Case Study

ADFS and Kerberos Constrained Delegation

Author ........................................... [Thorsten Pape]
1. **List of Content**

1. List of Content .................................................................................................................. 2
2. Background .......................................................................................................................... 3
3. Requirements ....................................................................................................................... 5
4. Technical Complexity ......................................................................................................... 5
5. Alternative Method: ADFS ................................................................................................. 5
6. Test Environment .................................................................................................................. 6
7. Configuration ADFS .......................................................................................................... 9
   7.1 Resource ADFS (Enterprise Domain ORION.LAN) Part 1 ........................................ 9
   7.2 Account ADFS (Customer Domain GEMINI.LAN) .................................................. 12
   7.3 Resource ADFS (Company domain ORION.LAN) Part 2 ....................................... 21
8. Configuration of the application WSS ............................................................................. 25
9. Configuration of the TMG/ISA ......................................................................................... 29
   9.1 Initialisation .................................................................................................................... 29
   9.2 Configuration on the TMG/ISA .................................................................................... 31
10. Function test ..................................................................................................................... 36
2. Background

A company runs two Share point farms, of which one is used as Intranet for the employees, whilst the other is used for the company's clients. The farm used as intranet is located in the local area network (LAN) while the latter is in a perimeter network assigned for clients respectively. Both Share point Farms share the same content to a large extent, because of which some applications are accessible to both employees as well as clients. Whilst employees use the integrated authentication or the basic authentication to access the internal farm, the clients use a RSA SecurID token to access the Share point farm of the perimeter network. For this purpose an extra Domain Controller, ACE Server and TMG/ISA Server in the client's perimeter network is set up. Every client (individuals too) is assigned a login account in the perimeter network domain which has a SecurID token. The advantage here is that the user does not need to remember a password; he only needs to type in his login ID, pin and token in order to be authenticated and authorised. The authentication occurs via the TMG/ISA network. The user logs on the TMG/ISA which is formula based and this authenticates the user on the domain in the perimeter network via the Kerberos Constrained Delegation.
Actual Development of a SharePoint Farm

The diagram illustrates the network architecture for a SharePoint Farm. It includes:

- **LAN**: Local Area Network where the SharePoint Farm for employees is located.
- **DMZ**: Demilitarized Zone where the ISA/TMG and Sharepoint Farm for clients are located.
- **Internet**: The outermost network.
- **Employee**: The end user accessing the SharePoint Farm.
- **ACE Server**: A server used for authentication purposes.
- **Internal dom**: The internal domain for employees.
- **External dom**: The external domain for clients.

The network uses ISA/TMG for secure access and Sharepoint for collaboration and file sharing.
3. Requirements

On the basis of cost reduction and implementation measures, the company considered eliminating one of the Share point farms as both farms contain more or less the same content. If the customers as well as the employees are allowed to access the same Share point, this could help reduce the number of servers in use, the licenses and the running costs. Furthermore, customers are to use the SecuriID token to log on to the customer’s domain and to receive the authorisation for accessing the Share point farm in the company’s domain.

4. Technical Complexity

The concept appears to fail at the very beginning of its implementation. The TMG/ISA server was delegated to authenticate the registered customers via Kerberos at the customer domain. The TMG/ISA is a member of the customer domain, and thus only in relation to the customer domain it can authenticate via KCD. In response, the users can only be authorised for services within this domain. A user cannot be authenticated and authorised at the Share point farm of the company's domain using Kerberos. Also the alternative, which is the set up of customer accounts in the company domain and the execution of the Kerberos Constrained Delegation across this domain is not possible as this is forbidden by the company’s security policies.

5. Alternative Method: ADFS

After various alternatives were discussed, which involved unsatisfactory results, a security expert from the company suggested in bringing the Kerberos Constrained Delegation and the ADFS together. He believed that this could satisfy the requirements. Sadly, the experience with ADFS was in general very limited. Also on the Internet, ADFS is vaguely described; the special company requirements, the combination of KCD with ADFS are still not specified. Therefore, the feasibility and the execution needed to be verified over a test environment.
6. Test Environment

In order to prove or refute the feasibility, a test environment was set up. This was kept small due to the lack of resources.

