Authentication and Single Sign-On

Patrick Hildenbrand
NW PM Security, SAP AG
Agenda

Authentication and Identities

Authentication with SAP

- in a Web Based Scenario
- At the SAP GUI for Windows

Summary
In computer security, authentication is the process by which a computer, computer program, or another user attempts to confirm that the computer, computer program, or user from whom the second party has received some communication is, or is not, the claimed first party.
Single Sign-On (SSO) is a specialized form of authentication that enables a user to authenticate **once** and gain access to the resources of multiple software systems.
Why Use Single Sign-On?

**Typical situation**
- In a complex system landscape an employee has many user IDs with different passwords
- Different procedures for each system to roll-out, reset and change new / existing passwords
- Users find continuous password changing for many systems annoying

**Problems**
- High administration cost and effort
- Security risk: Users write passwords down and store them where they can easily be found

**Solution: Single Sign-On**
- Users only have to remember one password to gain access to every system
- Administration costs and efforts are drastically reduced
What the User Wants ...

Authenticate once

Portal
WebAS
ITS

Access

Intranet
CRM

ERP
Internet

Groupware
Other...
What the Administrator Wants ...

Central user management
- Single point of administration
- Assign user rights in various applications with one keystroke
- Lock or delete users centrally

Central user repository
- Avoid redundant user information
- Easy De-Provisioning
Agenda

Authentication and Identities

Authentication with SAP

- in a Web Based Scenario
- At the SAP GUI for Windows

Summary
Web-Based Authentication Methods

- Anonymous/guest access
- User ID / password
  - Form-based *
  - Basic authentication *
- X.509 digital certificates
- SAP Logon Tickets
- External authentication methods
  - HTTP header variable authentication
    (not ABAP except for X.509 certificate information forwarding)
    - Enterprise Access Management - EAM
  - Security Assertion Markup Language (SAML – only Java)
  - Through Pluggable Authentication Services (PAS – only external ITS)
  - Through Java Authentication and Authorization Services (JAAS – only Java)

Java
SAP WebAS 640 Java or SAP Enterprise Portal 6 > SP3
* Only authentication, not Single Sign-On
X.509 Client Certificates – SSO Process

- Authentication occurs using SSL with mutual authentication
- User possesses a public / private key pair and public-key certificate

Access

X.509 Client Certificate

SSL

Intranet  CRM

ERP  Internet

Groupware  Other...
Authentication and SSL with X.509 Certificates

- Mutual authentication between Alice and the server
- The SSL – Process:

Client sends „Hello“-message to server
Server sends his certificate and asks for client cert.
Sends back confirmation
Session established

...using symmetric encryption

Mutual authentication between Alice and the server

The SSL – Process:

Alice

Client sends „Hello“-message to server
Server sends his certificate and asks for client cert.
Sends back confirmation
Session established

...using symmetric encryption
X.509 Certificates

- X.509 certificates are used for Secure Sockets Layer (SSL) based communications:
  - Internet standard for secure HTTP connections
  - Provides for server, client or mutual authentication and encryption
  - Uses both symmetric and public-key encryption for protection

- X.509 certificates (“digital certificates”) can be used both for initial authentication and for successive Single Sign-On

- Each certificate includes:
  - Name
  - CA name
  - Validity period
  - Public key
Obtaining a X.509 Certificate

Digital certificates must be X.509v3 compliant

Various options possible:

- Using SAP Trust Center Service
  - For SAP users only
  - Free of charge
  - Portal server acts as Registration Authority (RA)

- Setting up internal PKI system
  - Buy software from CA product vendor

- Using external PKI system
  - Contract with Trust Center Service
Log on using SAP user ID and password and initiate the SAP Passport request

Specify naming convention and trigger key generation

Web browser generates key pair and sends the SAP Passport request

Log on using the SAP Passport

Send approved certificate request

Verifies naming conventions and issues certificate
SAP Logon Tickets – SSO Process

Initial logon

Portal
WebAS
ITS

Access

Intranet
CRM

ERP

Internet

Groupware
Other...

