Kerberos SAML Profiles

Working Draft 03, 10th February 2004

Document identifier:
draft-sstc-solution-profile-kerberos-03

Location:
http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

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

Contributors:
Scott Cantor, Individual
Jeff Hodges, Sun Microsystems
Ron Monzillo, Sun Microsystems

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

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 Authentication Authority via the SAML Service so that an artifact or assertion can be returned using the authenticated identity of the user;
2. 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;

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;
3. A deployment of Microsoft Kerberos, as implemented in Windows 2000, XP and 2003.

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 [RFC2119].

2 Using Kerberos with SAML

2.1 Creating an Assertion using user's Kerberos identity

The diagram in Figure 1 illustrates the components involved to obtain the user's authenticated identity and pass a message on to the SAML Authentication Authority via a SAML Service so that an artifact or assertion may be returned.

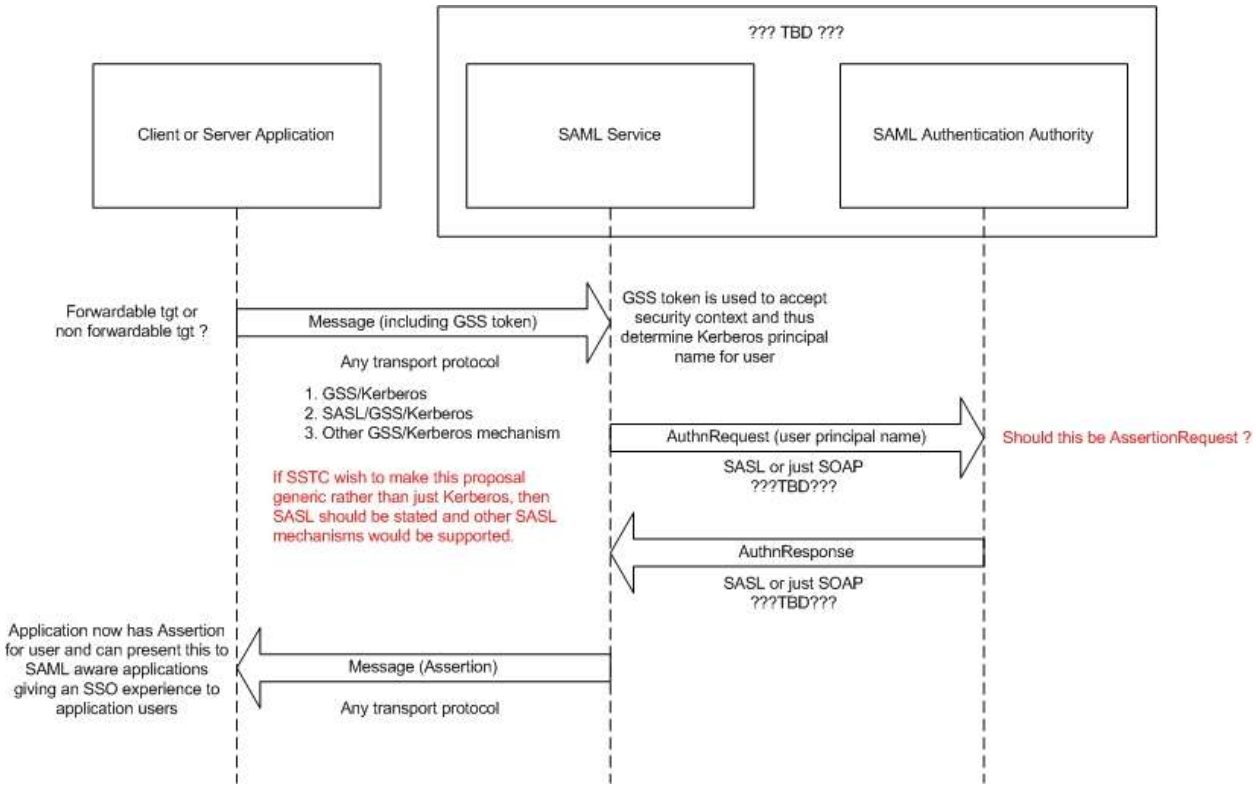

Figure 1 : Passing user's identity to SAML Authentication Authority

In the above diagram the Client, or Server Application which has already identified the Kerberos principal name of the user (maybe during logon to system, or via a Web server plugin, or some other method) can setup a security context using GSS-API, or SASL (likely SASL/GSS/Kerberos). This context allows the SAML Service to determine the user's identity and request that the Authentication Authority issues an assertion.

Outstanding questions – to be discussed during focus call on Tuesday 10th February, 2004.