<table>
<thead>
<tr>
<th>Computer</th>
<th>Domain</th>
<th>Task</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>TPSRV01</td>
<td>Orion.lan</td>
<td>DC, CA, Resource ADFS</td>
<td>Win 2008 SP2</td>
</tr>
<tr>
<td>WSS</td>
<td>Orion.lan</td>
<td>Windows Sharepoint</td>
<td>Win 2003 R2 SP3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Services 3.0</td>
<td></td>
</tr>
<tr>
<td>GEMSRV01</td>
<td>Gemini.lan</td>
<td>DC, Account ADFS</td>
<td>Win 2008 R2</td>
</tr>
<tr>
<td>GEMTMG</td>
<td>Gemini.lan</td>
<td>TMG</td>
<td>Win 2008 R2</td>
</tr>
</tbody>
</table>
An ACE server was not available; hence a FBA was used as an alternative. This however should have no influence on the result. The computers were positioned in two domains; a trust relationship was not established. The domain ORION.LAN covered the enterprise domain whilst the domain GEMINI.LAN covered the customer domain in the DMZ. The public domain was represented by the name PORTALS.LAN. Using the limited resources that were available, ADFS services were installed on the respective controller domains. Moreover, the enterprise domain controller provided a Certification Authority (CA), which imitated both Enterprise as well as Public CA.
7. Configuration ADFS

A detailed explanation concerning the installation of the ADFS can be found in http://technet.microsoft.com/en-us/library/cc731443(WS.10).aspx, hence no further description is provided here.

The ADFS is installed on every domain, as well as on Servers which have WSS and functions as an Account ADFS as well as a Resource ADFS.

The Account ADFS is responsible for log-on accounts, group associations and issues tokens respectively while the Resource ADFS interprets the tokens and issues authorising cookies for the application.

7.1 Resource ADFS (Enterprise Domain ORION.LAN) Part 1

Firstly, a trust policy is set-up.

Under General settings, the URI and the endpoint are determined.
Please note that the endpoint URL contains the official address which allows accessibility via internet. Later on, the Resource ADFS will be made accessible via https://radfs.portals.lan. (Portals.lan represents an official domain in the test environment).

Secondly, a display name is assigned for the Trust policies.
Lastly, a certificate has to be allocated to the ADFS computer. This certificate is issued by its own CA.
Shortly after the Trust Policy settings are set, the Claims are configured. On default 3 Claims are offered; they are identity-based Claims and are responsible for use identification. For test purposes, 3 more Claims are created. They are group-based and represent certain group affiliations in the account domain. These Claims are supposed to reflect certain authorisations on the WSS application level.

After this, the Trust Policy is saved and the resulting XML-Data is copied onto the computer with the account ADFS.

7.2 Account ADFS (Customer Domain GEMINI.LAN)

The first steps of the ADFS configuration in the customer domain GEMINI.LAN run similar to the enterprise’s domain ORION.LAN. Soon after, a Trust Policy is created. Just as in the ORION.LAN, the URI and the endpoint URL are also determined here.
Additionally, it is important that the endpoint URL complies with the public URL. Under Display name, Policy determination and certificate classification takes place.
The certificate was issued by the Enterprise CA in the domain ORION.LAN. Here it is important that the computer, which works with the certificates of these CA, hold the root certificate in the file Trusted Root CA.
Similar to the enterprise domain configuration, Orion.lan, 3 Group Claims are added.

Thereby, the configuration steps of the Account ADFS and of the Resource ADFS differ. In the Account ADFS a so called Account Store is set up.
In addition, it is determined which attribute from which source in the ADFS token can be made available. In this scenario, attributes from the domain GEMINI.LAN are made directly available.

On default, all Identity Claims are offered in the Account Store; for which only the UPN needs to be assigned to the token. The other two Identity Claims are deactivated.
The Account Store is then enhanced by the Group Claims, which were created under the Organisation Claims.

Among other things here, the Group Claim allocation takes place. For example, the Group Claim "gemini_wss_read" the AD-group wssread@gemini.lan is assigned.

As next step, the import of the Trust Policy of ORION.LAN follows, which is practical for the configuration for communication with the Resource partner (as an alternative, the configuration can be accomplished also manually).

Using the Wizard, one can choose the already saved and copied Trust Policy.

Once the Trust Policy is imported, the initial configuration of the Resource partner is complete; the only aspect which needs to be specified is the additional Claims that are to be added to the token on the Resource partner.
In this test scenario, the identity is to be primarily determined via UPN and handed over; email address or common name does not play any role here (Hence these Claims are deactivated).

In addition to the token, the group association has to be handed over. The authorisation groups were assigned to the initially defined Group Claims, when configuring the Account Stores. Now it is valid to illustrate these Organizational Group Claims on the outgoing so called Group Claims, which are entered into the token.

