



1 Security and Privacy Considerations for 2 the OASIS Security Assertion Markup 3 Language (SAML) V2.0

4 **OASIS Standard, 15 March 2005**

5 **Document identifier:**

6 saml-sec-consider-2.0-os

7 **Location:**

8 <http://docs.oasis-open.org/security/saml/v2.0/>

9 **Editors:**

10 Frederick Hirsch, Nokia
11 Rob Philpott, RSA Security
12 Eve Maler, Sun Microsystems

13 **SAML V2.0 Contributors:**

14 Conor P. Cahill, AOL
15 John Hughes, Atos Origin
16 Hal Lockhart, BEA Systems
17 Michael Beach, Boeing
18 Rebekah Metz, Booz Allen Hamilton
19 Rick Randall, Booz Allen Hamilton
20 Thomas Wisniewski, Entrust
21 Irving Reid, Hewlett-Packard
22 Paula Austel, IBM
23 Maryann Hondo, IBM
24 Michael McIntosh, IBM
25 Tony Nadalin, IBM
26 Nick Ragouzis, Individual
27 Scott Cantor, Internet2
28 RL 'Bob' Morgan, Internet2
29 Peter C Davis, Neustar
30 Jeff Hodges, Neustar
31 Frederick Hirsch, Nokia
32 John Kemp, Nokia
33 Paul Madsen, NTT
34 Steve Anderson, OpenNetwork
35 Prateek Mishra, Principal Identity
36 John Linn, RSA Security
37 Rob Philpott, RSA Security
38 Jahan Moreh, Sigaba
39 Anne Anderson, Sun Microsystems
40 Eve Maler, Sun Microsystems
41 Ron Monzillo, Sun Microsystems
42 Greg Whitehead, Trustgenix

43 **Abstract:**

44 This non-normative specification describes and analyzes the security and privacy properties of
45 SAML.

46 **Status:**

47 This is an **OASIS Standard** document produced by the Security Services Technical Committee. It
48 was approved by the OASIS membership on 1 March 2005.

49 Committee members should submit comments and potential errata to the [security-](mailto:security-services@lists.oasis-open.org)
50 [services@lists.oasis-open.org](mailto:security-services@lists.oasis-open.org) list. Others should submit them by filling out the web form located
51 at http://www.oasis-open.org/committees/comments/form.php?wg_abbrev=security. The
52 committee will publish on its web page (<http://www.oasis-open.org/committees/security>) a catalog
53 of any changes made to this document.

54 For information on whether any patents have been disclosed that may be essential to
55 implementing this specification, and any offers of patent licensing terms, please refer to the
56 Intellectual Property Rights web page for the Security Services TC ([http://www.oasis-](http://www.oasis-open.org/committees/security/ipr.php)
57 [open.org/committees/security/ipr.php](http://www.oasis-open.org/committees/security/ipr.php)).