SAP Logon Ticket

© SAP AG 2005, Authentication and Single Sign On / Patrick Hildenbrand / 15

THE BEST-RUN BUSINESSES RUN SAP™
Example of an HTTP Request

GET /someresource HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, [ ... ], /*
Referer: https://some.host.domain/some/other/resource
Accept-Language: en,de;q=0.5
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
Host: nw-portal.wdf.sap.corp
Connection: Keep-Alive
Cookie: saplb_*(J2EE6527200)6527250; PortalAlias=portal;
MYSAPSSO2=AjExMDAgAA5wb3J0YWw6ZDAzMzA5YgAE2Jhc2ljYXV0aGVudGljYXRpb24
BAAdEMDMzMDk5AgADMDAwAwADTldUBAAMMjAwNTA5MDIwNjE0BQAEAAAACAoAB0Q
wMzMwOTn%2FAPUwgfIGCSqGSIb3DQfHApqCB5DCB4QlBATELMakGBSsOAwlaBQAwCw
YJKoZIhvcNAQcBMYHBMIG%2BAgEBMBMWdJEMMAoGA1UEAxMDTldUAgEAMAkGBSsO
AwlaBQCGXTAYBgkqhkiG9w0BCQxMwYJKoZIhvcNAQcEBMBwGCSqGSIb3DQfJBEFPw0
wNTA5MDIwNjE0NDRaMCMGCSqGSIb3DQfJEJBDEWBBQ28IoAPAV2KfBJR18EILxaNenHzA
JBgcqhkJOOAQDBC8wLQIUaaWKYY4%2BCT26P07coHVYP63eCkCFQCLt0ERDvDKCpog8
9q5n%2BapQQCw%3D%3D;
JSESSIONID=(J2EE6527300)ID6527350DB307014776305034697End; sap-
ssolist=O3I9chdkZjA5njJfY3BwXzQ0
What is a SAP Logon Ticket

- SAP Logon Ticket is represented as cookie in the Browser
- Content of the SAP Logon Ticket is BASE64 encoded
- SAP Logon Tickets contain:
  - User ID(s)
  - Authentication scheme
  - Validity period
  - Issuing system
  - Digital signature
  - SAP Logon Tickets do NOT contain any passwords!

Problems?
- SAP Note 701205 (EP6.0: Single Sign-On using SAP Logon Tickets)
- SAP Note 654982 (URL requirements due to Internet standards)
SAP Logon Tickets – Prerequisites

Prerequisites

- At least same user IDs in connected backend systems (portal user ID can be different)
- In case portal user ID is different than backend user ID, you need to maintain a user mapping for the "SAP Reference System"
- Trust configured
  - Public key certificate of issuing system is available in verifying system (necessary for verification of digital signature)
  - Trust access control lists maintained (ABAP: strutsso2)

SAP Reference System User Mapping

- Standard user mapping functionality
- PLUS: Retrieval of user ID from LDAP Directory Server
SSO to Non-SAP Components Using SAP Logon Tickets

Initial logon → SAP Logon Ticket

1. 3rd party application
2. Ticket Verification Library SAPSSOEXT
3. Security product (SAPSECULIB)
4. Public address book (if not SAPSECULIB)
5. mySAP.com user ID

Access Control List
Workplace server <SID> <client>

Portal
WebAS
ITS

Access
Ticket Verification for Non-SAP Components

Web Server Filter
- SSO with SAP Logon Tickets to Web applications
- Application needs to support authentication with an HTTP header variable

Web Server Filter with Delegation for Windows Server 2003
- SSO with SAP Logon Tickets to a Microsoft Web-based application

Java Ticket Verification Library
- SSO with SAP Logon Tickets to non-SAP Java applications
- Development required

C Ticket Verification Library
- SSO with SAP Logon Tickets to non-SAP C applications
- Development required

Dynamic Link Library SAPSSSOEXT
- SSO with SAP Logon Tickets to Java and C applications
- Available for most kernel platforms
- Development required

Remark: Platform limitations may apply!
Multi Domain SSO

Recommendation:
- Use one DNS (sub-) domain for SSO purposes (→ increased security!)
- E.g. portal.sso.company.com, its.sso.company.com, ...
- Set UME property ”domainrelaxlevel” accordingly

Alternative: Configure SAP EP for multi domain SSO
- Ticket sending instances required in every domain
- Portal sends SAP Logon Ticket content via client redirects to every ticket sending instance.
- Client will get as many cookies as domains (also see SAP Note 654982)
- Configuration details:
- EP6 SP2 only supported on per project basis, see SAP note 673824
HTTP Header Authentication – SSO Process

Authentication Authority (intermediate)

Initial logon

Identity information within header variable

Access

Intranet

CRM

Internet

ERP

Groupware

Other...

© SAP AG 2005, Authentication and Single Sign On / Patrick Hildenbrand / 22
Adding the User Name Header

- The authentication takes place on the intermediate server
- The intermediate adds identity information to the request data
- The application servers get the identity information from the request data

```
GET /someresource HTTP/1.1
[ ... ]
GET /someresource HTTP/1.1
[ ... ]
HTTP-USER: MyUser
```
Integrated Windows Authentication

Initial authentication is done to the local system (Windows)

**Two methods of Integrated Windows authentication possible**

- NTLM
- Kerberos

**Requirement:**

- Applications need to run on an IIS
  or
- authentication needs to be done on an intermediate IIS (using IIS Proxy module from SAP) → available for SAP WebAS Java 6.40

Coming soon:
SAP Consulting solution for Kerberos Authentication directly on WebAS 6.40 Java
→ please contact your local SAP consulting organization
Header Based Authentication Best Practices

- Block risk of user impersonation!
  - Be aware of Header Spoofing

- Safeguard J2EE engine HTTP(S) ports from direct access by users
  - Prevent opportunity to bypass the proxy for J2EE engine access

- Configure SSL with mutual authentication between the web server and the J2EE engine
  - See documentation on ‘Using SSL with an Intermediary Server’
Security Assertion Markup Language (SAML)

SAML is a protocol for encoding security related information (assertions) into XML and exchanging this information in a request/response fashion.