Once all necessary outgoing Group claims are set-up, the Account ADFS is completely configured.

In the last step, the Trust Policy is exported and stored for example on the computer of the Resource ADFS, in order to import these there.
7.3 Resource ADFS (Company domain ORION.LAN) Part 2

After the account ADFS is finished, certain concluding configurations has to be conducted on the Resource ADFS, beginning with the production of a new partner account till the import of the GEMINI.LAN Trust Policy.

Using the Wizard, one can export and copy the Trust Policy.

![Add Account Partner Wizard](image)
In the configuration of the ADFS account, the Group Claims were illustrated on the outgoing Claims, which are conveyed to the resource ADFS using a token. In respect to the resource ADFS, these Claims are so called Incoming Claims, which is illustrated on the Organizational Claims of the ADFS resource.

For every incoming Claim, a certain allocation or association takes place.
So that every relevant AD group from the domain GEMINI.LAN receives certain permission on the WSS application (in the domain ORION.LAN).

In order to complete the configuration of the Resource ADFS, the applications have to be assigned to the Resource ADFS (via Applications -> New -> Application).

Even here, it is important, that the public URL applications are listed. Only those applications which are relevant for the Claims are activated.
8. Configuration of the application WSS

In this part, it is concerned with the preparation of the published WSS application for ADFS. After WSS 3.0 is installed, the ADFS web agents are added to the server.

(Under Windows 2008, one adds the agents over roles insertion.) Next the application will be prepared, which is to be published.
In the next step, this application will be enhanced, so that an IIS website will be provided, which will respond to the URL https://wss.orion.lan. This web site will be assigned to the extranet zone.

In addition, an Alternate Access Mapping will be provided for the public URL (https://wss.portals.lan).

Each of the zones has a so called authentication provider. For the default zone, it is Windows (NTLM or Negotiate); for the extranet zone, it is the SSO Provider. For this purpose, the application has to be configured via web.config data. This is made easy using the VB script SetupSharePointADFS.vbs umsetzen, which can be downloaded from the following link: http://blogs.msdn.com/b/sharepoint/archive/2007/10/11/a-script-to-configure-sharepoint-to-use-adfs-for-authentication.aspx

Through the execution from the following:

cscript SetupSharePointADFS.vbs -fs tpsrv01.orion.lan -appconfig
C:\inetpub\wwwroot\wss\VirtualDirectories\wss.orion.lan443\web.config -adminconfig
c:\inetpub\wwwroot\wss\virtualdirectories\37945\web.config -cookiepath / -returnurl https://wss.orion.lan/-urlzone extranet

The web.config files are automatically adapted for the use of ADFS. Changes are accomplished both on sides of the application as well as on the sides of the share point central administration (-adminconfig and -appconfig). The changes that the central administration undertook must also be done for the Web application, which is a reason why the VB-Script with changed adminconfig parameters is implemented for a second time:
Thorsten Pape • Hamburg

cscript SetupSharePointADFS.vbs -fs tpsrv01.orion.lan -appconfig
C:\inetpub\wwwroot\wss\VirtualDirectories\wss.orion.lan443\web.config -adminconfig
C:\inetpub\wwwroot\wss\virtualdirectories\SP180\web.config -cookiepath / -returnurl

1 = Verzeichnis Sharepoint Zentraladministration
2 = Verzeichnis Erstellte Applikations-Website (Default Zone)
3 = Verzeichnis Erweiterte Website (Extranet Zone)

After an IISRESET, an SSO authentication provider for ADFS is provided.

Authentication Providers

<table>
<thead>
<tr>
<th>Zone</th>
<th>Membership Provider Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Windows</td>
</tr>
<tr>
<td>Extranet</td>
<td>SingleSignOnMembershipProvider2</td>
</tr>
</tbody>
</table>

Additional information can be found under the following link:
The function of the SSO Authentication provider and also the function of the ADFS Web Agents can be tested, for example by adding users for the application.