58 Table of Contents

59	1 Introduction.....	5
60	2 Privacy.....	6
61	2.1 Ensuring Confidentiality.....	6
62	2.2 Notes on Anonymity.....	6
63	2.2.1 Definitions That Relate to Anonymity	6
64	2.2.2 Pseudonymity and Anonymity.....	7
65	2.2.3 Behavior and Anonymity.....	7
66	2.2.4 Implications for Privacy.....	8
67	3 Security.....	9
68	3.1 Background.....	9
69	3.2 Scope.....	9
70	3.3 SAML Threat Model.....	9
71	4 Security Techniques.....	11
72	4.1 Authentication.....	11
73	4.1.1 Active Session.....	11
74	4.1.2 Message-Level.....	11
75	4.2 Confidentiality.....	11
76	4.2.1 In Transit.....	11
77	4.2.2 Message-Level.....	11
78	4.3 Data Integrity.....	11
79	4.3.1 In Transit.....	11
80	4.3.2 Message-Level.....	11
81	4.4 Notes on Key Management.....	12
82	4.4.1 Access to the Key.....	12
83	4.4.2 Binding of Identity to Key.....	12
84	4.5 SSL/TLS Cipher Suites.....	12
85	4.5.1 SSL/TLS Cipher Suites.....	13
86	4.5.2 SSL/TLS Recommendations.....	14
87	5 General SAML Security Considerations.....	15
88	5.1 SAML Assertions.....	15
89	5.2 SAML Protocol.....	15
90	5.2.1 Denial of Service.....	15
91	5.2.1.1 Requiring Client Authentication at a Lower Level.....	15
92	5.2.1.2 Requiring Signed Requests.....	16
93	5.2.1.3 Restricting Access to the Interaction URL.....	16
94	6 SAML Bindings Security Considerations.....	17
95	6.1 SAML SOAP Binding.....	17
96	6.1.1 Eavesdropping.....	17
97	6.1.2 Replay.....	18
98	6.1.3 Message Insertion.....	18
99	6.1.4 Message Deletion.....	18
100	6.1.5 Message Modification.....	18
101	6.1.6 Man-in-the-Middle.....	19
102	6.1.7 Use of SOAP over HTTP.....	19

103	6.2 Reverse SOAP (PAOS) Binding.....	20
104	6.2.1 Denial of Service.....	20
105	6.3 HTTP Redirect binding.....	20
106	6.3.1 Denial of Service.....	20
107	6.4 HTTP Redirect/POST binding.....	20
108	6.4.1 Stolen Assertion.....	20
109	6.4.2 Man In the Middle Attack.....	21
110	6.4.3 Forged Assertion.....	21
111	6.4.4 Browser State Exposure.....	21
112	6.4.5 Replay.....	21
113	6.4.6 Modification or Exposure of state information.....	21
114	6.5 HTTP Artifact Binding.....	22
115	6.5.1 Stolen Artifact	22
116	6.5.2 Attacks on the SAML Protocol Message Exchange.....	22
117	6.5.3 Malicious Destination Site.....	22
118	6.5.4 Forged SAML Artifact.....	23
119	6.5.5 Browser State Exposure.....	23
120	6.5.6 Replay.....	23
121	6.6 SAML URI Binding.....	23
122	6.6.1 Substitution.....	23
123	7 SAML Profile Security Considerations.....	24
124	7.1 Web Browser Single Sign-On (SSO) Profiles.....	24
125	7.1.1 SSO Profile.....	24
126	7.1.1.1 Eavesdropping.....	24
127	7.1.1.2 Theft of the User Authentication Information.....	24
128	7.1.1.3 Theft of the Bearer Token.....	24
129	7.1.1.4 Replay.....	25
130	7.1.1.5 Message Insertion.....	25
131	7.1.1.6 Message Deletion.....	25
132	7.1.1.7 Message Modification.....	25
133	7.1.1.8 Man-in-the-Middle.....	25
134	7.1.1.9 Impersonation without Reauthentication.....	26
135	7.1.2 Enhanced Client and Proxy Profile.....	26
136	7.1.2.1 Man in the Middle.....	26
137	7.1.2.2 Denial of Service.....	26
138	7.1.3 Identity Provider Discovery Profile.....	26
139	7.1.4 Single Logout Profile.....	26
140	7.2 Name Identifier Management Profiles.....	27
141	7.3 Attribute Profiles.....	27
142	8 Summary.....	28
143	9 References.....	29

1 Introduction

144

145 This non-normative document describes and analyzes the security and privacy properties of the OASIS
146 Security Assertion Markup Language (SAML) defined in the core SAML specification [SAMLCore] and the
147 SAML bindings [SAMLBind] and profiles [SAMLProf] specifications. The intent in this document is to
148 provide information to architects, implementors, and reviewers of SAML-based systems about the
149 following:

- 150 • The privacy issues to be considered and how SAML architecture addresses these issues
- 151 • The threats, and thus security risks, to which a SAML-based system is subject
- 152 • The security risks the SAML architecture addresses, and how it does so
- 153 • The security risks it does not address
- 154 • Recommendations for countermeasures that mitigate those security risks

155 Terms used in this document are as defined in the SAML glossary [SAMLGloss] unless otherwise noted.

156 The rest of this section describes the background and assumptions underlying the analysis in this
157 document. Section 4 provides a high-level view of security techniques and technologies that should be
158 used with SAML. The following sections analyze the risks associated with the SAML assertions and
159 protocol as well as specific risks associated with SAML bindings and profiles.

2 Privacy

160

161 SAML includes the ability to make statements about the attributes and authorizations of authenticated
162 entities. There are very many common situations in which the information carried in these statements is
163 something that one or more of the parties to a communication would desire to keep accessible to as
164 restricted as possible a set of entities. Statements of medical or financial attributes are simple examples of
165 such cases.

166 Many countries and jurisdictions have laws and regulations regarding privacy and these should be
167 considered when deploying a SAML based system. A more extensive discussion of the legal issues
168 related to privacy and best practices related to privacy may be found in the Liberty Privacy and Security
169 Best Practices document [LibBestPractices].

170 Parties making statements, issuing assertions, conveying assertions, and consuming assertions must be
171 aware of these potential privacy concerns and should attempt to address them in their implementations of
172 SAML-aware systems.

2.1 Ensuring Confidentiality

173

174 Perhaps the most important aspect of ensuring privacy to parties in a SAML-enabled transaction is the
175 ability to carry out the transaction with a guarantee of confidentiality. In other words, can the information in
176 an assertion be conveyed from the issuer to the intended audience, and only the intended audience,
177 without making it accessible to any other parties?

178 It is technically possible to convey information confidentially (a discussion of common methods for
179 providing confidentiality occurs in the Security portion of the document in Section 4.2). All parties to SAML-
180 enabled transactions should analyze each of their steps in the interaction (and any subsequent uses of
181 data obtained from the transactions) to ensure that information that should be kept confidential is actually
182 being kept so.

183 It should also be noted that simply obscuring the contents of assertions may not be adequate protection of
184 privacy. There are many cases where just the availability of the information that a given user (or IP
185 address) was accessing a given service may constitute a breach of privacy (for example, an the
186 information that a user accessed a medical testing facility for an assertion may be enough to breach
187 privacy without knowing the contents of the assertion). Partial solutions to these problems can be provided
188 by various techniques for anonymous interaction, outlined below.

2.2 Notes on Anonymity

189

190 The following sections discuss the concept of anonymity.

2.2.1 Definitions That Relate to Anonymity

191

192 There are no definitions of anonymity that are satisfying for all cases. Many definitions [Anonymity] deal
193 with the simple case of a sender and a message, and discuss “anonymity” in terms of not being able to
194 link a given sender to a sent message, or a message back to a sender.

195 And while that definition is adequate for the “one off” case, it ignores the aggregation of information that is
196 possible over time based on behavior rather than an identifier.

197 Two notions that may be generally useful, and that relate to each other, can help define anonymity.

198 The first notion is to think about anonymity as being “within a set”, as in this comment from “Anonymity,
199 Unobservability, and Pseudonymity” [Anonymity]:

200 *To enable anonymity of a subject, there always has to be an appropriate set of subjects with*
201 *potentially the same attributes....*

202 *...Anonymity is the stronger, the larger the respective anonymity set is and the more evenly*
203 *distributed the sending or receiving, respectively, of the subjects within that set is.*

204 This notion is relevant to SAML because of the use of authorities. Even if a Subject is “anonymous”, that
205 subject is still identifiable as a member of the set of Subjects within the domain of the relevant authority.

206 In the case where aggregating attributes of the user are provided, the set can become much smaller – for
207 example, if the user is “anonymous” but has the attribute of “student in Course 6@mit.edu”. Certainly, the
208 number of Course 6 students is less than the number of MIT-affiliated persons which is less than the
209 number of users everywhere.

210 Why does this matter? Non-anonymity leads to the ability of an adversary to harm, as expressed in
211 Dingedine, Freedman, and Molnar’s Freehaven document [FreeHaven]:

212 *Both anonymity and pseudonymity protect the privacy of the user’s location and true name.*
213 *Location refers to the actual physical connection to the system. The term “true name” was*
214 *introduced by Vinge and popularized by May to refer to the legal identity of an individual.*
215 *Knowing someone’s true name or location allows you to hurt him or her.*

216 This leads to a unification of the notion of anonymity within a set and ability to harm, from the same source
217 [FreeHaven]:

218 *We might say that a system is partially anonymous if an adversary can only narrow down a*
219 *search for a user to one of a ‘set of suspects.’ If the set is large enough, then it is impractical*
220 *for an adversary to act as if any single suspect were guilty. On the other hand, when the set*
221 *of suspects is small, mere suspicion may cause an adversary to take action against all of*
222 *them.*

223 SAML-enabled systems are limited to "partial anonymity" at best because of the use of authorities. An
224 entity about whom an assertion is made is already identifiable as one of the pool of entities in a
225 relationship with the issuing authority.

226 The limitations on anonymity can be much worse than simple authority association, depending on how
227 identifiers are employed, as reuse of pseudonymous identifiers allows accretion of potentially identifying
228 information (see Section 2.2.2). Additionally, users of SAML-enabled systems can also make the breach
229 of anonymity worse by their actions (see Section 2.2.3).

230 **2.2.2 Pseudonymity and Anonymity**

231 Apart from legal identity, any identifier for a Subject can be considered a pseudonym. And even notions
232 like “holder of key” can be considered as serving as the equivalent of a pseudonym in linking an action (or
233 set of actions) to a Subject. Even a description such as “the user that just requested access to object XYZ
234 at time 23:34” can serve as an equivalent of a pseudonym.

235 Thus, that with respect to “ability to harm,” it makes no difference whether the user is described with an
236 identifier or described by behavior (for example, use of a key or performance of an action).

237 What does make a difference is how often the particular equivalent of a pseudonym is used.

238 [Anonymity] gives a taxonomy of pseudonyms starting from personal pseudonyms (like nicknames) that
239 are used all the time, through various types of role pseudonyms (such as Secretary of Defense), on to
240 “one-time-use” pseudonyms.

241 Only one-time-use pseudonyms can give you anonymity (within SAML, consider this as "anonymity within
242 a set").

243 The more often you use a given pseudonym, the more you reduce your anonymity and the more likely it is
244 that you can be harmed. In other words, reuse of a pseudonym allows additional potentially identifying
245 information to be associated with the pseudonym. Over time, this will lead to an accretion that can
246 uniquely identify the identity associated with a pseudonym.

247 **2.2.3 Behavior and Anonymity**

248 As Joe Klein can attest, anonymity isn’t all it is cracked up to be.

249 Klein is the "Anonymous" who authored Primary Colors. Despite his denials he was unmasked as the
250 author by Don Foster, a Vassar professor who did a forensic analysis of the text of Primary Colors. Foster
251 compared that text with texts from a list of suspects that he devised based on their knowledge bases and
252 writing proclivities.

253 It was Klein's idiosyncratic usages that did him in (though apparently all authors have them).
254 The relevant point for SAML is that an "anonymous" user (even one that is never named) can be identified
255 enough to be harmed by repeated unusual behavior. Here are some examples:

- 256 • A user who each Tuesday at 21:00 access a database that correlates finger lengths and life span
257 starts to be non-anonymous. Depending on that user's other behavior, she or he may become
258 "traceable" [Pooling] in that other "identifying" information may be able to be collected.
- 259 • A user who routinely buys a usual set of products from a networked vending machine certainly
260 opens themselves to harm (by virtue of booby-trapping the products).

261 **2.2.4 Implications for Privacy**

262 Origin site authorities (such as authentication authorities and attribute authorities) can provide a degree of
263 "partial anonymity" by employing one-time-use identifiers or keys (for the "holder of key" case).

264 This anonymity is "partial" at best because the Subject is necessarily confined to the set of Subjects in a
265 relationship with the Authority.

266 This set may be further reduced (thus further reducing anonymity) when aggregating attributes are used
267 that further subset the user community at the origin site.

268 Users who truly care about anonymity must take care to disguise or avoid unusual patterns of behavior
269 that could serve to "de-anonymize" them over time.

270 3 Security

271 The following sections discuss security considerations.

272 3.1 Background

273 Communication between computer-based systems is subject to a variety of threats, and these threats
274 carry some level of associated risk. The nature of the risk depends on a host of factors, including the
275 nature of the communications, the nature of the communicating systems, the communication mediums,
276 the communication environment, the end-system environments, and so on. Section 3 of the IETF
277 guidelines on writing security considerations for RFCs [Rescorla-Sec] provides an overview of threats
278 inherent in the Internet (and, by implication, intranets).

279 SAML is intended to aid deployers in establishing security contexts for application-level computer-based
280 communications within or between security domains. In this role, SAML transfers authentication data,
281 supporting end systems' ability to protect against unauthorized usage. Communications security is directly
282 applicable to the design of SAML. Systems security is of interest mostly in the context of SAML's threat
283 models. Section 2 of the IETF guidelines gives an overview of communications security and systems
284 security.

285 3.2 Scope

286 Some areas that impact broadly on the overall security of a system that uses SAML are explicitly outside
287 the scope of SAML. While this document does not address these areas, they should always be
288 considered when reviewing the security of a system. In particular, these issues are important, but currently
289 beyond the scope of SAML:

- 290 • Initial authentication: SAML allows statements to be made about acts of authentication that have
291 occurred, but includes no requirements or specifications for these acts of authentication.
292 Consumers of authentication assertions should be wary of blindly trusting these assertions
293 unless and until they know the basis on which they were made. Confidence in the assertions
294 must never exceed the confidence that the asserting party has correctly arrived at the
295 conclusions asserted.
- 296 • Trust Model: In many cases, the security of a SAML conversation will depend on the underlying
297 trust model, which is typically based on a key management infrastructure (for example, PKI or
298 secret key). For example, SOAP messages secured by means of XML Signature [XMLSig] are
299 secured only insofar as the keys used in the exchange can be trusted. Undetected compromised
300 keys or revoked certificates, for example, could allow a breach of security. Even failure to require
301 a certificate opens the door for impersonation attacks. PKI setup is not trivial and must be
302 implemented correctly in order for layers built on top of it (such as parts of SAML) to be secure.
- 303 • Suitable implementations of security protocols is necessary to maintain the security of a system,
304 including secure random or pseudo-random number generation and secure key storage.

305 3.3 SAML Threat Model

306 The general Internet threat model described in the IETF guidelines for security considerations [Rescorla-
307 Sec] is the basis for the SAML threat model. We assume here that the two or more endpoints of a SAML
308 transaction are uncompromised, but that the attacker has complete control over the communications
309 channel.

310 Additionally, due to the nature of SAML as a multi-party authentication and authorization statement
311 protocol, cases must be considered where one or more of the parties in a legitimate SAML transaction—
312 who operate legitimately within their role for that transaction—attempt to use information gained from a
313 previous transaction maliciously in a subsequent transaction.

314 The following scenarios describe possible attacks:

- 315 • Collusion: The secret cooperation between two or more system entities to launch an attack, for
316 example:
 - 317 Collusion between Principal and service provider
 - 318 Collusion between Principal and identity provider
 - 319 Collusion between identity provider and service provider
 - 320 Collusion among two or more Principals
 - 321 Collusion between two or more service providers
 - 322 Collusion between two or more identity providers

323 • Denial-of-Service Attacks: The prevention of authorized access to a system resource or the
324 delaying of system operations and functions.

