



---

## 2 Kerberos SAML Profiles

### 3 Working Draft 03, 10<sup>th</sup> February 2004

#### 4 Document identifier:

5 draft-sstc-solution-profile-kerberos-03

#### 6 Location:

7 [http://www.oasis-open.org/committees/documents.php?wg\\_abbrev=security](http://www.oasis-open.org/committees/documents.php?wg_abbrev=security)

#### 8 Editors:

9 Tim Alsop, CyberSafe Limited ([tim.alsop@cybersafe.ltd.uk](mailto:tim.alsop@cybersafe.ltd.uk))

10 John Hughes, Entegrity Solutions ([john.hughes@entegrity.com](mailto:john.hughes@entegrity.com))

#### 11 Contributors:

12 Scott Cantor, Individual

13 Jeff Hodges, Sun Microsystems

14 Ron Monzillo, Sun Microsystems

#### 15 Abstract:

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

#### 19 Status:

20 Interim draft. Please send comments to the editors.

21  
22 Committee members should send comments on this specification to the  
23 [securityservices@lists.oasis-open.org](mailto:securityservices@lists.oasis-open.org) list. Others should subscribe to and send comments to the  
24 [security-services-comment@lists.oasis-open.org](mailto:security-services-comment@lists.oasis-open.org) list. To subscribe, send an email message to  
25 [security-services-comment-request@lists.oasis-open.org](mailto:security-services-comment-request@lists.oasis-open.org) with the word "subscribe" as the body  
26 of the message.  
27

28 For information on whether any patents have been disclosed that may be essential to  
29 implementing this specification, and any offers of patent licensing terms, please refer to the  
30 Intellectual Property Rights section of the Security Services TC web page  
31 (<http://www.oasisopen.org/committees/security/>).

---

## Table of Contents

32		
33	1 Introduction.....	3
34	1.1 Terminology.....	3
35	2 Using Kerberos with SAML.....	4
36	2.1 Creating an Assertion using user's Kerberos identity.....	4
37	2.2 Creating an Assertion using Kerberos service tickets.....	5
38	2.2.1 Option 1.....	5
39	2.2.2 Option 2.....	6
40	2.3 Secure communication between components.....	6
41	3 Solution Components Description.....	7
42	3.1 SAML Service.....	7
43	3.1.1 SOAP binding.....	7
44	3.1.1.1 Element <SubjectRequestArtifact>.....	7
45	3.1.1.2 Element <SubjectRequestAssertion>.....	7
46	3.1.1.3 Element <ArtifactResponse>.....	7
47	3.1.2 Non-HTTP binding.....	7
48	3.2 Authorisation Data.....	7
49	4 Normalisation.....	8
50	4.1 Introduction.....	8
51	4.2 Kerberos.....	8
52	4.3 Microsoft Windows Kerberos.....	8
53	4.4 Distributed Computing Environment (DCE).....	8
54	5 SAML Defined Identifiers.....	9
55	5.1 Authentication Method Identifiers.....	9
56	5.1.1 Kerberos.....	9
57	5.2 NameIdentifier Format Identifiers.....	9
58	5.2.1 Kerberos Principal Name.....	9
59	6 References.....	10
60	6.1 Normative References.....	10
61		

---

62 **1 Introduction**

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

- 64 1. Provide a secure and trusted mechanism to pass a user identity to the SAML Authentication Authority  
65 via the SAML Service so that an artifact or assertion can be returned using the authenticated identity  
66 of the user;
- 67 2. Implement a Single SignOn (“SSO”) experience for users - especially useful when the workstation  
68 and/or server operating systems have a Kerberos implementation available and multiple vendors  
69 operating systems are used;

70

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

- 72 1. An implementation based of the Kerberos standard, as defined in [\[RFC1510\]](#);
- 73 2. A DCE (Distributed Computing Environment) based implementation;
- 74 3. A deployment of Microsoft Kerberos, as implemented in Windows 2000, XP and 2003.

75

76 **1.1 Terminology**

77 The key words *must*, *must not*, *required*, *shall*, *shall not*, *should*, *should not*, *recommended*, *may*, and  
78 *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.