While searching for users beginning with orion_, the group claims for example were shown, which were listed during the set-up of the Resource ADFS.
9. Configuration of the TMG/ISA

9.1 Initialisation

In order to authenticate itself via KCD at the account ADFS, certain framework parameters must be fulfilled. First a user has to be set-up (here Gemini \ ADFSviaKCD); in relation to which the ADFS Application pool runs. A service Principal name must be assigned to this user, either with the tools SetSPN or by ADSIEDIT.

```
Setspn -a http://federation.gemini.lan gemini\adfsviaKCD
```

In addition, this user must be member of the group IIS_IUSR (starting from Windows 2008). Moreover the user needs the following user rights on the ADFS (account) computer:
• Act as part of the operating system
• Generate Security Audit Events
• Logon as a Service

In addition, the following authorisations are necessary:
• Write/read only to C:\ADFS
• Write/read only to C:\Windows\TEMP
• Write/read only to C:\Windows\Microsoft.NET\Framework64\v2.0.50727
• Read only to C:\Windows\SystemData\ADFS
• Write/read only to C:\Windows\SystemData\ADFS\Logs
• Read only to the private key of the internal web certificate, which was assigned in the Trust Policy (gemsrv01.gemini.lan)

Lastly, the ADFS Application Pool has to be restarted.

In regards to the TMG/ISA, it must be guaranteed, that the computer is secure for delegation:
9.2 Configuration on the TMG/ISA

In the next step, the firewall policies and the web listener is set-up on the TMG/ISA. For this, three public IP addresses and three IP addresses from the DMZ are required in addition to the three public URLs; the public addresses are re-routed by NAT on the DMZ IP addresses. Moreover public certificates are necessary for each public URL. In the test environment, a so called SAN certificate is used, so that each URL can be authenticated by the same certificate:
Furthermore, the Web Listener is created. Here, it is to be noted that every Web Listener is assigned its own DMZ IP.
The TMG/ISA functions as the reverse proxy with a network card, thus the internal net is to be selected. The Web Listeners are to react only to SSL protected inquiries, which is a reason why the public certificate is to be assigned to Web Listener.

The Web Listener of the WSS Portals and the Resource ADFS does not necessary require a client authentication; hence a no authentication is chosen for the Web Listener.
While for the Web Listener of the Account ADFS, the Form Based Authentication has to be selected.

Since the users are expected to authenticate themselves on the domain GEMINI.LAN, the Windows authentication validation method is selected.

After the web listener is completed, the firewall policies are prepared. The parameters of the three firewall policies are shown in the following table:
<table>
<thead>
<tr>
<th>Function</th>
<th>Sub function</th>
<th>Policy: WSS</th>
<th>Policy: radfs</th>
<th>Policy: aadfs</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
<td>WSS/enabled</td>
<td>radfs/enabled</td>
<td>aadfs/enabled</td>
</tr>
<tr>
<td>Action</td>
<td></td>
<td>Allow</td>
<td>Allow</td>
<td>Allow</td>
</tr>
<tr>
<td>From</td>
<td></td>
<td>Anywhere</td>
<td>Anywhere</td>
<td>Anywhere</td>
</tr>
<tr>
<td>To</td>
<td>Forward org. Hostheader</td>
<td>wss.orion.lan</td>
<td>tpsrv01.orion.lan</td>
<td>gemsrv01.gemini.lan</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Nein</td>
<td>Nein</td>
<td>Nein</td>
</tr>
<tr>
<td>Requests appear to come from</td>
<td>TMG/ISA</td>
<td>TMG/ISA</td>
<td>TMG/ISA</td>
<td></td>
</tr>
<tr>
<td>Traffic</td>
<td></td>
<td>HTTPS</td>
<td>HTTPS</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Listener</td>
<td></td>
<td>WSS listener</td>
<td>radfs listener</td>
<td>aadfs listener</td>
</tr>
<tr>
<td>Public Name</td>
<td></td>
<td>wss.portals.lan</td>
<td>radfs.portals.lan</td>
<td>aadfs.portals.lan</td>
</tr>
<tr>
<td>Paths</td>
<td></td>
<td>/*</td>
<td>/adfs/ls/*</td>
<td>/adfs/ls/*</td>
</tr>
<tr>
<td>Auth. Delegation</td>
<td>No delegation</td>
<td>No delegation</td>
<td>KCD</td>
<td></td>
</tr>
<tr>
<td>SPN</td>
<td></td>
<td>N/A</td>
<td>N/A</td>
<td>http/federation.gemini.lan</td>
</tr>
<tr>
<td>Application Settings</td>
<td>inaktiv</td>
<td>inaktiv</td>
<td>inaktiv</td>
<td></td>
</tr>
<tr>
<td>Bridging</td>
<td></td>
<td>SSL nach 443</td>
<td>SSL nach 443</td>
<td>SSL nach 443</td>
</tr>
<tr>
<td>Users</td>
<td></td>
<td>All Users</td>
<td>All Users</td>
<td>All Auth. Users</td>
</tr>
<tr>
<td>Schedule</td>
<td></td>
<td>Always</td>
<td>Always</td>
<td>Always</td>
</tr>
<tr>
<td>Link Translation</td>
<td>Apply to rule</td>
<td>Apply to rule</td>
<td>Apply to Rule</td>
<td></td>
</tr>
</tbody>
</table>

And an overview of the Policies on the TMG/ISA:
Thereby, the test environment is configured.