325 • Man-in-the-Middle Attacks: A form of active wiretapping attack in which the attacker intercepts
326 and selectively modifies communicated data to masquerade as one or more of the entities
327 involved in a communication association.

328 • Replay Attacks: An attack in which a valid data transmission is maliciously or fraudulently
329 repeated, either by the originator or by an adversary who intercepts the data and retransmits it,
330 possibly as part of a masquerade attack.

331 • Session Hijacking: A form of active wiretapping in which the attacker seizes control of a
332 previously established communication association.

333 In all cases, the local mechanisms that systems will use to decide whether or not to generate assertions
334 are out of scope. Thus, threats arising from the details of the original login at an authentication authority,
335 for example, are out of scope as well. If an authority issues a false assertion, then the threats arising from
336 the consumption of that assertion by downstream systems are explicitly out of scope.

337 The direct consequence of such a scoping is that the security of a system based on assertions as inputs is
338 only as good as the security of the system used to generate those assertions, and of the correctness of
339 the data and processing on which the generated assertions are based. When determining what issuers to
340 trust, particularly in cases where the assertions will be used as inputs to authentication or authorization
341 decisions, the risk of security compromises arising from the consumption of false but validly issued
342 assertions is a large one. Trust policies between asserting and relying parties should always be written to
343 include significant consideration of liability and implementations should provide an appropriate audit trail.

344 4 Security Techniques

345 The following sections describe security techniques and various stock technologies available for their
346 implementation in SAML deployments.

347 4.1 Authentication

348 Authentication here means the ability of a party to a transaction to determine the identity of the other party
349 in the transaction. This authentication may be in one direction or it may be bilateral.

350 4.1.1 Active Session

351 Non-persistent authentication is provided by the communications channel used to transport a SAML
352 message. This authentication may be unilateral—from the session initiator to the receiver—or bilateral.
353 The specific method will be determined by the communications protocol used. For instance, the use of a
354 secure network protocol, such as TLS [RFC2246] or the IP Security Protocol [IPsec], provides the SAML
355 message sender with the ability to authenticate the destination for the TCP/IP environment.

356 4.1.2 Message-Level

357 XML Signature [XMLSig] and the OASIS Web Services Security specifications [WSS] provide methods of
358 creating a persistent “authentication” that is tightly coupled to a document. This method does not
359 independently guarantee that the sender of the message is in fact that signer (and indeed, in many cases
360 where intermediaries are involved, this is explicitly not the case).
361 Any method that allows the persistent confirmation of the involvement of a uniquely resolvable entity with a
362 given subset of an XML message is sufficient to meet this requirement.

363 4.2 Confidentiality

364 Confidentiality means that the contents of a message can be read only by the desired recipients and not
365 anyone else who encounters the message.

366 4.2.1 In Transit

367 Use of a secure network protocol such as TLS [RFC2246] or the IP Security Protocol [IPsec] provides
368 transient confidentiality of a message as it is transferred between two nodes.

369 4.2.2 Message-Level

370 XML Encryption [XMLEnc] provides for the selective encryption of XML documents. This encryption
371 method provides persistent, selective confidentiality of elements within an XML message.

372 4.3 Data Integrity

373 Data integrity is the ability to confirm that a given message as received is unaltered from the version of the
374 message that was sent.

375 4.3.1 In Transit

376 Use of a secure network protocol such as TLS [RFC2246] or the IP Security Protocol [IPsec] may be
377 configured to provide integrity protection for the packets transmitted via the network connection.

378 4.3.2 Message-Level

379 XML Signature [XMLSig] provides a method of creating a persistent guarantee of the unaltered nature of a

380 message that is tightly coupled to that message.
381 Any method that allows the persistent confirmation of the unaltered nature of a given subset of an XML
382 message is sufficient to meet this requirement.

383 **4.4 Notes on Key Management**

384 Many points in this document will refer to the ability of systems to provide authentication, data integrity,
385 and confidentiality via various schemes involving digital signature and encryption. For all these schemes
386 the security provided by the scheme is limited based on the key management systems that are in place.
387 Some specific limitations are detailed below.

