



1 **eGov Profile**

2 **SAML 2.0**

3 **Version 1.5**

4 **Editor:**

5 Kyle Meadors, Drummond Group Inc.

6 **Abstract:**

7 This document describes the eGovernment profile for SAML 2.0.

8 **Filename:**

9 Liberty_Alliance_eGov_Profile_1.5_Final.pdf



10 Notice

11 This document has been prepared by Sponsors of the Liberty Alliance. Permission is hereby granted
12 to use the document solely for the purpose of implementing the Specification. No rights are granted
13 to prepare derivative works of this Specification. Entities seeking permission to reproduce portions
14 of this document for other uses must contact the Liberty Alliance to determine whether an
15 appropriate license for such use is available.

16 Implementation or use of certain elements of this document may require licenses under third party
17 intellectual property rights, including without limitation, patent rights. The Sponsors of and any
18 other contributors to the Specification are not and shall not be held responsible in any manner for
19 identifying or failing to identify any or all such third party intellectual property rights. This
20 Specification is provided "AS IS," and no participant in the Liberty Alliance makes any warranty of
21 any kind, express or implied, including any implied warranties of merchantability, non-infringement
22 of third party intellectual property rights, and fitness for a particular purpose. Implementers of this
23 Specification are advised to review the Liberty Alliance Project's website
24 (<http://www.projectliberty.org/>) for information concerning any Necessary Claims Disclosure
25 Notices that have been received by the Liberty Alliance Management Board.

26 Copyright © 2009 ActivIdentity, Trent Adams, Adetti, Adobe Systems, AOL, BEA Systems, Berne,
27 University of Applied Sciences, Gerald Beuchelt, BIPAC, John Bradley, British
28 Telecommunications plc, Hellmuth Broda, Bronnoysund Register Centre, BUPA, CA, Canada Post
29 Corporation, Center for Democracy and Technology, Chief, Information Office Austria, China
30 Internet Network Information Center (CNNIC), ChoicePoint, Citi, City University, Clarity
31 Security, Dan Combs, Computer & Communications Industry Association, Courion Corporation,
32 Danish Biometrics Research Proj. Consortium, Danish National IT and Telecom Agency, Deny All,
33 Deutsche Telekom AG, DGME, Diversinet Corp., Drummond Group Inc., East of England
34 Telematics Development Trust Ltd, EIFEL, Electronics and Telecommunications Research Institute
35 (ETRI), Engineering Partnership in Lancashire, Enterprise Java Victoria Inc., Entr'ouvert, Ericsson,
36 eValid8, Evidian, Fidelity Investments, Financial Services Technology Consortium (FSTC), Finland
37 National Board of Taxes, Fischer International, France Telecom, Fraunhofer-Gesellschaft,
38 Fraunhofer Institute for Integrated Circuits IIS, Fraunhofer Institute for Secure Information
39 Technology (SIT), Fraunhofer Institut for Experimentelles Software Engineering, Fugen Solutions,
40 Fujitsu Services Oy, Fun Communications GmbH, Gemalto, Giesecke & Devrient GMBH, Global
41 Platform, GSA Office of Governmentwide Policy, Healthcare Financial Management Association
42 (HFMA), Health Information and Management Systems Society (HIMSS), Helsinki Institute of
43 Physics, Jeff Hodges, Hongkong Post, Guy Huntington, Imprivata, Information Card Foundation,
44 Institute of Bioorganic Chemistry Poland, Institute of Information Management of the University,
45 Institut Experimentelles Software Engineering (IESE), Intel Corporation, International Institute of
46 Telecommunications, International Security, Trust and Privacy Alliance, Internet2, Interoperability
47 Clearinghouse (ICH), ISOC, Java Wireless Competency Centre (JWCC), Kantega AS, Kuppinger
48 Cole & Partner, Kuratorium OFFIS e.V., Colin Mallett, Rob Marano, McMaster University,
49 MEDNETWorld.com, Methics Oy, Mortgage Bankers Association (MBA), Mydex, National
50 Institute for Urban Search & Rescue Inc NEC Corporation, Network Applications Consortium
51 (NAC), Neustar, Newspaper Association of America, New Zealand Government State Services
52 Commission, NHK (Japan Broadcasting Corporation) Science & Technical Research Laboratories,

53 Nippon Telegraph and Telephone Company, Nokia Corporation, Nortel, NorthID Oy, Norwegian
54 Agency for Public Management and eGovernment, Norwegian Public Roads Administration, Novell,
55 NRI Pacific, Office of the Information Privacy Commissioner of Ontario, Omnibranch, OpenIAM,
56 Oracle USA, Inc., Organisation Internationale pour la Sécurité des Transactions Électroniques
57 (OISTE), Oslo University, Our New Evolution, PAM Forum, Parity Communications, Inc., PayPal,
58 Phase2 Technology, Ping Identity Corporation, Bob Pinheiro, Platinum Solutions, Postsecondary
59 Electronic Standards Council (PESC), Purdue University, RSA Security, Mary Ruddy, SAFE
60 Biopharma, SanDisk Corporation, Shidler Center for Law, Andrew Shikiar, Signicat AS, Singapore
61 Institute of Manufacturing Technology, Software & Information Industry Association, Software
62 Innovation ASA, Sprint Nextel Corporation, Studio Notarile Genghini-SNG, Sunderland City
63 Council, SUNET, Sun Microsystems, SwissSign AG, Technische Universität Berlin, Telefonica
64 S.A., TeleTrusT, TeliaSonera Mobile Networks AB, TERENA, Thales e-Security, The Boeing
65 Company, The Financial Services Roundtable/BITS, The Open Group, The University of Chicago
66 as Operator of Argonne National Laboratory, TRUSTe, tScheme Limited, UNINETT AS,
67 Universidad Politecnica de Madrid, University of Birmingham, University of Kent, University of
68 North Carolina at Charlotte, University of Ottawa (TTBE), U.S. Department of Defense, VeriSign,
69 Vodafone Group Plc, Web Services Competence Center (WSCC), Zenn New Media

70 All rights reserved.
71 Liberty Alliance Project
72 Licensing Administrator
73 c/o IEEE-ISTO
74 445 Hoes Lane
75 Piscataway, NJ 08855-1331, USA
76 info@projectliberty.org
77 Liberty Alliance Project

78	Contents	
79	Introduction.....	3
80	Overview of eGov Profile.....	3
81	Document References.....	3
82	Draft History.....	4
83	Key Words.....	4
84	Conformance Requirements.....	5
85	Web SSO.....	5
86	IdP Discovery.....	5
87	SP Authentication Request.....	5
88	IdP Authentication Response.....	5
89	Assertion.....	5
90	Single Logout.....	6
91	Security.....	6
92	Metadata.....	7
93	General Metadata.....	7
94	<SPSSODescriptor>.....	7
95	<IDPSSODescriptor>.....	7
96	<AttributeAuthorityDescriptor>.....	7
97	Considerations for Version 2.0.....	8

98 Introduction

99 Overview of eGov Profile

100 The eGov profile is a Liberty Alliance defined SAML 2.0 conformance specification for SP and IdP
101 applications operating in approved eGovernment federations and deployments. The eGov profile is
102 based on the SAML 2.0 specifications created by the Security Services Technical Committee
103 (SSTC) of OASIS. It constrains the base SAML 2.0 features, elements, attributes and other values
104 required for approved eGovernment federations and deployments. Unless otherwise specified,
105 SAML operations and features follow those found in the OASIS SAML 2.0 specifications.

106 This eGov profile *does not* reflect which aspects of SAML the individual governments must utilize
107 in their respective federations. Thus, it is not a deployment level profile. This eGov profile *does*
108 reflect the SAML features that vendors must implement within their product offerings to satisfy SP
109 and IdP functionality necessary to be conformant to this profile.

110 Document References

- 111 [SAMLAuthnCxt] J. Kemp et al, “Authentication Context for the OASIS Security Assertion
112 Markup Language (SAML) V2.0,” OASIS SSTC (March 2005), [http://
113 docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf).
- 114 [SAMLBind] Scott Cantor et al, “Bindings for the OASIS Security Assertion Markup
115 Language (SAML) V2.0,” OASIS SSTC (March 2005), [http://docs.oasis-
116 open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf)
- 117 [SAMLConf] Prateek Mishra et al, “Conformance Requirements for the OASIS Security
118 Assertion Markup Language (SAML) V2.0,” OASIS SSTC (March 2005).
119 <http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf>.
- 120 [SAMLCore] S. Cantor et al, “Assertions and Protocols for the OASIS Security Assertion
121 Markup Language (SAML) V2.0,” OASIS SSTC (March 2005),
122 <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>.
- 123 [SAMLerrata] Jahan Moreh, “Errata for the OASIS Security 2 Assertion Markup Language
124 (SAML) V2.0, Working Draft 28,” OASIS SSTC (May 8, 2006),
125 [http://www.oasis-open.org/committees/download.php/18070/sstc-saml-errata-
126 2.0-draft-28.pdf](http://www.oasis-open.org/committees/download.php/18070/sstc-saml-errata-2.0-draft-28.pdf).
- 127 [SAMLGloss] J. Hodges et al. Glossary for the OASIS Security Assertion Markup Language
128 (SAML) V2.0. OASIS SSTC, March 2005. Document ID saml-glossary-2.0-
129 os. See <http://www.oasis-open.org/committees/security/>.
- 130 [SAMLMeta] S. Cantor et al, “Metadata for the OASIS Security Assertion Markup
131 Language (SAML) V2.0,” OASIS SSTC (March 2005), [http://docs.oasis-
132 open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf).
- 133 [SAMLMetaExt] Tom Scavo et al, “SAML Metadata Extension for Query Requesters,
134 Committee Draft 01”, OASIS SSTC (March 2006), <http://www.oasis->

- 135 open.org/committees/download.php/18052/sstc-saml-metadata-ext-query-cd-
136 01.pdf
- 137 [SAMLProf] S. Cantor et al, “Profiles for the OASIS Security Assertion Markup Language
138 (SAML) V2.0,” OASIS SSTC (March 2005), [http://docs.oasis-
139 open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf).
- 140 [SAMLSec] Frederick Hirsch et al, “Security and Privacy Considerations for the OASIS
141 Security Assertion Markup Language (SAML) V2.0,” OASIS SSTC (March
142 2005), [http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-
143 os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf)

144 **Draft History**

- 145 • Draft F
- 146 Added requirement on <SubjectConfirmationData> and changed SLO binding as “SOAP”
147 rather than “SOAP Artifact”.
- 148 • Draft E
- 149 Removed “TEST” bullets added in Draft D.
- 150 • Draft D
- 151 Removed many requirements which were redundant to the base SAML requirements.
152 Clarified other requirements. Removed the document defined key word “SUPPORT” and not
153 only use RFC 2119 defined key words. Added “TEST” bullets stating how stated
154 requirements are currently tested in the Liberty test plan and what new test specifications are
155 needed.
- 156 • Draft C
- 157 Defined constrained conformance requirements for complying SPs and IdPs.
- 158 • Draft B
- 159 Based on initial feedback, this Draft placed requirements in align, nearly aligned and non-
160 aligned groups to determine where the differences were in terms of expectations.
- 161 • Draft A
- 162 First attempt to reconcile requirements of US, New Zealand and Denmark governments.
163 Utilized the “Comparison and Analysis of Government Web Browser SSO Profiles” input
164 from the Liberty eGov SIG.
- 165 • eGov Profile 1.0
- 166 The eGov Profile 1.0 follows the SAML 2.0 requirements for the General Service
167 Administration (GSA) of the US Government. It was tested in the Liberty Alliance 2008
168 SAML 2.0 IOP event.

169 **Key Words**

170 The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD",
171 "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be
172 interpreted as described in RFC 2119.

173 Conformance Requirements

174 Web SSO

- 175 • SSO profile in [SAMLProf] MUST be supported by both SP and IdP with both capable of
176 initiation. Unsolicited IdP <Response> messages MUST be supported.

177 IdP Discovery

- 178 • IdP Discovery MUST be supported.
- 179 • If a common domain cookie (CDC) exists the SP MUST SUPPORT functionality of
180 presenting the user with a tailored list of compatible Identity Providers featuring, at a
181 minimum, the compatible Identity Providers in the CDC.

182 SP Authentication Request

- 183 • MUST be communicated using HTTP Redirect binding.
- 184 • *isPassive* MUST be supported. It MAY be used when the IdP is not to take direct control. If
185 *isPassive* is true, the Identity Provider and client MUST NOT take over the user interface.
- 186 • *ForceAuthn* MUST be supported. It MAY be used to require the IdP to force the end user to
187 authenticate.
- 188 • <AuthnRequest> MUST be signed.
- 189 • <NameIDPolicy> MUST be supported and MUST SUPPORT formats of 'persistent',
190 'transient' and 'unspecified'.
- 191 • <RequestedAuthnContext> MUST be supported. IdP MUST recognize *Comparison* field and
192 evaluate the requested context classes.

193 IdP Authentication Response

- 194 • MUST be communicated using HTTP POST binding or SOAP Artifact binding.
- 195 • Assertion MUST be encrypted when using POST binding.
- 196 • The *Consent* attribute MUST be supported. The *Consent* values which MUST be supported,
197 but not limited to, are:
 - 198 • urn:oasis:names:tc:SAML:2.0:consent:obtained
 - 199 • urn:oasis:names:tc:SAML:2.0:consent:prior
 - 200 • urn:oasis:names:tc:SAML:2.0:consent:current-implicit
 - 201 • urn:oasis:names:tc:SAML:2.0:consent:current-explicit
 - 202 • urn:oasis:names:tc:SAML:2.0:consent:unspecified

203 Assertion

- 204 • Assertion MUST be signed.

- 205 • MUST have one <AuthnStatement> present. SessionIndex parameter MUST be present and
206 SessionNotOnOrAfter MUST NOT be present.
- 207 • MUST support <AttributeStatement> and MAY contain up to one <AttributeStatement>.
- 208 • MUST support NameFormat of <Attribute> values of “basic”, “uri” and “unspecified”.
- 209 • <AttributeStatement> MUST use <Attribute> and MUST NOT use <EncryptedAttribute>.
- 210 • The <SubjectConfirmationData> attributes *NotOnOrAfter* MUST be supported.
- 211 • The <Conditions> attributes *NotBefore* and *NotOnOrAfter* MUST be supported.
- 212 • The <Conditions> element <AudienceRestriction> MUST be supported.

213 **Single Logout**

- 214 • SP-initiated Single Logout and IdP-initiated Single Logout MUST be supported.
- 215 • Single Logout binding MAY be HTTP Redirect or SOAP.
- 216 • <LogoutRequest> MUST be signed.
- 217 • <LogoutResponse> MUST be signed.
- 218 • SP MUST offer user choice between local logout from SP only or SLO.
- 219 • User SHOULD confirm logout. If Single Logout is unsuccessful, user MUST be informed.

220 **Security**

- 221 • The minimum requirements for algorithm, key length and other security requirements are
222 defined in Section 4 of [SAMLConf]. eGov applications and deployments MUST follow
223 those minimum requirements.
- 224 • Utilization of a certificate authority and other security practices not defined in this profile are
225 deployment decisions outside the scope of this profile.
- 226 • <AuthnRequest>, <SingleLogoutRequest> and <SingleLogoutResponse>
227 messages SHOULD use HTTPS over SSL (v3.0 or higher) or TLS (v1.0 or higher) to
228 establish a security context with the user agent (web browser) but earlier versions of SSL are
229 permissible.

230 Metadata

231 The choice of Metadata information is largely a deployment level decision. However, all conformant
232 SP and IdP implementations MUST support the consumption and proper use of all Metadata
233 elements, attributes and specifications listed in this section.

234 General Metadata

- 235 • SP and IdP SHOULD authenticate metadata before using it.
- 236 • The exchange of metadata is outside the scope of this profile.
- 237 • Signing of Metadata MUST be supported.
- 238 • MUST support root elements of <EntityDescriptor> or <EntitiesDescriptor>.
- 239 • <Organization> MUST be supported.
- 240 • Attributes *validUntil* AND *cacheDuration* MUST be supported.
- 241 • Certificates consumption and use in metadata MUST be supported.
- 242 • Certificate revocation methods of Online Certificate Status Protocol (OCSP), Certificate
243 Revocation List (CRL), CRL Distribution Point (CDP) Extension MUST be supported.

244 <SPSSODescriptor>

- 245 • <KeyDescriptor> MUST be supported.
- 246 • <SingleLogOutService> MUST be supported.
- 247 • *WantAssertionSigned* MUST be supported.
- 248 • *AuthnRequestsSigned* MUST be supported.

249 <IDPSSODescriptor>

- 250 • <KeyDescriptor> MUST be supported.
- 251 • *WantAuthnRequestsSigned* MUST be supported.
- 252 • <SingleLogOutService> MUST be supported.
- 253 • <SingleSignOnService> MUST be supported.

254 <AttributeAuthorityDescriptor>

- 255 • <AttributeAuthorityDescriptor> MUST be supported.

256 Considerations for Version 2.0

257 This section is a “catch all” for pertinent issues that need to be addressed in the next version of the
258 eGov profile. They are not required for adoption of eGov 1.5 profile. These bullet points exist as
259 reminders and placeholders for future discussion.

- 260 ○ Some don't consider CDC approach to IdP discovery to be an effective model. Suggest
261 putting on roadmap consideration for moving to other discovery service approach.
- 262 ○ On a deployment level, we had stated that optional metadata elements <RoleDescriptor>,
263 <AuthnAuthorityDescriptor>, <PDFDescriptor>, <AffiliationDescriptor> and
264 <AdditionalMetadataLocation> SHOULD NOT be used. However, it is not necessary or
265 particularly wise to state for vendors that they are NOT to support certain elements.
- 266 ○ Metadata and Public Key Infrastructure (PKI) methods need to be better specified to
267 insure interoperability.