10. Function test

For the function test, 4 test accounts are set-up on the customer’s domain GEMINI.LAN. Every test user except Frank Borman is a member of the authorisation group for the WSS Portal.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frank Borman</td>
<td>User</td>
<td>No Rights on Orion WSS</td>
</tr>
<tr>
<td>John W. Young</td>
<td>User</td>
<td>WSS Orion Member</td>
</tr>
<tr>
<td>Michael Collins</td>
<td>User</td>
<td>WSS Orion Reader</td>
</tr>
<tr>
<td>Neil A. Armstrong</td>
<td>User</td>
<td>WSS Orion Admin</td>
</tr>
</tbody>
</table>

In this example, user John Young will try to log on to the WSS Portal.

John Young is directed to the ADFS account and has to authenticate himself on the TMG/ISA.
In the TMG/ISA Log, it is shown as follows:

<table>
<thead>
<tr>
<th>De...</th>
<th>Protocol</th>
<th>Action</th>
<th>Rule</th>
<th>HTTP Status Code</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>https</td>
<td>Allowed Co...</td>
<td>WSS</td>
<td>302 Moved Temporarily</td>
<td><a href="https://was.aonlan.de:443/">https://was.aonlan.de:443/</a></td>
</tr>
<tr>
<td>443</td>
<td>https</td>
<td>Allowed Co...</td>
<td>soap</td>
<td>302 Moved Temporarily</td>
<td><a href="https://soap1.aonlan.de:443/adfs/ls/?wa=wsignin1.0&amp;nt=192.168.1.23&amp;lsd=0d9e8eb3">https://soap1.aonlan.de:443/adfs/ls/?wa=wsignin1.0&amp;nt=192.168.1.23&amp;lsd=0d9e8eb3</a> &amp;wpsign...</td>
</tr>
<tr>
<td>443</td>
<td>https</td>
<td>Denied Con...</td>
<td>soap</td>
<td>401 Unauthorized</td>
<td><a href="http://adfs.portals.de/adfs/ls/?wa=wsignin1.0&amp;nt=192.168.1.23&amp;lsd=0d9e8eb3">http://adfs.portals.de/adfs/ls/?wa=wsignin1.0&amp;nt=192.168.1.23&amp;lsd=0d9e8eb3</a> ...</td>
</tr>
<tr>
<td>443</td>
<td>https</td>
<td>Allowed Co...</td>
<td>WSS</td>
<td>200 The operation completed successfully,</td>
<td><a href="http://adfs.portals.de/cookieauth.dll?geologon?url=http://adfs.portals.de/e...">http://adfs.portals.de/cookieauth.dll?geologon?url=http://adfs.portals.de/e...</a></td>
</tr>
</tbody>
</table>

The user tries to access the portal (line 1) and is re-routed to the ADFS account, so that the user can obtain a token. The re-routing occurs due to missing cookies on the Resource ADFS page (line 2). The TMG/ISA stops the user (line 3), as a non-authenticated access is not allowed. A registration formular is made ready (line 4). The user then registers via TMG/ISA successfully.
Thorsten Pape • Hamburg

![Event Properties - Event 4769, Microsoft Windows security auditing.](image1)

Log Name: Security
Source: Microsoft Windows security
Logged: 5/27/2010 1:25:01 AM
Event ID: 4769
Task Category: Kerberos Service Ticket Operation
Level: Information
Keywords: Audit Success
User: N/A
Computer: GEMSRT01.Geminillan
OpCode: Info
More Information: Event Log Online Help

![Event Properties - Event 4769, Microsoft Windows security auditing.](image2)

Log Name: Security
Source: Microsoft Windows security
Logged: 5/27/2010 1:25:01 AM
Event ID: 4769
Task Category: Kerberos Service Ticket Operation
Level: Information
Keywords: Audit Success
User: N/A
Computer: GEMSRT01.Geminillan
OpCode: Info
More Information: Event Log Online Help
and the user obtains his token (line 4) and is forwarded to Resource ADFS. Here, it receives its Cookie (line 5) and requests the URL of the portal again, where he is successfully authorised (starting from line 6).
An authenticated user who has no authorisation on the WSS Portal receives the following message: