Abstract:
This non-normative document describes a number of user cases pertaining to the application of SAML with Kerberos, DCE and Windows.

Status:
Working draft. Send comments to the mailing list.
Committee members should send comments on this specification to the securityservices@lists.oasis-open.org list. Others should subscribe to and send comments to the security-services-comment@lists.oasis-open.org list. To subscribe, send an email message to security-services-comment-request@lists.oasis-open.org with the word "subscribe" as the body of the message.
For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Security Services TC web page (http://www.oasisopen.org/committees/security/).
# Table of Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>1 Scope Statement .................................................................</td>
</tr>
<tr>
<td>27</td>
<td>2 Credential Conversion Service ..................................................</td>
</tr>
<tr>
<td>28</td>
<td>2.1 Requirements ........................................................................</td>
</tr>
<tr>
<td>29</td>
<td>3 Use Cases ..................................................................................</td>
</tr>
<tr>
<td>30</td>
<td>3.1 Bridge Servers .......................................................................</td>
</tr>
<tr>
<td>31</td>
<td>3.1.1 Application Scenarios ........................................................</td>
</tr>
<tr>
<td>32</td>
<td>3.1.2 Candidate Profiles .............................................................</td>
</tr>
<tr>
<td>33</td>
<td>3.2 Browser/Kerberos use case ......................................................</td>
</tr>
<tr>
<td>34</td>
<td>3.2.1 Application Scenario ..........................................................</td>
</tr>
<tr>
<td>35</td>
<td>3.2.2 Candidate Profiles .............................................................</td>
</tr>
</tbody>
</table>
1 Scope Statement

This document proposes a number of use cases where SAML can be used in conjunction with Kerberos based technology. This includes:

- Kerberos v5 (as defined in RFC 1510)
- Kerberos GSS-API mechanism (as defined in RFC 1964)
- DCE (Distributed Computing Environment)
- Windows 2000/2003

In particular of interest are the last two technologies. Both of these leverage the ability of Kerberos to transport authorization data.

Note that some of the user cases contained within this document do not necessarily require any new profiles or SAML constructs to be defined. Those use cases and their associated “candidate profiles” can be considered to be “Design Patterns”.
2 Credential Conversion Service

2.1 Requirements

A number of technologies support the transportation of credentials within a defined structure. It is proposed that the OASIS SSTC develops a standard for a “Credential Conversion Service”. This will permit the conversion of a number of credential formats into SAML assertions, and vice versa. This standard should also define the set of rules of how given credential formats are converted into SAML assertions.

2.2 Proposal

It is proposed that a new service is added to SAML, called the Credential Conversion Service. This will require a new protocol, messages and bindings to be produced. A new protocol called the SAML Convert-Response is proposed. The SAML Convert message should have the following characteristics:

- The “to be converted” credential is supplied in the message
- The message defines the incoming credential format, e.g. DCE EPAC, Windows PAC, SAML assertion
- An indicator defines the type of response required. This could either be a SAML assertion, an artifact that references the assertion or some other format. If the artifact response is selected then the Credential Conversion Service must cache the produced SAML assertion in a cache that a local SAML Responder can access
- A trust relationship must be maintained between the caller and the Credential Conversion Service.

The response provided back to the client is either a SAML assertion or an artifact.

Figure 1 shows the overall architecture.

![Figure 1 – Credential Conversion Service](image)
3 Use Cases

3.1 Bridge Servers

3.1.1 Application Scenarios

In the context of this document Bridge Servers are devices that provide middleware translation from one protocol to another, for example EJB/RMI to RPC. Two application scenarios are described, although many others could be envisaged, they are:

- EJB Bridge Server.
- RPC Bridge Server

3.1.1.1 EJB Bridge Server

The EJB Bridge Server “translates” between EJB/RMI and RPC (either the DCE or Windows dialect). Figure 2 illustrates the basic architecture and typical usage. On the left of the Bridge Server are a browser and a web server. The web user authenticates to the web server using an appropriate authentication mechanism and Single Sign-on is provided by a proprietary SSO mechanism. At some point the user will initiate access to a resource or application host in another security domain that uses a different middleware technology. In this example the left hand side of the Bridge server is using EJB/RMI and the right hand side RPC. The requirement is to pass the security context of the user’s session to the RPC based application. Typically in these architectures the Bridge Server acts as an EJB server and as a RPC client. The intent is to pass a SAML assertion to the Bridge Server so that it can create a client session with the RPC server application.

Figure 2 – Browser/Kerberos Use case
3.1.1.2 RPC Bridge Server

In this scenario the client side is a Kerberos based environment, more specifically either DCE or Windows RPC (e.g. DCOM, COM+). One of the use cases could be an inverse of the previous scenario: the client side application is RPC based, and wishes to access an EJB application within a security domain. Figure 3 illustrates this scenario.

![Diagram of RPC Bridge Server Use Case]

Figure 3 – RPC Bridge Server Use Case

3.1.2 Candidate Profiles

3.1.2.1 EJB Bridge Server

As the method by which the security context is passed to the EJB container typically varies between J2EE application server vendors, it’s not possible to pass the SAML assertion in-band. Therefore when the connection is made to the bridge server, the security context needs to be extracted and used to request a SAML assertion from a SAML Responder. For instance if the EJB container (as hosted by the Bridge Server) is protected by using a SSL connection then the client identity can be extracted from the client certificate. This identity can then be used in a <AuthenticationQuery> and <AttributeQuery> to obtain authentication and attribute information pertaining to the subject. By this method the Bridge Server can obtain the subject’s session attributes that ordinarily would not be available to it. The local site’s SAML Responder needs to be able to query the access management infrastructure on the local site to obtain details and attributes of the user’s current session.

Having obtained the subject’s session identity and attributes a RPC client can be created to service the request. If the receiving side is DCE, the Bridge Server could create a new credential using either chained delegation or impersonation, the EPAC being populated from the SAML assertion. If the receiving side is pure Kerberos, and has access to the KDC key then the Bridge Server can create a TGT for securing the connection to the RPC server.

The Bridge Server could either be within its own realm/cell/domain or within the one associated with the RPC application. In the former case the cross-realm trust feature of Kerberos can be used to form a trust relationship between the Bridge Server’s KDC and the KDC used by the application.

Figure 4 illustrates the processing steps.
1. The user authenticate to their local web site and uses the provided authentication and SSO mechanisms
2. At some point an application they are using on the web site requires access to an EJB.
3. The web site contacts the EJB Home interface (hosted on the Bridge Server) using the supported mechanism for transporting the security context to the EJB server (e.g. SSL)
4. The EJB server extracts the user’s identity and sends a SAML Request to the SAML Responder
5. The SAML Responder replies with appropriate SAML statements
6. The Bridge Server creates a RPC client. A TGT is created for access to the RPC Server application. The PAC is created from the received information within the SAML response. The TGT for the foreign user is created by a new service provided by the KDC, based on data in the SAML assertion and local policy data

3.1.2.2 RPC Bridge Server

As in the previous use case this Bridge Server translates between RPC and EJB/RMI. The Bridge Server is formed out of two halves, a RPC server application and an EJB client. The processing is would be a follows:
1. The user authenticates to their local realm/cell/domain KDC.
2. The user (or an application they are using) wishes to access a RPC server application and request a Service Ticket.
3. The RPC server on the Bridge Server receives the request and authenticates the Service Ticket.
4. The RPC server extracts the PAC contained with the Service Ticket
5. It sends a request to the Credential Conversion Service to convert the supplied PAC to a SAML assertion.
6. The EJB client then calls the EJB Server, passing the security context across to the EJB.
A number of techniques could be employed in providing the security context to the EJB server, which one is selected, would depend on the specific environment.

- The SAML assertion could be provided “in-band” as one of the parameters in the EJB Home Interface
- An artifact is provided as one of the parameters in the EJB Home Interface. The EJB would then use the artifact to obtain the SAML assertion from a SAML Responder. Use of this technique would require the Credential Conversion Service to store the created SAML assertion so that the SAML Responder can obtain it.
- The EJB client uses any of the mechanism supported by the EJB server for transporting the security context (e.g., SSL)

The last two techniques could be combined so that SSL is used to provide some of the security context, and by using the artifact obtain the SAML assertion which contains additional session attribute information.
3.2 Browser/Kerberos use case

3.2.1 Application Scenario

In the Browser/Kerberos use case the client workstation logs on to the local KDC, the Kerberos client software being present on the workstation. Following successful authentication the session credentials reside on the workstation.

