Using SAP Logon Tickets for Single Sign on to Microsoft based web applications

André Fischer, Project Manager CTSC, SAP AG
Michael Sambeth, NetWeaver Practice Unit Enterprise Portal, SAP Deutschland AG & Co. KG

Summary

Single Sign-On (SSO) is a key feature of the SAP Enterprise Portal that eases user interaction with the many component systems available to the user in a portal environment. Single Sign-On to web based Microsoft backend systems such as Outlook Web Access in extranet scenarios was limited to the user id password mechanism since windows integrated authentication in extranet scenarios. To avoid the administrative overhead that is caused by the need to maintain the user credentials a seamless SSO technique is needed such as SAP Logon Tickets.

Users of the SAP Enterprise Portal can now take advantage of a new ISAPI Filter provided by SAP. The *SSO22KerbMap Module* uses the new delegation features that are available with Microsoft's Kerberos implementation in Windows Server 2003 and Active Directory 2003. The ISAPI Filter provided by SAP securely identifies the user by the SAP Logon Ticket and requests a constrained Kerberos ticket from Active Directory on behalf of that user which can than be used for SSO to a Microsoft web based application.

Applies to

- SAP Enterprise Portal 6.0 SP2 Patch 4 and higher
- Microsoft Windows Server 2003, Active Directory 2003

Keywords

Single Sign-On (SSO), Kerberos, Constrained Delegation, SAP Logon Ticket

Level of difficulty

Technical consultants, Developers

Contact

For feedback or questions you can contact the Collaboration Technology Support Center at ctsc@sap.com. Please check the .NET interoperability area in the SAP Developer Network http://www.sdn.sap.com/sdn/developerareas/dotnet.sdn for any updates or further information.

© Copyright 2004 SAP AG. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, and Informix are trademarks or registered trademarks of IBM Corporation in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

Contents

Summary 1

Applies to 1

Keywords 1

Level of difficulty 1

Contents 3

Introduction 4

SSO to non-SAP applications 5

- SAP Logon Tickets 5
- Web Server Filter 6
- Dynamic Link Libary 6
- Account Aggregation 7

SSO from SAP to a Microsoft environment 7

- Constrained delegation and protocol transition 8

The SAP SSO2KerbMap Module 9

Conclusion 10

Limitations 10

References 11

Introduction

Integration of Microsoft based applications into SAP Enterprise Portal is a demand of customers. A typical integration scenario is the use of Outlook Web Access in SAP Enterprise Portal. The portal user should be able to access the applications in the backend systems without the need to provide username and password. For this it is needed that the backend applications can be accessed using SSO.

SAP Logon Tickets are the flexible central authentication token used in the SAP world and can be used for SSO to all SAP products in the back end. 3rd party applications can also leverage SAP Logon Tickets for SSO. For this SAP provides a Web Server Filter that can be used for an authentication by means of a http header variable and a Dynamic Link Library for Verifying SSO Tickets in 3rd party software which can be used to provide native support for SAP Logon Tickets in applications written in C or JAVA.

Microsoft web based applications usually only support the *authentication methods basic authentication* or *windows integrated authentication* (Kerberos) provided by the Internet Information Server. However, Kerberos does not work well over the internet due to the typical configuration of client-side firewalls. As a result SSO to Microsoft backend systems in extranet scenarios was limited to the user id password mechanism.

A seamless solution that allows SAP Logon Tickets to be used for SSO to Microsoft based backend systems could not be developed by SAP until Microsoft provided new features to its implementation of the Kerberos protocol. Based on the new feature called *protocol transition using constrained delegation* SAP developed the *SSO22KerbMap Module*. This new ISAPI Filter requests a constrained Kerberos ticket for users identified by valid SAP Logon Ticket that can be used for SSO to Microsoft web based applications in the back end.

SSO to non-SAP applications

SAP offers two main methods of Single Sign-On inside SAP NetWeaver: *SAP Logon Tickets* and *account aggregation*. SAP Logon Tickets are the method of choice for authentication in the SAP world and are supported by all SAP products and various non-SAP products.

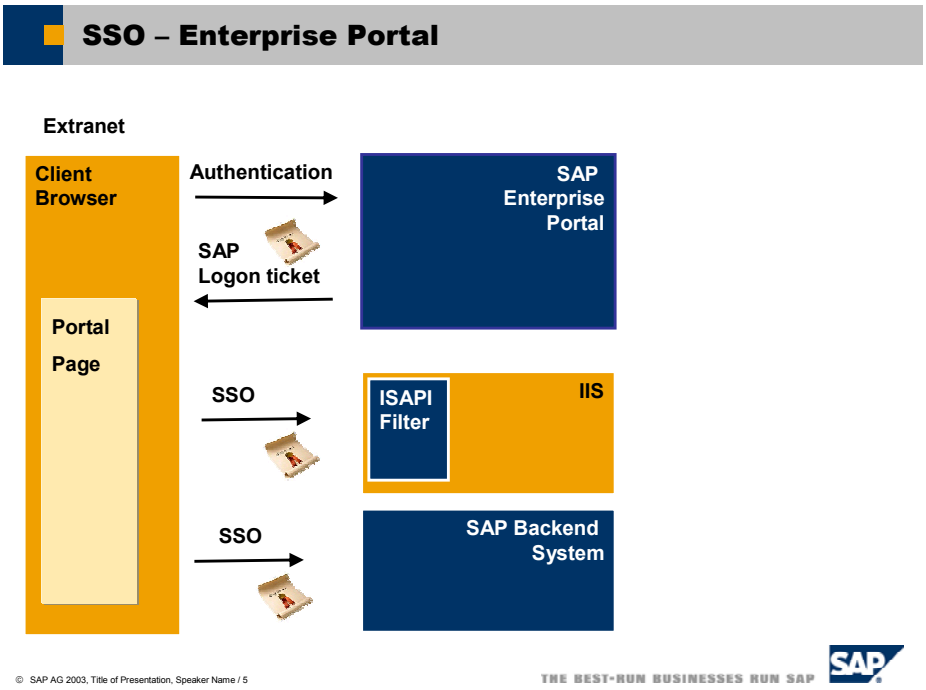

Figure 1: Single Sign-On using SAP Enterprise Portal

SAP Logon Tickets

SAP Logon Tickets serve as authentication tokens. The SAP Enterprise Portal issues a SAP Logon Ticket to a user after successful initial authentication at the portal against a user persistence specified in the portal user management engine (UME). The SAP Logon Ticket that contains the portal user id of the authenticated user is stored as per session cookie on the client browser. The authenticity and integrity is protected using digital signatures whereas the confidentiality of the token is protected through the use of the SSL protocol while in transport. As a third measure the SAP Logon Ticket contains a validity period that can be configured in the security settings of the SAP Enterprise Portal.

All SAP applications and various non-SAP applications support SAP Logon Tickets as SSO mechanism. The user credentials that are contained in a valid SAP Logon Ticket can be used by an external application using either SAP's Web Server Filter or SAP's Dynamic Link Library for verifying SSO Tickets in 3rd party software. An application that accepts SAP Logon Tickets must have access to the issuing server's public-key certificate so that it can verify the digital signature provided with the ticket.

Web Server Filter

As of SAP Enterprise portal 5.0 SAP offers a Web Server Filter that can be used to implement Single Sign On to web based applications that support authentication by a http header variable. The Web Server filter is available on Windows for the Microsoft Internet Information Server (IIS), Apache and the iPlanet Web Server.

The filter verifies the logon ticket using the digital certificate of the Portal Server, then extracts the name of the authenticated user from the logon ticket, and writes it into the http header. The name of the http header variable can be specified using the parameter *remote_user_alias* in the filter configuration file.

A simple example for an ASP application that is using the SAP Web Server Filter is shown in the following listing. It is assumed that the parameter *remote_alias_user* has been assigned the value “MY_SAP_USER”.

```
<%@ LANGUAGE="VBSCRIPT" %>

<%
Dim strUser
strUser = Request.ServerVariables("MY_SAP_USER")
If MY_SAP_USER <> "SecretUserID" Then UserNotAuthenticated
If MY_SAP_USER = "SecretUserID" Then UserAuthenticated

Sub UserNotAuthenticated()
      Response.Write " User is NOT authenticated. "
End Sub
Sub UserAuthenticated()
      Response.Write " User is authenticated. "
End Sub
%>

<HTML>
<HEAD>
Test page check user id
</HEAD>
<BODY>
Welcome to the test page
</BODY>
</HTML>
```

The Web Server Filter can be downloaded from the SAP Service Marketplace using the shortcut “patches” and following the *path Technology Components-> SAP SSOEXT -> SAP SSOEXT-> NT/I386*.

Dynamic Link Libary

If a self written application should provide native support for SSO using SAP Logon Tickets *the Dynamic Library for Verifying SSO Tickets in Third-Party Software* ***sapssoext.dll*** can be used. SAP provides Java and C sample files that can provide some hints how the library can be implemented in the source code of a high level programming language such as Visual Basic, C or JAVA.

The library can be downloaded from the SAP Service Marketplace using the shortcut patches and following the path *Technology Components-> SAP SSOEXT -> SAP SSOEXT-> NT/I386*.

Account Aggregation

With this SSO mechanism the Portal Server uses user mapping information (user id and password) provided by users or administrators to give the portal user access to external systems. The portal components connect to the external system with the user's credentials stored in the portal database.

