Kerberos SAML Profiles

Working Draft 02, 1st February 2004

Document identifier:

draft-sstc-solution-profile-kerberos-02

Location:


Editors:

John Hughes, Entegrity Solutions (john.hughes@entegrity.com)
Tim Alsop, CyberSafe Limited (tim.alsop@cybersafe.ltd.uk)

Contributors:

TBD

Abstract:

This document describes the profiles for using the Kerberos protocol with SAML to provide a Single Sign-On ("SSO") service to users and applications, and/or provide integration with an existing Kerberos authentication infrastructure that might be deployed.

Status:

Interim draft. Please send comments to the editors.

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

1 Introduction.................................................................................................................................3
  1.1 Terminology............................................................................................................................3
2 Using Kerberos with SAML............................................................................................................4
  2.1 Overview....................................................................................................................................4
  2.2 Secure communication between components..........................................................................5
  2.3 Secure communication with SAML Service..............................................................................5
  2.4 Securing communication between SAML Service and Responder........................................5
3 Solution Components....................................................................................................................6
  3.1 SAML Service..........................................................................................................................6
    3.1.1 SOAP binding...................................................................................................................6
      3.1.1.1 Element <SubjectRequestArtifact>.............................................................................6
      3.1.1.2 Element <SubjectRequestAssertion>...........................................................................6
      3.1.1.3 Element <ArtifactResponse>.....................................................................................6
    3.1.2 Non-HTTP binding.............................................................................................................6
  3.2 Authorisation Data...................................................................................................................6
4 Normalisation......................................................................................................................................7
  4.1 Introduction................................................................................................................................7
  4.2 Kerberos.....................................................................................................................................7
  4.3 Microsoft Windows Kerberos...................................................................................................7
5 SAML Defined Identifiers................................................................................................................8
  5.1 Authentication Method Identifiers.........................................................................................8
    5.1.1 Kerberos...........................................................................................................................8
  5.2 NameIdentifier Format Identifiers.......................................................................................8
    5.2.1 Kerberos Principal Name..................................................................................................8
6 References.........................................................................................................................................9
  6.1 Normative References...............................................................................................................9
1 Introduction

This document explains how the Kerberos protocol can be used in conjunction with SAML in order to:

1. Provide a secure and trusted mechanism to pass a user identity to the SAML Responder via the SAML Service so that an artifact or assertion can be returned using the authenticated identity of the user. See [SAML20AuthN] for a generalised description of this secure communication;
2. Provide a secure and trusted mechanism to allow the SAML Service to communicate with the SAML Responder;
3. Provide secure sessions (e.g. mutual authentication, data integrity, confidentiality, channel binding, replay attack detection) between the authentication and authorisation related infrastructure components required for a SAML deployment;
4. Implement a Single SignOn ("SSO") experience for users - especially useful when the workstation and/or server operating systems have a Kerberos implementation available and multiple vendors operating systems are used;
5. Take advantage of the credential delegation/forwarding capability in the Kerberos protocol to pass credentials securely from middle tier to back-end tier application and infrastructure components;
6. Provide a secure approach for passing a SAML Assertion to an application that is Kerberos enabled.

The various implementations of Kerberos are catered for in this document, in particular:

1. An implementation based of the Kerberos standard, as defined in [RFC1510];
2. A DCE (Distributed Computing Environment) based implementation;

1.1 Terminology

The key words must, must not, required, shall, shall not, should, should not, recommended, may, and optional in this document are to be interpreted as described in IETF RFC 2119 [RFC2119].
2 Using Kerberos with SAML

2.1 Overview

In this section various scenarios are described where communications between components in a SAML deployment are secured using the Kerberos protocol. Also, the diagram in Figure 1 illustrates the components involved to obtain the user's authenticated identity and pass a message to the SAML Responder via a SAML Service so that an artifact or assertion may be returned.

![Figure 1: Passing user's identity to SAML Responder](image)

In Figure 1, A represents either:

i. A user at a workstation who has authenticated and is using an application (typically a thick client application or a Web browser). The application then passes the user's identity to a server at B or;

ii. A server running an application (e.g. a web server or a server process/service) that has already determined a user's identity and delegates the user's credentials to a server at B.

The communication between A and B, illustrated by (1) in Figure 1 represents a Kerberos based application authentication performed using standard techniques (e.g. A GSS-API initiate context and accept context). The end result is that delegated/forwarded user credentials are available at B so that they can subsequently be used to communicate with C on behalf of the user at A.

B represents either:

i. A user at a workstation who has authenticated and is running an application (e.g. a thick client application or a Web browser). The application presents the user's identity to the SAML Service after first performing any user name mapping that may be required or;

ii. A server running an application (e.g. a web server or a server process/service) that has already determined a user's identity so that it can present the identity to the SAML Service.

The communication between B and C, illustrated by (2) in Figure 1 represents a secure session used to pass the identity of the user at B or A to the SAML Service (e.g. A GSS-API initiate context and accept context). The SAML Service communicates with the Responder over a secure session (3) and then sends an artifact or assertion to B.

The SAML Service and SAML Responder may actually be deployed on the same server and so the secure session between these components may not be considered to be as important. However, it is RECOMMENDED that a secure session is still implemented regardless of the deployment approach chosen at C.
2.2 Secure communication between components

This section describes various technologies that may be used to pass a Kerberos authenticated identity between components.

i. Client to Server:
   a) GSS-API initiate/accept with channel bindings, mutual authentication and integrity enabled;

ii. Browser to Web server:
   a) TLS with Kerberos 5 Cipher as defined in [RFC2712],
   b) SASL/HTTP; [Also explore how this can be used with SASL/GSS/Kerberos]
   c) SPNEGO/GSS – as used by Microsoft in IE and IIS and also available as a plugin for many commercial and non-commercial web server products.

iii. SOAP bindings. See [SAML20Soap] for more details. [Need to describe when SOAP is appropriate and how it will work with Kerberos Profile]

iv. Other ???

[This section is not complete – more details required for each of above]

2.3 Secure communication with SAML Service

[This section is not complete]

When the Kerberos authenticated identity is available at B, the user's Kerberos session key issued by the KDC at the time the user authenticated should be used to bind with the assertion. [Explain how and why]

When B communicates with C an <AuthnRequest> message is sent over a non-SOAP transport - e.g. RPC or pure sockets and secured using a GSS-API security context. The use of GSS-API ensures that communication channel binding, mutual authentication, integrity, confidentiality and other Kerberos network security capabilities can easily be implemented. An <AuthnResponse> message is then returned to B in the same GSS-API secured and mutually authenticated session.

In section 4 and 5 of this document an explanation is given regarding how the user's Kerberos principal name is represented in the <AuthnRequest> message and in the SAML Assertion.

2.4 Securing communication between SAML Service and Responder

[This section is not complete]
3 Solution Components

3.1 SAML Service

The SAML Service is a front end to a SAML Responder and is implemented as a Kerberos service with its own unique Kerberos service principal name (e.g. saml20svc/s1.company.com@COMPANY.COM). The SAML Service can be co-located with the SAML Responder or implemented as a simple wrapper. In all cases the connection between the SAML Service and SAML Responder MUST be secure.

3.1.1 SOAP binding

This uses the standard SOAP binding for the SAML protocol as defined in TBD. Two types of requests can be made on the SAML Service, to either request an assertion or an artifact (which refers to a SAML assertion). In both cases the SAML protocol <SubjectQuery> element is extended

3.1.1.1 Element <SubjectRequestArtifact>

This query requests that an artifact is returned for the given subject. The following schema fragment defines the <SubjectRequestArtifact>

TBD

The SAML Service MUST validate that the identity supplied in the Service Tick matches that in the <Subject> element.

