PKI in SAP

Stefanie García Laule
SAP AG

Presentation Overview

- Authentication
- Single Sign-On
- Trust Center Service
- Digital Signatures
### Authentication Mechanism

**External Authentication**
- User ID / password
- X.509 certificates
- NTLM
- LDAP bind
- Radius
- ...

**Pluggable Authentication Adapter**

**SAP Enterprise Portal**

**Applications**

---

### Authentication

- **X.509 Digital Certificate (SAP Passport)**
  - SSL client authentication

- **Logon ticket**
  - Digitally signed by Web Application Server

- **Pluggable Authentication Service (PAS)**
  - Use external authentication mechanisms

---

© SAP AG 2004, Title of Presentation, Speaker Name
Logon Ticket

The logon ticket contains public information:
- User ID
- Validity period
- Issuing system
- Digital signature

Therefore we can offer a library which can be linked to other systems. These systems can verify the user’s logon ticket and use the stored information for their own logon.

SSO Using Logon Tickets

Digitally signed logon ticket
Via encrypted channel

*SSL (Secure Sockets Layer) and SNC (Secure Network Communications) are used to secure the communication path between the Web browser and the SAP System.
**Products Available (Jan 2001)**

- **Computer Associates**
  - eTrust Single Sign-On™

- **CyberSafe**
  - TrustBroker Security Solution for R/3™

- **Entrust Technologies**
  - Entrust/SNC™

- **RSA Security**
  - Keon Agent v. 4.5 for R/3™

- **SHYM Technology**
  - PKEnable™

- **SECUDE GmbH**
  - SECUDE for R/3™

- **SAP Crypto Library**

---

**SSO Using X.509 Client Certificates**

- **X.509 Client Certificate** (SAP Passport)
  - SSL client authentication

- **Web server**
  - W Gate
  - A Gate
  - User ID

- **SSL with mutual authentication**

---

THE BEST-RUN E-BUSINESSES RUN SAP
Pluggable Authentication Service (PAS)

- Authentication using an external authentication service
  - Windows NTLM protocol
  - Windows User ID / password checking using the domain controller
  - LDAP bind
  - Radius / SecureID
  - ...
- After authentication, the user is issued a logon ticket for use with SAP Services

Pluggable Authentication Service

1. Authentication (user ID and password)
2. User external ID mapping table (USREXTID)
3. Web Application Server
4. SAP System user ID
5. External Authentication Server
6. User ID
7. SAP System user ID
8. Web Application Server

https://host1.mycompany.com/scripts/wgate/<service>/
https://host1.mycompany.com/scripts/wgate/sapwa/
**Presentation Overview**

- Authentication
- Single Sign-On
- Trust Center Service
- Digital Signatures

**Single Sign-On and Impersonation Mechanisms**

**Authentication Mechanisms**
- Certificate
- Smart card
- Radius
- User name/password

**SAP Enterprise Portal**
- Ticketing
- Account aggregation

**Application Access**
- Single sign-on
- Impersonation
Verifying the Logon Ticket

Step 1: Verify the digital signature provided with the logon ticket.

Step 2: Check the Access Control List that contains the names of trusted Web Application Servers and check the validity time.

Step 3: Logon using the user ID which is stored in the logon ticket. No password necessary.

SSO to Non-SAP Components Using Logon Tickets: Summary

The non-SAP component must:

- Verify the Web Application Server’s digital signature
  - Use the SSO shared library
- Make sure the ticket has been issued by the designated Web Application Server
  - Maintain an ACL
- Map the User IDs

Availability:
- [www.sap.com/miniapps](http://www.sap.com/miniapps) > Development Zone
**SAP Trust Center Service: Enrollment Process**

1. Log on using SAP user ID and password and initiate the SAP Passport request.
2. Specify naming convention and trigger key generation.
3. Web browser generates key pair and sends the SAP Passport request.
4. Send approved certificate request.
5. Verifies naming conventions and issues certificate.
6. Log on using the SAP Passport.

**Presentation Overview**

- **Authentication**
- **Single Sign-On**
- **Trust Center Service**
- **Digital Signatures**

**Note:** Available at GA date.
New: Digitally Signed Documents

- Private key
- Public key

"Document content"

- Document unchanged
- Identity of the signer
- Legal certainty

Internet

Sign

Verify

(Register)

Trust

CA

Secure Store & Forward (SSF) Interface

ABAP

Applications using digital signatures

ABAP

Process Planning
HTTP Content Server
Public Sector

Application server signs (SAPSECULIB)

Signing in SAP GUI for Windows front end (Software Partner Program SPP)

Signing in Web browser (IE: ActiveX-Control, Netscape: Java-Script)
Integrating Digital Signatures in Applications

1. Create document (application)
2. Show document (application / SSF >= Rel. 6.10)
3. Create signature (SSF >= Rel. 4.0)

Very important! To be legally binding, certain requirements must be met.

Signing Documents in the Web Browser
Digitally Signed Documents in Batch Processing

SAP application

IDOC Connector

For example, invoices in IDOC format

Conversion in XML/EDIFACT

Create signature

S/MIME PKCS#7 (XML signature)

Receiving Digitally Signed Documents

S/MIME Connector

Business Connector

Archive

For example, invoices in IDOC format

Conversion into IDOC

SAP application

IDOC TYPE: Invoice

1. Verification of digital signature

2. Archive

3. Conversion into IDOC
**Receiving Digitally Signed Documents**

- **MIME file** contains the electronic invoice in PKCS#7 (XML with digital signature and certificate) and PDF format.
- **PKCS#7**
  - **Verify digital signature**
  - **Yes**: Convert XML into IDOC and send to SAP System and archive PKCS#7 and PDF
  - **No**: Return to sender with message

**Business Connector**

**Verification of Digital Signature**

1. **Verify digital signature**
2. **Is the certificate revoked by CA?**
   - **No**: Return to sender with message
   - **Yes**:
     - **Is the signature value OK?**
       - **No**: Return to sender with message
       - **Yes**: Convert XML into IDOC and send to SAP System and archive PKCS#7 and PDF
1. Certificate Revocation List (CRL)

Trust Center Service

CA

Issue CRLs

Revocation List

Customer landscape

Authentication / digital signature

Is the digital certificate valid?

Verification for Revocation I

2. OCSP Responder (Online Certificate Status Protocol)

Trust Center Service

CA

Issue CRLs

OCSP Responder

Customer landscape

Authentication / digital signature

Is the digital certificate valid?

Verification for Revocation II
3. OCSP Responder & CRLs

Trust Center Service

Customer landscape

Authentication / digital signature

Is the digital certificate valid?

Secure Business in Open Environments

Questions?

Stefanie García Laule
SAP AG

SAP Security Competence Team
E-Mail: Security@sap.com
URL: http://service.sap.com/Security