The usage of account aggregation has several drawbacks. First of all it requires that a SAP portal user has to maintain a user id and password for each application that is using account aggregation. If the password in one backend application changes the SAP portal user has to maintain the stored credentials too. Though account aggregation can be used as an option where no other solution might work it causes a significant administrative overhead.

Using account aggregation to access a web based backend system that is configured to use basic authentication results in sending a URL that contains user name and password. A security update from Microsoft that has been published recently removes support for handling user names and passwords in HTTP and HTTP with Secure Sockets Layer (SSL) or HTTPS URLs in Microsoft Internet Explorer. The following URL syntax is no longer supported in Internet Explorer if this security patch has been applied.

http(s)*://username:password@server/resource.ext*

SSO from SAP to a Microsoft environment

The preferred method for authentication in a Microsoft environment is Kerberos on which windows integrated authentication is based. Since the Kerberos protocol is usually blocked by firewalls windows integrated authentication cannot be used over the internet. A common problem in extranet scenarios is thus client authentication and authorization for external facing Windows services. While in a pure Intranet scenario windows integrated authentication can be used this is not an option for extranet scenarios. Therefore external facing services have to use other authentication techniques.

This problem is addressed by two new extensions that have been added by Microsoft to its implementation of the Kerberos protocol which allow the use of *constrained delegation* and *protocol transition*. The new features can only be used on members of the Windows Server 2003 family and require that the functional level of the domain and forest have been raised to Windows Server 2003.

Constrained delegation and protocol transition

The idea behind *protocol transition* is that the communication between browser and front end server leverages common internet technologies whereas backend communication is securely performed by authenticating with Kerberos. The initial client authentication can thus be performed using protocols other than Kerberos.

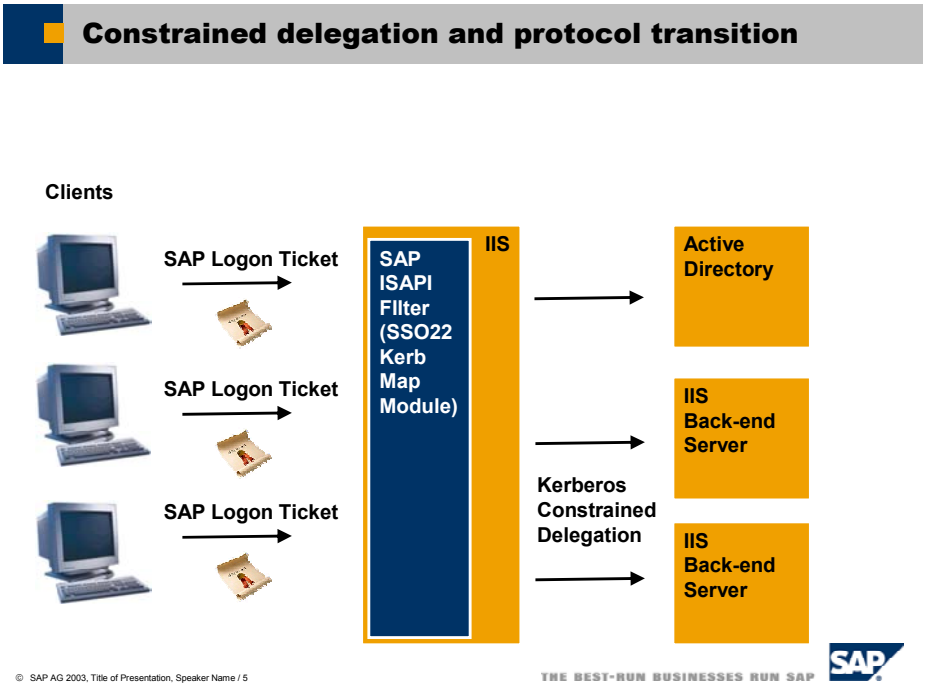

Figure 2: Constrained delegation and protocol transition – The SSO22KerbMap Module

The delegation model known *as constrained delegation* allows a service to delegate client credentials. It is called constrained delegation since the delegation of authentication can be restricted to specified services only. Delegation of authentication means that a service A may request Kerberos tickets on behalf of a user from Active Directory to authenticate against a service B.

An administrator can specify which Service Principal Names (SPNs) an account is able to delegate to with constrained delegation. If the service A is running under the built-in Local System account it is running on behalf of the machine itself. This is the case for the SAP SSO22KerbMap Module described in the following section. Therefore this computer account has to be configured such that it is trusted for delegation to the specified service B that may run on another server. The configuration is performed using the MMC SnapIn Users and Computers in the delegation tab as shown in the following figure:

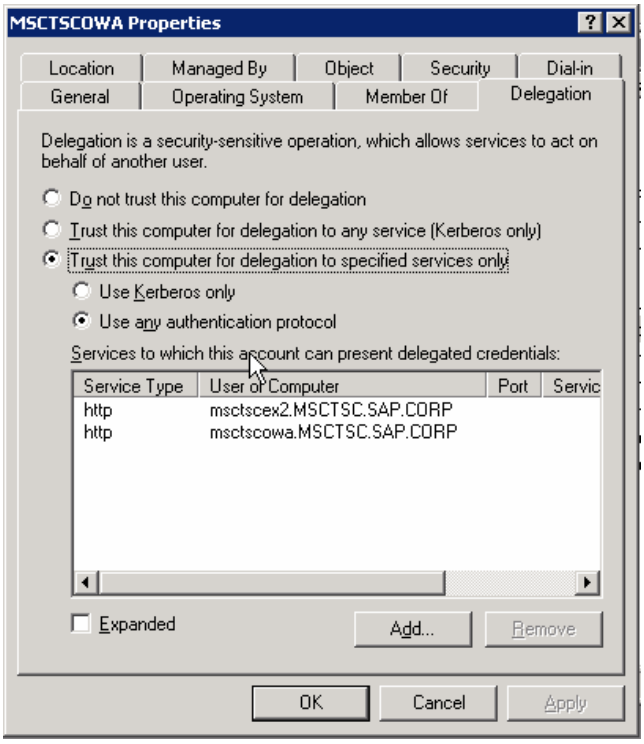

Figure 3: Configuration of constrained delegation using MMC

Note that for protocol transition to be used the network administrator must explicitly grant the right for constrained delegation using "any authentication protocol" on the front end server.

The SAP SSO2KerbMap Module

Based on the technology of *constrained delegation using protocol transition* SAP offers the SSO2KerbMap module. SAP's new SSO22KerbMap ISAPI Filter securely identifies the user by the SAP Logon Ticket and requests a constrained Kerberos ticket from Active Directory on behalf of the interactive SAP portal user.

The idea behind the SSO22KerbMap Module is that both SAP Logon Tickets and Kerberos Tickets represent user credentials for their respective security contexts. Constrained delegation using protocol transition allows the use of user credentials represented by a SAP Logon Ticket to obtain a Kerberos ticket which can be used for SSO to MS based backend systems. The SSO22KerbMap Module consists technically out of an ISAPI Filter DLL. The filter allows to obtain Kerberos Tickets on behalf of the user that has been successfully authenticated by the portal and thus has been submitted a valid SAP Logon Ticket.

How does the filter work in detail ?

If the filter DLL is installed as an ISAPI Filter all http requests that are passing the filter will be analyzed. If a SAP Logon Ticket is found in the header of an http request the portal user id is extracted. The next step performed is the identification of the user in Active Directory based on the information found in the SAP Logon Ticket. Using the configuration file SSO22KerbMap.ini the filter retrieves the information from the

parameter *SSO2AccountAttribute* which user attribute in Active Directory is used as portal logon id. It is recommended to use a unique attribute such as the userPrincipalName as portal user id. The filter checks for a user in active directory where the value of the attribute matches the value found in the SAP Logon Ticket. If exactly one user is found the ISAPI Filter requests a Kerberos ticket on behalf of that user and adds the Kerberos token to the header.

Conclusion

SAP Enterprise Portal serves as an end to end solution for SSO for both SAP and Microsoft backend applications. No 3rd party software is needed to set up a Single Sign-On solution to access SAP and IIS based backend systems. No additional software has to be installed on the frontends to enable this SSO solution.

Limitations

Constrained delegation can only be enabled on a member of the Windows Server 2003 family. The functional level of your domain and forest has to be raised to Windows Server 2003. SAP Logon Tickets as being implemented as cookies are only sent to servers in the same DNS domain as the portal server. If SAP Enterprise Portal and the backend applications reside in different DNS domains one has to configure “Issuing SAP Logon Tickets for multiple Domains”. Please see http://service.sap.com/ep60howtoguides -> Cross Domain SSO.

References

- Exploring S4U Kerberos extensions in windows 2003
  http://msdn.microsoft.com/msdnmag/issues/03/04/SecurityBriefs/
- A security update is available that modifies the default behavior of Internet Explorer for handling user information in HTTP and in HTTPS URLs
  http://support.microsoft.com/default.aspx?scid=kb;en;834489
- http://service.sap.com/patches follow the path:
  Technology Components-> SAP SSOEXT -> SAP SSOEXT-> NT/I386
  - SSO22KerbMap ISAPI Module
  - Dynamic Library for Verifying SSO Tickets in Third-Party Software
  - Web Server Filter
- SAP Note 735639 “SSO2 To Kerberos Mapping Filter: Known issues”
  http://service.sap.com/~form/handler?_APP=01100107900000000342&_EVENT=DISPL_TXT&_NNUM=735639&_NLANG=E