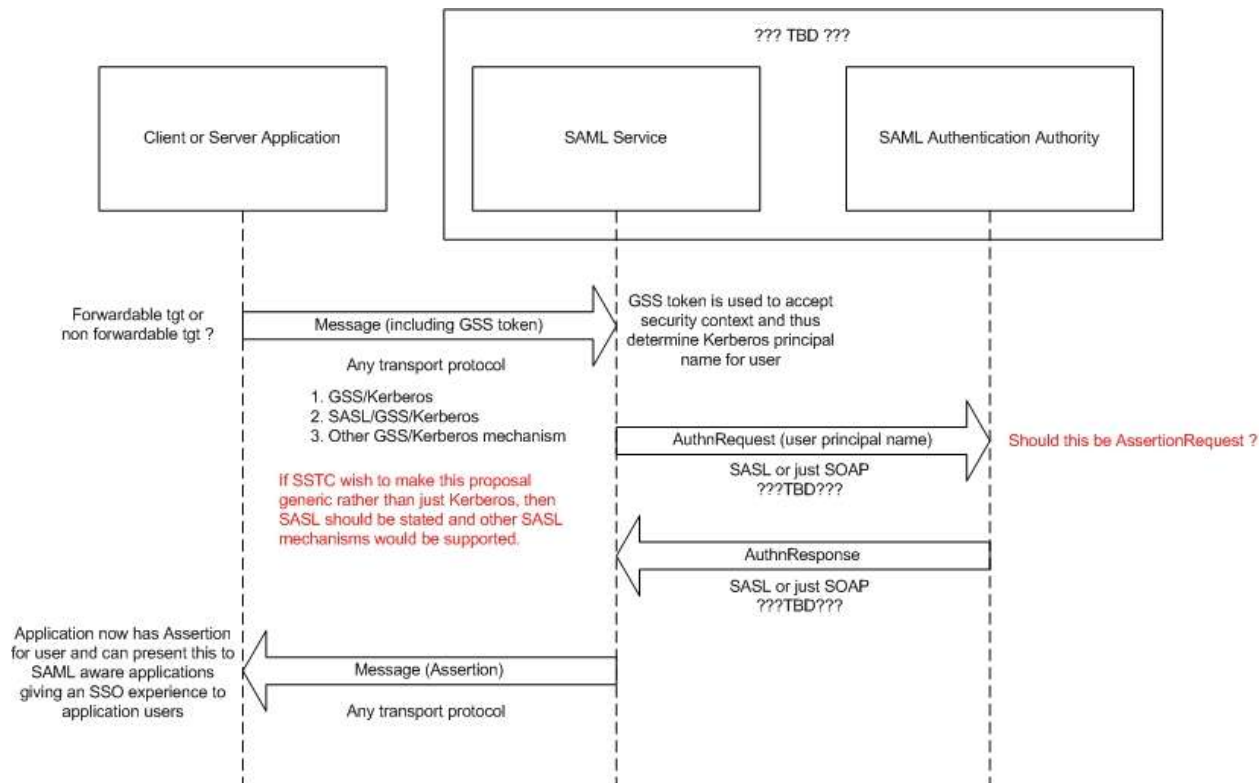


Figure 1 : Passing user's identity to SAML Authentication Authority

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.

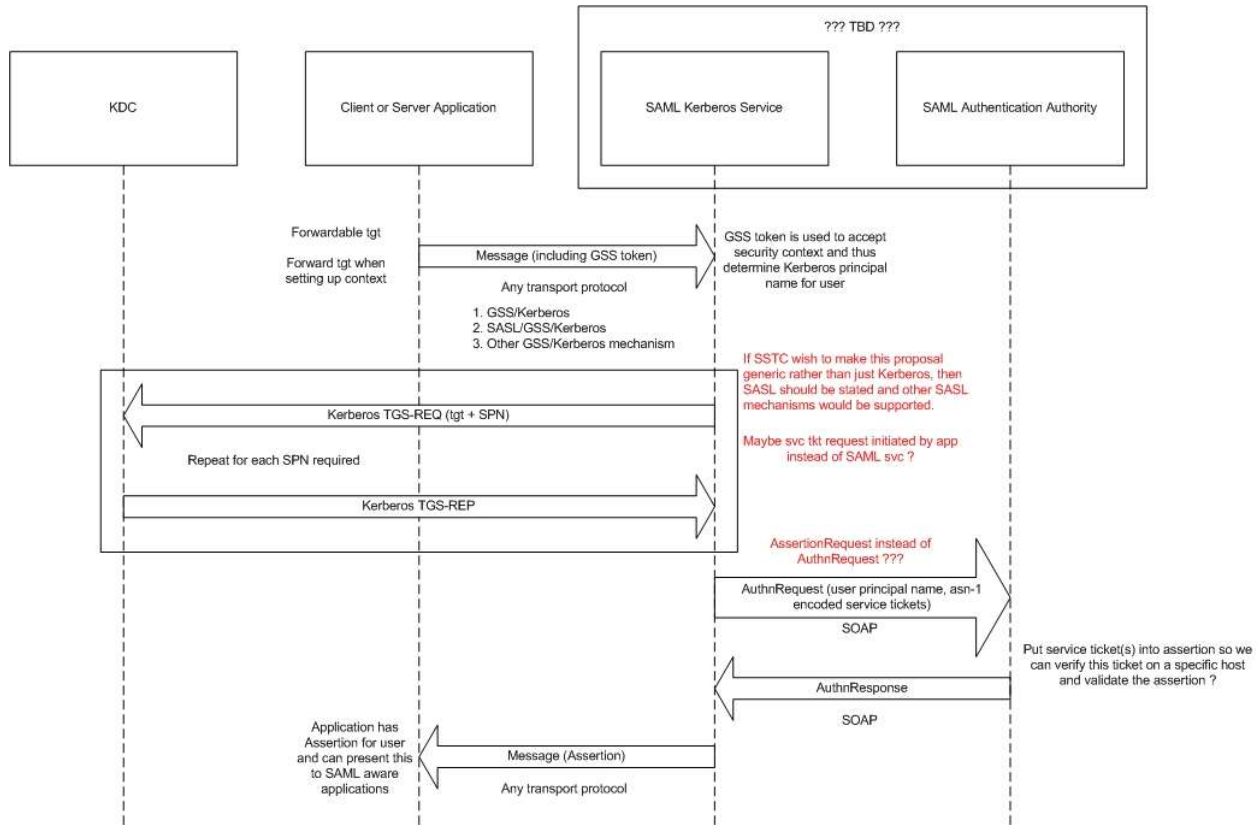
Outstanding questions – to be discussed during focus call on Tuesday 10<sup>th</sup> February, 2004.

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.

102 **2.2 Creating an Assertion using Kerberos service tickets**

103 **2.2.1 Option 1**

104 The diagram in Figure 2 represents a scenario where Kerberos tickets are stored in the Assertion. This  
105 allows closer association between the trusted Kerberos identity of the user requesting the assertion and  
106 the name stored in the NameIdentifier. This also allows improved verification of Assertion's.  
107



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

109

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

114

115 Outstanding questions – to be discussed during focus call on Tuesday 10<sup>th</sup> February, 2004.

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

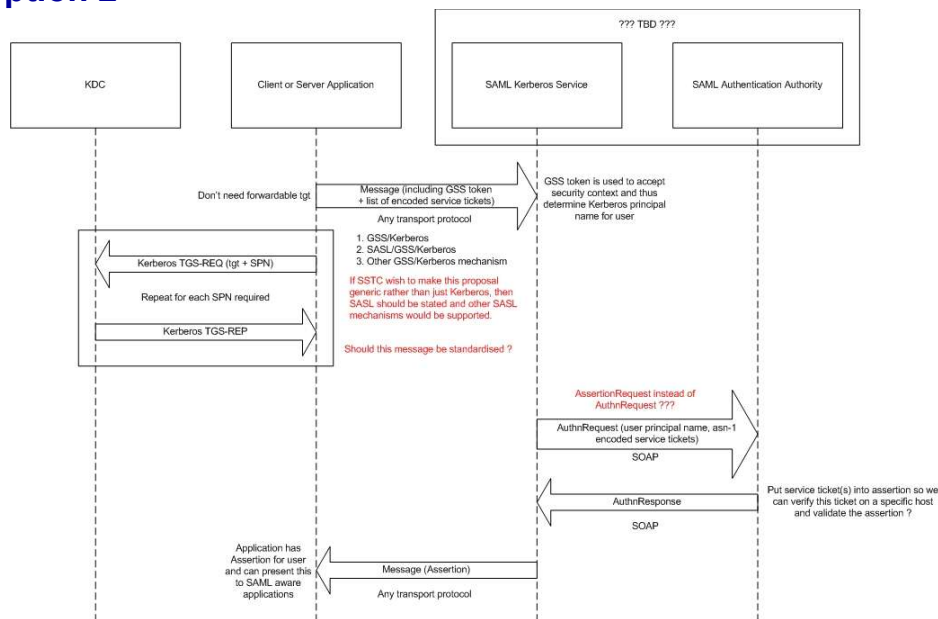
118

119

120

121

122 **2.2.2 Option 2**



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

126 In the above diagram an alternative approach is shown, where the service tickets are obtained by the  
 127 application and not by the SAML Service (as in Option 1).  
 128  
 129

130 **2.3 Secure communication between components**

131 This section describes various technologies that may be used to pass a Kerberos authenticated identity  
 132 between components.  
 133