1. Is this diagram correctly representing the SAML components that are involved ?
2. Should we be using AssertionRequest, or AuthnRequest ?
3. What do we call the combination of SAML Service + SAML AA ? Is there a name for this already ?
4. Do we document the use of SASL for security context, or be more specific ?
5. Should SAML Service be called SAML Kerberos Service, or generic, supporting multiple authentication protocols ?
6. Is the use of SOAP for securing the Assertion Request appropriate, or should we use SASL and mention SASL with a SOAP profile.

2.2 Creating an Assertion using Kerberos service tickets

2.2.1 Option 1

The diagram in Figure 2 represents a scenario where Kerberos tickets are stored in the Assertion. This allows closer association between the trusted Kerberos identity of the user requesting the assertion and the name stored in the NameIdentifier. This also allows improved verification of Assertion's.

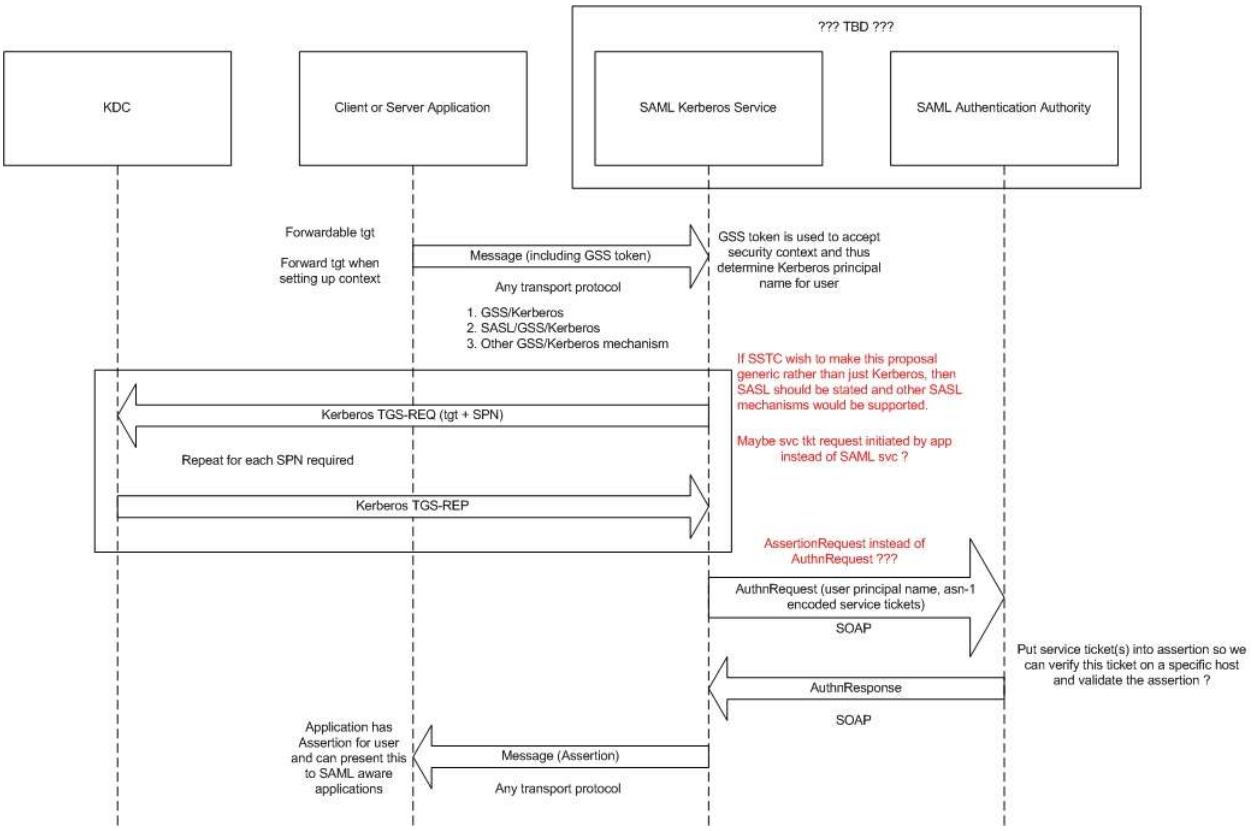

Figure 2 : Storing Kerberos tickets in SAML Assertion (Option 1)

In the above diagram the Kerberos identity is used by the SAML Service to request service tickets which are then put into the Assertion response by the AA. The Assertion can then be verified by appropriate components in the deployment (either locally, or on remote servers) and the principal name in the service ticket can be compared with the name in the **NameIdentifier**

Outstanding questions – to be discussed during focus call on Tuesday 10th February, 2004.

1. Is this diagram correctly representing the SAML components that are involved ?
2. Should we be using AssertionRequest, or AuthnRequest ?