SAML does not authenticate users – comparable to SAP Logon Ticket.

SAML relies for message exchange on standard security protocols like SSL, TLS and uses XML signatures.

SAML authorities produce “assertions” in response to client requests. An assertion can be either an authentication or an authorization assertion.

- Authentication assertion: piece of data that represents an act of authentication performed on a subject (user) by the authority.
- Authorization assertion: piece of data that represents authorization permissions for a subject (user) on a resource.

SAML can be used for authentication and authorization requests and assertions.

SAML is an emerging OASIS standard.
SAML – SSO Process

Authenticate once

Access

1. Call transfer URL
2. Redirect URL + artifact
3. Access
4. Pull assertion
5. Assertion
6. Resource

Authentication Authority
(Source Web Site)

Initial logon

Intranet

ERP

Internet

ESS

Groupware

THE BEST-RUN BUSINESSES RUN SAP™
Support of SAML in the SAP WebAS 640 Java

Only SAML client for authentication available at destination site is available

Support limited

- Only browser artifact scenario supported
- Digital signatures for SOAP documents are ignored
- No support for additional “Condition” elements
- The received assertion may only contain one authentication statement
- The authentication statement must contain the NameIdentifier
- AuthorizationDesicionStatement and AttributeStatement are ignored

Nevertheless SAML is strategic within SAP. In the future there will be further support for SAML.
Pluggable Authentication Service (PAS)

Requires the external (standalone) version of the Internet Transaction Server (ITS)

Provides the following authentication variants:

- Windows NT LAN Manager protocol (NTLM)
- Verifying user ID and password on the Windows domain controller
- SSL and X.509 client certificates
- Arbitrary mechanism on the Web server or an intermediate that sets HTTP header variable
- LDAP bind
- Arbitrary mechanisms provided by a partner product like
  - Radius
  - RSA SecureID
  - Netegrity Siteminder
  - ...

Windows NT LAN Manager (NTLM)

SSL and X.509 client certificates

Arbitrary mechanism on the Web server that sets HTTP header variable
Pluggable Authentication Service: AGate

Verifying user ID and password on the Windows domain controller

LDAP bind

Arbitrary mechanisms provided by a partner
Interface defined by Java Authentication and Authorization Service (JAAS) standard

As of JDK 1.4 integral part of J2SE

Access control based on user credentials

User-centric approach with two components:
- Authentication (-> login modules)
- Authorization

http://java.sun.com/products/jaas
JAAS Authentication

JAAS uses login modules for authentication

- Login modules get user information via callbacks
- SAP proprietary handlers can be used to gather additional information:
  - HttpGetterCallback – used to obtain information from the request (header/cookies)
  - HttpSetterCallback – used to attach information to the response
- Standard information available is only User/Passphrase, all other information requires a Callback
Agenda

Authentication and Identities

Authentication with SAP

- in a Web Based Scenario
- At the SAP GUI for Windows

Summary
Use SNC and external security product

- Authentication takes place outside of SAP system

Use SAP-certified SNC product

Also available:

- Windows NTLM (gssntlm.dll)
- Windows 2000 Kerberos (gsskrb5.dll)
Two Worlds: SAP GUI for Windows and Web

Traditional

SAP GUI for Windows

Secure Network Communications (SNC)

- SNC partner product
- SNC: Microsoft NTLM or Kerberos
- SAP Shortcut Method (SAP Logon Ticket)

Web

SAP GUI for HTML

X.509 client certificate

SAP Logon Ticket

Pluggable Authentication Service (PAS)

→ Use external authentication mechanisms
SSO From Web to Traditional - ITS

- Using logon tickets, ITS, and SAP Shortcuts
- Logon ticket is passed to SAP Shortcut using ITS service wngui

SAPGUI for HTML

SAPGUI for Windows

Only supported on external ITS up to release 6.10!
Using logon tickets, Enterprise Portal and SAP Shortcuts

Logon ticket is passed to SAP Shortcut using a portal iView

SSO From Web to Traditional – Enterprise Portal
Prerequisites

1) Users have the same user ID in all of the systems they access using the logon ticket. Passwords do not have to be the same in all systems.

2) The user has an account in the active user store on the SAP J2EE Engine.

3) The end users Web browsers accept cookies. In Internet Explorer 5.0, accept session cookies for the local intranet zone.

4) Any Web servers or SAP Web AS servers (to include the SAP J2EE Engine) that are to accept the logon ticket as the authentication mechanism are located in the same DNS domain as the issuing server. The logon ticket cannot be used for authentication to servers outside of this domain.

5) The clocks for the accepting systems are synchronized with the ticket-issuing system.

If you do not synchronize the clocks, then the accepting system may receive a logon ticket that is not yet valid, which causes an error.

6) The issuing server must possess a public and private key pair and public-key certificate so that it can digitally sign the logon ticket.

7) Systems that accept logon tickets must have access to the issuing server's public-key certificate so that they can verify the digital signature provided with the ticket.

8) The UMEs of the Portal and Web Dynpro systems are set up to authenticate users against the ABAP system.
Import Portal public key into WebAS ABAP

Configure trust from ABAP to EP

Set profile parameters of ABAP system to accept logon tickets

Restart SAP WebAS ABAP system

Create and configure iView for the target system
System Preparation

1. Export Portal Public Key using Keystore
   - Go to the keystore view in visual admin
   - Select TicketKeystore
   - Choose Download verify.der

2. Import public key into WebAS ABAP
   - Start STRUSTSSO2
   - Click on Import Certificate
   - Specify the location of the file verify.der
   - Set the file format to DER coded and confirm
   - In the Trust Manager, choose Add to PSE
   - Save the new certificate list
IView Creation

1. Create an iView using the 'SAP Transaction iView' Template.
   - In the Portal choose Content Administration -> Portal Content.
   - In the Content Catalog on the left, right-click on the folder in which you wish to create the iView and choose 'New -> iView'.
   - In the iView wizard, choose 'SAP Transaction iView', then 'Next'.
   - Enter iView name etc, then choose Next.
   - Choose 'SAP GUI for Windows', then Next.
   - In the 'System' field, choose the system alias for the system object you created, enter a transaction code, then choose Next.
   - And Finish.

2. Integrate the iView in a role and assign the role to your user.
 Agenda

Authentication and Identities

Authentication with SAP

- in a Web Based Scenario
- At the SAP GUI for Windows

Summary
Communication in Integration Scenarios

User Id / Password
  - NTLM
  - Kerberos

SAP Logon Ticket

X.509 Certificate

SAML Artifact

WAM Token

Web access management products

SAP Enterprise Portal

Applications

- Plug-In / Agent

© SAP AG 2005, Authentication and Single Sign On / Patrick Hildenbrand / 44
## Single Sign-On Possibilities

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>SSO to non-SAP Applications</th>
<th>SSO to SAP Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>X.509 Digital Certificates</td>
<td>■Direct client connection</td>
<td>■Direct Client Connection&lt;br&gt;■Certificate sent by EP Server</td>
</tr>
<tr>
<td>SAP Logon Tickets</td>
<td>■SAP Web Server Filter&lt;br&gt;■SAP Ticket Verification Library</td>
<td>■SAP Application configuration</td>
</tr>
<tr>
<td>Integrated Windows Authentication</td>
<td>■NTLM/Kerberos via direct client connection to IIS applications</td>
<td>■NTLM/Kerberos via IIS (plus IISProxy) to WebAS Java 6.40 or SAP EP 6.0</td>
</tr>
<tr>
<td>EAM-Authentication</td>
<td>■Using EAM SSO Agent Software</td>
<td>■Using WAM SSO Agent plus HTTP Header Authentication to WebAS Java 6.40 or SAP EP 6.0</td>
</tr>
<tr>
<td>SAML</td>
<td>■Application specific</td>
<td>■WebAS Java 6.40</td>
</tr>
<tr>
<td>Other</td>
<td>■Application specific</td>
<td>■JAAS (Custom Authentication Modules)</td>
</tr>
</tbody>
</table>
Selecting SSO Possibilities for Applications …

PKI
X.509 certs?

- Use PKI

Integrated
Windows
Auth.?

- Use Integrated Windows authentication

EAM in use?

- Use EAM Integration

SAP Logon
tickets?

- Use SAP Logon tickets

Use SAP EP User Mapping
Further Information

Public Web:
www.sap.com
SAP Developer Network: www.sdn.sap.com ➔ SAP NetWeaver ➔ Security

Related SAP Education Training Opportunities
http://www.sap.com/education/
ADM960 Security in SAP System Environment

Related Workshops/Lectures at SAP TechEd 2004
SCUR352 Leveraging External Authentication Based on Industry Standards
SCUR201 SAP Infrastructure Security
SCUR102 User Management and Authorizations: Overview
SCUR351 User Management and Authorizations: The Details