The workstation user then wishes to gain access to resources on a remote web site in another management domain, so that:

* No further authentication is required
* Session attributes are transferred seamlessly over to the remote web server so that it makes appropriate authorization decisions

Note that the local site may, or may not have a web server.

![Browser/Kerberos Use case diagram](image)

3.2.2 Candidate Profiles

Two candidate profiles are proposed, in both of them the intent is to use the identity and optionally authorization information in a PAC to generate a SAML assertion, the SAML assertion is then provided to the remote web site. The candidate profiles leverage the existing Browser profiles defined in SAML 1.1 as well as the propose credential conversion service.

3.2.2.1 Kerberos Browser/Artifact Candidate Profile

The proposed processing is as follows:

1. The user on the workstation authenticates into the local domain/cell/realm, using application software resident on the workstation. Successful authentication results in an appropriate TGT being provided back to the workstation. The user can then access resources in the Local Site.
2. The user then wishes to gain access to a remote site. In this profile the remote site is a web server, however the basic approach could be applied to other scenarios. The first step in the process is to
obtain a Service Ticket (ST) for a SAML Service with the local site. The workstation could initiate this either from a signed applet or an application running.

3. Having obtained the SAML Service ST, the application (or applet) then sends a request to the SAML service to generate a SAML Assertion. A new protocol will require to be defined for this interaction.

4. The SAML Service will then extract the user identification and PAC attributes from the ST and provide this to the Credential Conversion Service.

5. The Credential Conversion Service provides back to the SAML Service the SAML Assertion, which is then cached for later usage.

6. The SAML Service responds back to the application/applet an artifact (as per SAML 1.0/1.1) that references the previously generated SAML assertion.

7. The Browser on the workstation then attempts to gain access to a resource on the remote web site. A HTTP request is made to the Artifact Receiver, identifying the resource being accessed as well as containing the Artifact.

8. The Artifact Receiver, using the artifact sends a SAML request to the originating site’s Responder, which returns the SAML assertion generated in step 5. The SAML assertion is cached and a cookie generated that references the SAML assertion.

9. The Artifact Receiver then sends a redirect message to the workstation for the final destination resource. The message also contains the cookie.

10. The web server on receiving the cookie can then make an access decision according to the statements within the SAML assertion.

Notes:

- Much of the processing of this candidate profile is similar to that of the Browser/Artifact profile defined in SAML 1.0/1.1
- The SAML service in the local site has many of the same features as that of the Inter-Site Transfer Service. Implementations of the SAML Service could be based on, or enhanced of. The Inter-Site Transfer Service

Figure 7 provides an overview of the candidate profile.
3.2.2.2 Kerberos Browser/Post Candidate Profile

The proposed processing is as follows:

1. The user on the workstation authenticates into the local domain/cell/realm, using application software resident on the workstation. Successful authentication results in an appropriate TGT being provided back to the workstation. The user can then access resources in the Local Site.

2. The user then wishes to gain access to a remote site. In this profile the remote site is a web server, however the basic approach could be applied to other scenarios. The first step in the process is to obtain a Service Ticket (ST) for a SAML Service with the local site. The workstation could initiate this either from a signed applet or an application running.

3. Having obtained the SAML Service ST, the application (or applet) then sends a request to the SAML service to generate a SAML Assertion. A new protocol will require to be defined for this interaction.

4. The SAML Service will then extract the user identification and PAC attributes from the ST and provide this to the Credential Conversion Service.

5. The Credential Conversion Service provides back to the SAML Service the SAML Assertion, which is then cached for later usage.

6. The SAML Service responds back to the application/applet the SAML assertion (as per SAML 1.0/1.1).

7. The Browser on the workstation then attempts to gain access to a resource on the remote web site by using a HTTP POST. The POST data contains the SAML assertion.

8. The web server on receiving the POST can then make an access decision according to the statements within the SAML assertion.
Notes:

- Much of the processing of this candidate profile is similar to that of the Browser/POST profile defined in SAML 1.0/1.1

Figure 8 provides an overview of the candidate profile.

![Figure 8 – Browser/Kerberos Use case](image-url)