3.1.1.2 Element <SubjectRequestAssertion>

This query requests that an assertion is returned for the given subject. The following schema fragment defines the <SubjectRequestAssertion>

TBD

The SAML Service MUST validate that the identity supplied in the Service Tick matches that in the <Subject> element.

3.1.1.3 Element <ArtifactResponse>

When an Artifact is requested using the query SubjectRequestArtifact, the SAML response contains a <ArtifactResponse> element. The following schema fragment defines the <ArtifactResponse> element

TBD

3.1.2 Non-HTTP binding

TBD

3.2 Authorisation Data

TBD – refer to following section
4 Normalisation

4.1 Introduction

TBD

4.2 Kerberos

TBD

Example of how a Kerberos principal name is carried within a SAML Assertion.

```xml
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
    MajorVersion="1"
    MinorVersion="1"
    AssertionID="P1YaAztP6UfswxAjax5TPxQ"
    Issuer="www.entegrity.com"
    IssueInstant="2002-06-19T17:05:37.795Z">
    <saml:Conditions NotBefore="2002-06-19T17:00:37.795Z"
        NotOnOrAfter="2002-06-19T17:10:37.795Z"/>
    <saml:AuthenticationStatement
        AuthenticationMethod="urn:ietf:rfc:1510"
        AuthenticationInstant="2002-06-19T17:05:17.706Z">
        <saml:Subject>
            <saml:NameIdentifier
                NameQualifier="http://www.entegrity.com/"
                Format="urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos"
                talsoCYBERSAFE.LTD.UK>
                <saml:SubjectConfirmation>
                    <saml:ConfirmationMethod>
                        urn:oasis:names:tc:SAML:1.0:cm:artifact
                    </saml:ConfirmationMethod>
                    <saml:ConfirmationMethod>
                        AAGZE1RNQJEFzYNCGAGFJWvtDIRSZ4lWDqBphqA
                    </saml:ConfirmationMethod>
                </saml:SubjectConfirmation>
            </saml:NameIdentifier>
        </saml:Subject>
    </saml:AuthenticationStatement>
</saml:Assertion>
```

4.3 Microsoft Windows Kerberos

TBD. How Windows PAC attributes are mapped into SAML Attribute Statements.

Need to check potential patent/license issues with reference to PAC contents
5 SAML Defined Identifiers

5.1 Authentication Method Identifiers

5.1.1 Kerberos

URI: urn:ietf:rfc:1510

The authentication was performed by means of the Kerberos protocol [RFC1510], an instantiation of the Needham-Schroeder symmetric key authentication mechanism [Needham78].

5.2 NameIdentifier Format Identifiers

5.2.1 Kerberos Principal Name

URI: urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos

Indicates that the content of the <NameIdentifier> element is in the form of a Kerberos principal name.
6 References

6.1 Normative References


[Needham78] ???


TBD
A. Acknowledgments

The editors would like to acknowledge the contributions of the OASIS Security Services Technical Committee, whose voting members at the time of publication were:

- TBD
## B. Revision History

<table>
<thead>
<tr>
<th>Rev</th>
<th>Date</th>
<th>By Whom</th>
<th>What</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>8th Jan 2004</td>
<td>John Hughes</td>
<td>Initial version.</td>
</tr>
<tr>
<td>02</td>
<td>1st Feb 2004</td>
<td>Tim Alsop</td>
<td>Changed format of so a more generic approach is presented with references to complementary bindings and profiles drafts when applicable.</td>
</tr>
</tbody>
</table>
C. Notices

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS’s procedures with respect to rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification, can be obtained from the OASIS Executive Director.

OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to implement this specification. Please address the information to the OASIS Executive Director.

Copyright © OASIS Open 2004. All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself does not be modified in any way, such as by removing the copyright notice or references to OASIS, except as needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an “AS IS” basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.