- 134 i. Client to Server, or Server to Server :
  - 135 a) GSS-API initiate/accept with channel bindings, mutual authentication and integrity enabled;
  - 136 b) SASL/GSS/Kerberos;
- 137 ii. Browser to Web server :
  - 138 a) TLS with Kerberos 5 Cipher as defined in [RFC2712],
  - 139 b) SASL/HTTP;
  - 140 c) SPNEGO/GSS – as used by Microsoft in IE and IIS and also available as a plugin for many
  - 141 commercial and non-commercial web server products. The latest versions of Apache have this
  - 142 included as standard;

144 Outstanding questions – to be discussed during focus call on Tuesday 10<sup>th</sup> February, 2004.

- 145 1. In addition to the above, we need to understand and describe how and when SOAP should be used.  
 146

---

## 147 3 Solution Components Description

### 148 3.1 SAML Service

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

#### 154 3.1.1 SOAP binding

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

##### 158 3.1.1.1 Element `<SubjectRequestArtifact>`

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

161

162 TBD

163

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

##### 166 3.1.1.2 Element `<SubjectRequestAssertion>`

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

169

170 TBD

171

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

##### 174 3.1.1.3 Element `<ArtifactResponse>`

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

178

179 TBD

#### 180 3.1.2 Non-HTTP binding

181 TBD

### 182 3.2 Authorisation Data

183 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.

```
191 <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
192   MajorVersion="1"
193   MinorVersion="1"
194   AssertionID="P1YaAztP6UfswxAjax5TPxQ"
195   Issuer="www.entegrity.com"
196   IssueInstant="2002-06-19T17:05:37.795Z">
197   <saml:Conditions NotBefore="2002-06-19T17:00:37.795Z"
198     NotOnOrAfter="2002-06-19T17:10:37.795Z"/>
199   <saml:AuthenticationStatement
200     AuthenticationMethod="urn:ietf:rfc:1510"
201     AuthenticationInstant="2002-06-19T17:05:17.706Z">
202     <saml:Subject>
203       <saml:NameIdentifier
204         NameQualifier="http://www.cybersafe.ltd.uk/"
205         Format="urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos">
206         talsop@CYBERSAFE.LTD.UK
207       </saml:NameIdentifier>
208       <saml:SubjectConfirmation>
209         <saml:ConfirmationMethod>
210           urn:oasis:names:tc:SAML:1.0:cm:artifact
211         </saml:ConfirmationMethod>
212         <saml:SubjectConfirmationData>
213           AAGZE1RNQJEFzYNGGAGPjWvtDIRSZ4lWDqBphqA
214         </saml:SubjectConfirmationData>
215       </saml:SubjectConfirmation>
216     </saml:Subject>
217   </saml:AuthenticationStatement>
218 </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.



---

228 **5 SAML Defined Identifiers**

229 **5.1 Authentication Method Identifiers**

230 **5.1.1 Kerberos**

231 **URI:** urn:ietf:rfc:1510

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

234 **5.2 NameIdentifier Format Identifiers**

235 **5.2.1 Kerberos Principal Name**

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

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

239  
240

---

## 6 References

241

### 6.1 Normative References

- 242     **[RFC2119]**     S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, IETF  
243                   RFC 2119, March 1997, <http://www.ietf.org/rfc/rfc2119.txt>.
- 244     **[RFC1510]**     J. Kohl, C. Neuman. *The Kerberos Network Authentication Requestor (V5)*.  
245                   IETF RFC 1510, September 1993. <http://www.ietf.org/rfc/rfc1510.txt>.
- 246     **[Needham78]**     ???
- 247     **[RFC2712]**     A Medvinsky, M Hur. *Addition of Kerberos Cipher Suites to Transport Layer*  
248                   *Security (TLS)*. IETF RFC 2712, October 1999.  
249                   <http://www.ietf.org/rfc/rfc2712.txt>.
- 250     **[SAML20Core]**     Assertions and Protocols for the OASIS Security Assertion Markup Language  
251                   (SAML) V2.0. Document ID sstc-saml-core-2.0-draft-02
- 252     **[SAML20AuthN]**    Generalised AuthnRequest Profiles for the OASIS Security Assertion Markup  
253                   Language (SAML) V2.0. Document ID draft-sstc-solution-generalized-authn-01.
- 254     **[SAML20Soap]**    SAML Soap Binding. Document ID sstc-saml-bindings-2.0-draft-02 reference  
255                   section 3.1. Also, Document ID draft-sstc-solution-profile-soap-01
- 256
- 257     **TBD**

---

258 **A. Acknowledgments**

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

- 261 • TBD

262

## B. Revision History

263

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

264

265

## C. Notices

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

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

277 **Copyright © OASIS Open 2004. All Rights Reserved.**

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

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

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