2.2.2 Option 2

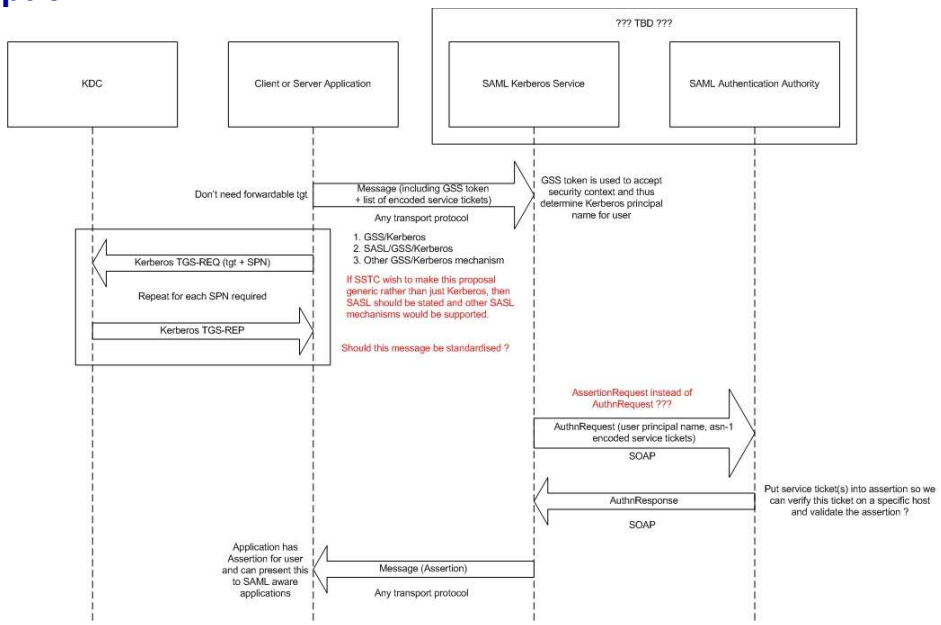

Figure 3 : Storing Kerberos tickets in SAML Assertion (Option 2)

In the above diagram an alternative approach is shown, where the service tickets are obtained by the application and not by the SAML Service (as in Option 1).

2.3 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, or Server to Server :
   a) GSS-API initiate/accept with channel bindings, mutual authentication and integrity enabled;
   b) SASL/GSS/Kerberos;
ii. Browser to Web server :
   a) TLS with Kerberos 5 Cipher as defined in [RFC2712],
   b) SASL/HTTP;
   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. The latest versions of Apache have this included as standard;

Outstanding questions – to be discussed during focus call on Tuesday 10th February, 2004.

1. In addition to the above, we need to understand and describe how and when SOAP should be used.

3 Solution Components Description

3.1 SAML Service

The SAML Service is a front end to a SAML Authentication Authority 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 Authentication Authority or implemented as a simple wrapper. In all cases the connection between the SAML Service and SAML Authentication Authority 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.

```
<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.cybersafe.ltd.uk/"
                    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos">
                    talsop@CYBERSAFE.LTD.UK
               </saml:NameIdentifier>
               <saml:SubjectConfirmation>
                    <saml:ConfirmationMethod>
                         urn:oasis:names:tc:SAML:1.0:cm:artifact
                    </saml:ConfirmationMethod>
                    <saml:SubjectConfirmationData>
                         AAGZE1RNQJEFzYNCGAGPjWvtDIRSZ4lWDqBphqA
                    </saml:SubjectConfirmationData>
               </saml:SubjectConfirmation>
          </saml:Subject>
     </saml:AuthenticationStatement>
</saml:Assertion>
```

4.3 Microsoft Windows Kerberos

Describe how Windows PAC attributes are mapped into SAML Attribute Statements.

Need to check potential patent/license issues with reference to PAC contents

4.4 Distributed Computing Environment (DCE)

The Baseline Attributes (???Document Name TBD???) document describes the format of DCE PAC data in an Assertion.

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

[RFC2119] S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, IETF RFC 2119, March 1997, http://www.ietf.org/rfc/rfc2119.txt.

[RFC1510] J. Kohl, C. Neuman. *The Kerberos Network Authentication Requestor (V5).* IETF RFC 1510, September 1993. http://www.ietf.org/rfc/rfc1510.txt.

[Needham78] ???

[RFC2712] A Medvinsky, M Hur. *Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)*. IETF RFC 2712, October 1999. http://www.ietf.org/rfc/rfc2712.txt.

[SAML20Core] Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. Document ID sstc-saml-core-2.0-draft-02

[SAML20AuthN] Generalised AuthnRequest Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0. Document ID draft-sstc-solution-generalized-authn-01.

[SAML20Soap] SAML Soap Binding. Document ID sstc-saml-bindings-2.0-draft-02 reference section 3.1. Also, Document ID draft-sstc-solution-profile-soap-01

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

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

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.