



1

2 **Session Management in SAML 2**

3 **Working Draft 01, 25 September 2003**

4 Document identifier:

5 draft-sstc-session-management-01

6 Location:

7 N/A

8 Editor:

9 John Kemp

10 Abstract:

11 This document proposes candidate scenarios and requirements for session management in SAML 2.0. Subsequent
12 versions will be augmented with use case and mechanism proposals.

13 Status:

14 Interim draft. Send comments to the editors.

15 If you are on the <security-services@lists.oasis-open.org> list for committee members, send comments
16 there. If you are not on that list, subscribe to the <security-services-comment@lists.oasis-open.org> list
17 and send comments there. To subscribe, send an email message to <security-services-comment-request@
18 lists.oasis-open.org> with the word "subscribe" as the body of the message.

19 Copyright © 2003 OASIS Open, Inc. All Rights Reserved.

20 **Table of Contents**

21	1. Introduction	4
22	1.1. Terminology	4
23	1.2. Definitions	4
24	2. Scenarios	4
25	3. Requirements	7
26	4. Notes	8

27 **Appendixes**

28 [A. Committee Members \(Non-Normative\)](#) 8

29 [B. Notices](#) 8

30 [C. Intellectual Property Rights](#) 9

31 [D. Revision History](#) 9

32 [References](#) 9

1. Introduction

This document proposes CANDIDATE scenarios and requirements for session management and logout in SAML 2.0. Subsequent versions will be augmented with use case and mechanism proposals.

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 [RFC 2119].

1.2. Definitions

It should be noted that the following definitions ONLY apply to the use-cases, requirements and other statements made in this document. They CANNOT be assumed to have any particular meaning in any other context.

<i>Session</i>	A period of time, during which a single user's actions are considered to be linked together for the purpose of session state management. Some artifact that when presented by a user may be used to gain access to a service or services under conditions specified by a session authority. Such an artifact may be valid only for a local service, or it may be valid for a set of services (see <i>Shared session</i>).
<i>Service</i>	Some system resource that requires an active session from a user. An example might be a website, or an enterprise software application.
<i>Shared session</i>	A session that is used to gain access to a <i>set</i> of services, not necessarily co-located.
<i>Shared-session ecosystem</i>	Some set of system resources that requires an active session from a user, where each resource may share a session with the other resources in the ecosystem. An example might be a set of enterprise software applications that are used as part of a corporate intranet. AKA simply <i>Ecosystem</i> .
<i>Login</i>	The act of requesting a session. A user who requests a session, and is granted one is said to be <i>logged-in</i> .
<i>Logout</i>	The act of explicitly invalidating or destroying a session. Any attempted access by a user possessing some artifact identifying a session that the user has logged-out of, should be considered as if the user did not possess a session artifact.
<i>Time-out</i>	A period of time, after which, a given session may be considered invalid.
<i>Idle Time-out</i>	A period of time, after which, if there is no activity by the user associated with a session, the session may be considered invalid.
<i>Session Authority</i>	The system entity responsible for creating and managing the session.

2. Scenarios

The following scenarios represent use-cases involving session management:

Note

Liberty scenarios are marked with

[Liberty]

1. User login to a local service [Liberty]

- *Pre:* User accesses a service, has no current session

- *Post:* User receives a local session only

2. User login to an entire ecosystem of services, including the local service [Liberty]

- *Pre:* User access a service, has no current session

- *Post:* User receives a global session, which allows them access (subject potentially to non-session-based policy) to both the service to which they originally requested access, and to other services in the eco-system.

3. User access the same service to which they were originally logged-in, and is granted access, based on their session [Liberty]

- *Pre:* (1) or (2)

- *Post:* User is granted access

4. User accesses a service that is part of a shared-session ecosystem, and is granted access based on their session. [Liberty]

- *Pre:* (2)

- *Post:* User is considered to have an active global session, so they are granted access

5. User explicitly logs out of a single service - not the entire shared-session ecosystem.

- *Pre:* (1) and/or (2)

- *Post:* User must request a new session for this service in order to gain access to it. The user may still have access without acquiring a new local session to other services if they still have a global session with those other services.

95 6. User explicitly logs out of the entire shared-session eco-system [Liberty]
96

97 • *Pre:* (2)

98 • *Post:* User must acquire a new session in order to use ANY of the services in the eco-system.

99 7. User is inactive at a particular service using a specific session for some time period specified by that service for
100 the session, and then requests further service, under that session. (IDLE TIMEOUT)
101

102 • *Pre:* (1) or (2)

103 • *Post:* User is required to acquire a new session to use that service. The user may still have access to other services
104 if (2) and any timeout period specified globally has not been reached

105 8. User is inactive at all services within an eco-system for some time period specified for that specific session, and
106 requests further access to a service in the eco-system, under that specific session. (IDLE TIMEOUT)
107

108 • *Pre:* (2)

109 • *Post:* User is required to acquire a new session to use both the service for which they request access or any other
110 service in that eco-system.

111 9. User is required to acquire a new session for access to some service after some locally-specified period of time,
112 based on a particular session, and regardless of their level of activity. (NON-IDLE TIMEOUT)
113

114 • *Pre:* (1) or (2)

115 • *Post:* User is required to acquire a new session to use that service. The user may still have access to other services
116 if (2) and any timeout or idle period specified globally has not been reached

117 10. User is required to acquire a new session to use any service in the eco-system, based on a specifically identified
118 session, and regardless of their level of activity within the eco-system. (NON-IDLE TIMEOUT)
119

120 • *Pre:* (2) and global timeout expired

121 • *Post:* User is required to acquire a new session to use all services in the eco-system.

122 11. Session Authority invalidates a user's active single service session(s) (for example, the administrator logs all users
123 out of a service within the system).
124

125 • *Pre:* (1) and/or (2)

126 • *Post:* User is required to get a new session to use that service. The user may still have access to other services if
127 (2) and any timeout or idle period specified globally has not been reached, and the Session Authority has not also
128 terminated any shared session required for access.

129 12. Session Authority invalidates a user's active shared session(s) (for example, the administrator logs all users out
130 of the system).
131

132 • *Pre:* (2)

133 • *Post:* User is required to get a new session to use either a single service, or all services in the eco-system.

134 3. Requirements

135 Note

136 Requirements satisfied with the Liberty ID-FF Single Logout protocol and related work are marked with
137 [Liberty]
138 .

139 1. SAML 2.0 shall provide the ability for a service provider to obtain a session from a session authority for a specific
140 user, that allows that user access to the service. The session must be uniquely identified across the realm of all
141 sessions provided by that session authority. [Liberty]

142 2. SAML 2.0 shall provide the ability for a service provider to obtain a *shared* session from a session authority for
143 a specific user, that allows that user access to a group of services who act as relying parties for sessions created
144 by that session authority. [Liberty]

145 3. SAML 2.0 shall provide the ability for a service provider to offer the user access to a local service either using a
146 session targetted at that local service, or one which is provided for use across a shared-session ecosystem. (Note:
147 this might imply that a user could log out of their local or shared session, and still have access to the local service,
148 based on the terms of the *other* session they might hold. [Not precluded by Liberty]

149 4. SAML 2.0 shall provide a solution that allows the user to indicate a preferred idle timeout period for a session to
150 the service provider.

151 5. SAML 2.0 shall provide a solution that allows a service provider to indicated both their own preferred timeout
152 period, and possibly also that of a user to a session authority.

153 6. SAML 2.0 shall provide the ability for a service provider to notify a session authority of a user logout for a shared
154 session. (Note: They could also notify of logout from a local session, but I'm not sure that this is required?)
155 [Liberty]

156 7. SAML 2.0 shall enable the session authority to create a shared session for use by relying parties. Sessions should
157 be identified in such a way that they can be uniquely identified within the realm of all sessions issued by that
158 authority. [Liberty]

159 8. SAML 2.0 shall enable the session authority to indicate idle, or non-idle timeout periods on a specific session.
160 In some environments it may be possible for the user or service provider to indicate the timeout period(s) they'd
161 like to use, but as a matter of policy, the session authority should probably have control over this.

- 162 9. SAML 2.0 shall enable the session authority to notify shared-session recipients of session timeouts either due to
163 user idleness, or some set timeout period being exceeded. [Liberty]
- 164 10. SAML 2.0 shall provide the ability for the authority to notify shared-session recipients of user logout (when user
165 logs out at session authority) [Liberty]
- 166 11. SAML 2.0 shall provide the ability for the authority to notify shared-session recipients of session invalidation by
167 Session Authority (eg. if an administrator were to log the user out). [Liberty]

168 4. Notes

- 169 • Authentication is not assumed. A Session Authority may be co-located with or be an Authentication Authority,
170 but it is not required. It is assumed that if authentication is required that the Session Authority and Authentication
171 Authority have some basis for mutual trust, and can transact securely.
- 172 • Service providers receiving sessions from a Session Authority are assumed to have some basis for trusting the
173 Session Authority.
- 174 • It is possible for a user to have multiple valid sessions for either a single service, or an entire shared-session
175 ecosystem. This might occur due to a user logging in from multiple locations while previous sessions existed
176 (ie. from a mobile phone while travelling to work, and their personal computer when arriving, without first
177 logging/timing out from the mobile phone.

178 A. Committee Members (Non-Normative)

179 The following individuals were members of the committee during the formulation of this document:

180 B. Notices

181 Copyright © The Organization for the Advancement of Structured Information Standards [OASIS] 2001, 2002. All
182 Rights Reserved.

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

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

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

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

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

205 OASIS has been notified of intellectual property rights claimed in regard to some or all of the contents of this
206 specification. For more information consult the online list of claimed rights.

207 **C. Intellectual Property Rights**

208 For information on whether any patents have been disclosed that may be essential to implementing this specification,
209 and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the {technical-
210 committee} web page (<http://www.oasis-open.org/committees/{technical-committee}>)

211 **D. Revision History**

Revision 01	25 Sept 2003	jk
First full draft with feedback from F2F.		

212 **References**

213 **Normative**

214 [RFC 2119] S. Bradner. *RFC 2119: Key words for use in RFCs to Indicate Requirement Levels*
215 [<http://www.ietf.org/rfc/rfc2119.txt>]. IETF (Internet Engineering Task Force). 1997.

216 **Informative**

217 [DynSessWD] D.Orchard, G.Pilz, eds. *OASIS Security Services Dynamic Session Specification*
218 [<http://www.ietf.org/rfc/rfc2119.txt>]. Working Draft. 2001.