure
  - Office management systems are the first application to use PKI in university information systems
  - Authentication federation among organizations should be the next issue
    - While it should be considered from the beginning...
  - Current PKI used in Grid Community is not enough secure for office management system
    - e.g. Private keys are stored on disks
Assumption (2/2)

- Assumptions for our consideration
  - Each university has own private CA/RA for the office management system
  - Physical security is not discussed here but device base security is assumed
    - e.g. User key store: USB key, Smart Card
    - CA key store: HSM and restricted room
  - Personnel Department and Local Administration Department can trace the holder of the issued certificate in the organization
Definition of “VO Management” (1/2)

- Virtual Organization (VO)
  - Temporary organization constructed across real organizations
  - Can be managed by attributes of persons and resources belonging to the VO
  - e.g. managing with LDAP attributes
    - CN=Toyokazu Akiyama,
      Affiliation="/C=JP/ST=Osaka/O=Osaka University/OU=Cybermedia Center"
    - CN=Toyokazu Akiyama,
      Virtual Affiliation="/O=PRAGMA"
Definition of “VO Management” (2/2)

- **VO Management**
  - Implement authorization mechanism based on the attribute of the target object for all resources
  - Define the management policy of VO attributes
    - VO description format, VO attribute assignment policy
    - *e.g.* Web application and Web services (SAML)
      - SAML has the authentication and authorization mechanism based on authentication authority, attribute authority and policy decision point
      - If the application developer defines proper enforcement policy based on users’ VO attributes and its management policy is clarified, VO in SSO for Web application and Web services is considered under the control of VO Management.
PKI management

- Private CA management
- CA federation
Private CA management (1/4)

- Separate target identity management and attribute management
  - Certificate is usually defined as follows:
    - DN=”/C=JP/ST=Osaka/O=Osaka University/OU=Cybermedia Center/CN=Toyokazu Akiyama”
  - If attributes (in the above case, “affiliation”) are included in the certificate, then the certificate should be reissued when the target is ordered for an internal transfer
  - Define a unique name space in the organization for CN and remove attributes from certificate:
    - DN=”/C=JP/ST=Osaka/O=Osaka University/CN=k050001”
    - DN should be unique in the world for ID federation
    - CN name space should have guest account space
      - e.g. CN=g050001
Private CA management (2/4)

- DO NOT distribute the organization CA Certificate to the trust CA list for an end user
  - Certificates installed in the trust CA list for an end user are used to authenticate the server managed not only in your organization but also in the other organization
  - If your organization CA Certificate is installed to the trust CA list for an end user, you may be complained against due to an inappropriate certificate issuance from your CA to the criminal site
    - CPS should define the coverage of the assurance
    - CA server should be required high level security
  - Currently, certificates issued by a third party (commercial CA) is better to be used for public servers
Private CA management (3/4)

- Entities in CA management explanations
  - Certificate authority and registration authority
    - For simplicity does NOT consider division of CA and RA
    - The private key pairs with the CA certificate is stored via secure device
  - CA certificate (public key)
    - The color of characters shows the organization where the CA is managed
    - The color of sign shows the issuer CA
  - End entity (user or server) certificate (public key)
    - The color of characters shows the organization where the user belongs to
    - The color of sign shows the issuer CA
  - A server requiring client (user) authentication
    - The color of characters shows the organization where the server belongs to
    - The private key pairs with the server certificate is stored
  - A client requiring server authentication
    - The color of characters shows the organization where the client belongs to
    - The private key pairs with the user certificate is stored via secure device
Private CA management (4/4)

- Important points in CA management
  - Separate server authentication and client authentication
    - Assume two types of the user, a system administrator and an ordinary user
  - CA certificate distribution
  - Trust CA selection
    - Each CA has different management policy

Osaka University CA

Third Party CA (e.g. NII CA, VeriSign CA)

※ In Windows, trusted CA lists are distributed by Windows Update mechanism using Certificate Trust List (CTL) format from Microsoft Web site.
CA federation (1/8)

- CA federation model
  - Trust list CA model (Application level federation)
  - Bridge CA model (CA level federation)
CA federation (2/8)

- Trust list CA model (Application level federation)
  - CA certificate of your organization
    - Off-line secure distribution path is required between CA/RA management department and service provider department
  - CA certificate of a federated organization
    - End entity (service provider) chooses trust CAs and downloads from the distribution points
      - Peer-to-peer distribution
      - Hierarchical distribution
  - CRL can be distributed in the same manner
CA federation (3/8)

- Application level federation (peer-to-peer)
CA federation (4/8)

- Application level federation (hierarchical)
CA federation (5/8)

• Application level federation
  – Benefits
    • Trust anchor can be chosen flexibly by service provider
    • Certificate policy agreement is not necessary between the CA certificate distributor and the relying party
      – Different management level CA can be used together
  – Issues
    • There is no standard protocols
      – How to operate the federation should be defined
    • When the number of federated organization is increased, trust anchor selection becomes difficult for the service providers
    • The coverage of assurance for CA certificate distributor should be clarified
CA federation (6/8)

- Bridge CA model (CA level federation)
  - The organization who wants to join the federation exchanges mutually signed CA certificate with the bridge CA organization
    - This requires CPS agreements between the organization and the bridge CA organization
  - End entity (service provider) chooses trust CAs and downloads from the distribution points
CA federation (7/8)

- CA level federation

1. off-line

Osaka University CA

CA/RA

CA CERT
sign

CA CERT
sign

Server

CA CERT
sign

CA CERT
sign

CA CERT
sign

Kyoto University CA

CA/RA

CA CERT
sign

CA CERT
sign

Server

CA CERT
sign

CA CERT
sign

CA CERT
sign

NII CA

2. mutually signed certificate

3. on-line

4. on-line

2. mutually signed certificate

4. on-line

3. on-line

1. off-line
CA federation (8/8)

- CA level federation
  - Benefits
    - CA level federation is already standardized
    - Service provider’s Trust anchor selection cost is reduced
      - This may be a trade-off between selection cost and selection flexibility
  - Issues
    - Trust anchor can be chosen only from the CA level federated organization
      - The meaning of the CA level federation and how to make the certificate policy agreement between federated CAs should be investigated
    - Multiple federation community should be considered when all the organization can not get together
      - The possibility of hybrid federation model should be considered
Sample implementations

- **Wireless LAN**
  - 802.1x + EAP-TLS

- **VPN**
  - SoftEther CA
Sample implementation (1) (1/5)

- **Wireless LAN**
  - 802.1x authentication mechanism
    - EAP-TLS supports client certificate authentication
  - RADIUS + LDAP
    - EAP function is realized by RADIUS server
    - Attribute management is realized by LDAP server
    - RADIUS server can authorize an account by its attributes obtained from LDAP server
Sample implementation (1) (2/5)

- **Attribute management**
  - **Root LDAP server**
    - Attributes of each target are registered when the certificate is issued to the target
    - Attributes used commonly in the organization are registered
  - **Branch LDAP server for each department**
    - Replicate attributes managed by Root LDAP server
    - Add independent attributes for the department if necessary
- **Name space management**
  - Attribute name decision rule is required
    - Root LDAP server: Common_Affiliation
    - Branch LDAP server: DeptA_Affiliation
Sample implementation (1) (3/5)

- Simple case

Issued certificate is registered with its attributes (attribute registration service should be implemented)

Root LDAP server

Mirror or Sync Common Attributes

Authentication with SASL Encryption with TLS

Branch LDAP server A

Branch LDAP server B

Common Attributes
C-ATTR1
C-ATTR2

Independent Attributes
SUB-ATTR1

Attributes mapping
C-ATTR1 to Auth1
SUB-ATTR1 to Auth2

Wireless LAN Access point

Pre-shared key

RADIUS server

Pre-shared key

Authentication with EAP-TLS
Policy decision with LDAP attributes

Wireless LAN Access point

Client

CAC

CA Certificate

SC

Server Certificate issued by ORG1 CA

UC

User Certificate issued by ORG1 CA

CAC

CA Certificate of third party CA

SC

Server Certificate issued by third party CA
Sample implementation (1) (4/5)

- Federation case

  CA/RA for ORG1
  Guest account registration service

  Root LDAP server
  Common Attributes
  C-ATTR1
  C-ATTR2
  Register from ORG2 network with SAML authentication

  Mirror or Sync
  Common Attributes
  Authentication with SASL
  Encryption with TLS

  Branch LDAP server A
  SC CAC
  Independent Attributes
  SUB-ATTR1

  Branch LDAP server B
  SC CAC
  Attributes mapping
  C-ATTR1 to Auth1
  SUB-ATTR1 to Auth2
  Authentication with SASL
  Encryption with TLS

  RADIUS server
  Pre-shared key
  Authenticate with EAP-TLS
  Policy decision with LDAP attributes

  Wireless LAN Access point
  CAC UC
  Pre-shared key

  Wireless LAN Access point
  CAC UC

  Issued certificate is registered with its attributes (attribute registration service should be implemented)

  ORG1 CA Certificate
  Server Certificate issued by ORG1 CA
  User Certificate issued by ORG1 CA
  CA Certificate of third party CA
  Server Certificate issued by third party CA
  ORG2 CA Certificate
  User Certificate issued by ORG2 CA
Sample implementation (1) (5/5)

- VO Management
  - Target attribute management interface should implement VO Management functions
    - LDAP server management interface should have the function
      - e.g. Guest account registration service
  - VO organizer should manage attributes of related targets
    - VO organizer should have ability to define policies on the attribute management interface
    - VO attribute management policy must be defined in PMA
Sample implementation (2) (1/3)

- **VPN service**
  - **SoftEther CA** (commercial VPN software)
    - Layer 2 VPN service over multiple protocols
      - Supported protocols are TCP/IP, HTTPS, SOCKS, SSH
    - Virtual Interface and Virtual HUB (authentication server)
    - Virtual HUB can provide multiple segment (zone)
    - Client certificate authentication support
  - **PKCS#11** is not supported yet (original format to write certificate and key)
    - Asking to support PKCS#11 and CryptAPI
  - **802.1x** is not supported yet (original authentication mechanism)
    - Asking to support 802.1x EAP-TLS and RADIUS authorization mechanism
Sample implementation (2) (2/3)

- Possibility of L2 VPN service with VO Management
  - Resources that do not support Grid mechanism, such as instrument controllers, can be accessed securely from remote sites
  - Legacy computing and data sharing environment may be used without modification across multiple clusters
    - e.g. MPI, Linda, etc (Computing), NFS, FTP, etc (Data sharing)
- Address conflict must be resolved
- Performance evaluation is necessary
Sample implementation (2) (3/3)

- Address conflict resolution
  - IPv6 address can be one of the solutions
    - Multiple address allocation to one node is supported
    - Address selection strategy is already defined (RFC3484)
    - Local IPv6 address is easy to use in VO
  - Problems
    - Host auto configuration should be considered along with host name resolution
    - Check the IPv6 supporting status of legacy applications
Conclusion

• Deployment of PKI and VO Management is essential in Grid Computing technologies
• Attribute base authorization mechanism should also be investigated for other applications

Acknowledgement

• I would like to thank the members of the following organizations for joining the discussion of Security/VO Management
  – NAREGI
  – Authentication Workshop (7 Computing Center, NII)
  – SecureNet Project (Cybermedia Center)
  – WIDE Project
  – JGN II Project (NICT)
  – Jenning King (proof reading)