388 **4.4.1 Access to the Key**

389 It is assumed that, if key-based systems are going to be used for authentication, data integrity, and non-
390 repudiation, security is in place to guarantee that access to a private or secret key representing a principal
391 is not available to inappropriate parties. For example, a digital signature created with Bob's private key is
392 only proof of Bob's involvement to the extent that Bob is the only one with access to the key.

393 In general, access to keys should be kept to the minimum set of entities possible (particularly important for
394 corporate or organizational keys) and should be protected with passphrases and other means. Standard
395 security precautions (don't write down the passphrase, when you're away from a computer don't leave a
396 window with the key accessed open, and so on) apply.

397 **4.4.2 Binding of Identity to Key**

398 For a key-based system to be used for authentication there must be some trusted binding of identity to
399 key. Verifying a digital signature on a document can determine if the document is unaltered since it was
400 signed, and that it was actually signed by a given key. However, this does not confirm that the key used is
401 actually the key of a specific individual appropriate for the time and purpose. Verifying the binding of a key
402 to a party requires additional validation.

403 This key-to-individual binding must be established. Common solutions include local directories that store
404 both identifiers and key—which is simple to understand but difficult to maintain—or the use of certificates.
405 Using certificates can provide a scalable means to associate a key with an identity, but requires
406 mechanisms to manage the certificate lifecycle and changes to the status of the binding (e.g. An
407 employee leaves and no longer has a corporate identity). One common approach is to use a Public Key
408 Infrastructure (PKI).

409 In this case a set of trusted root Certifying Authorities (CAs) are identified for each consumer of signatures
410 —answering the question “Whom do I trust to make statements of identity-to-key binding?” Verification of
411 a signature then becomes a process of first verifying the signature (to determine that the signature was
412 done by the key in question and that the message has not changed) and then validating the certificate
413 chain (to determine that the key is bound to the right identity) and validating that the binding is still
414 appropriate. Validating the binding requires steps to be taken to ensure that the binding is currently valid
415 —a certificate typically has a “lifetime” built into it, but if a key is compromised during the life of the
416 certificate then the key-to-identity binding contained in the certificate becomes invalid while the certificate
417 is still valid on its face. Also, certificates often depend on associations that may end before their lifetime
418 expires (for example, certificates that should become invalid when someone changes employers, etc.)
419 Different mechanisms may be used to validate key and certificate validity, such as Certificate Revocation
420 Lists (CRLs), the Online Certificate Status Protocol [OCSP], or the XML Key Management Specification
421 (XKMS) [XKMS], but these mechanisms are out of scope of the SSTC work.

422 A proper key management system is thus quite strong but very complex. Verifying a signature ends up
423 being a process of verifying the document-to-key binding, then verifying the key-to-identity binding, as well
424 as the current validity of the key and certificate.

425 **4.5 SSL/TLS Cipher Suites**

426 The use of HTTP over SSL 3.0 or TLS 1.0 [RFC2246], or use of URLs with the HTTPS URL scheme, is
427 strongly recommended at many places in this document.

428 Unless otherwise specified, in any SAML binding's use of SSL 3.0 [SSL3] or TLS 1.0 [RFC2246], servers
429 MUST authenticate to clients using a X.509 v3 certificate. The client MUST establish server identity based
430 on contents of the certificate (typically through examination of the certificate's subject DN field).

431 SSL/TLS can be configured to use many different cipher suites, not all of which are adequate to provide
432 "best practices" security. The following sections provide a brief description of cipher suites and
433 recommendations for cipher suite selection.

434 4.5.1 SSL/TLS Cipher Suites

435 **Note:** While references to the US Export restrictions are now obsolete, the constants
436 naming the cipher suites have not changed. Thus,
437 SSL_DHE_DSS_EPORT_WITH_DES40_CBC_SHA is still a valid cipher suite identifier,
438 and the explanation of the historical reasons for the inclusion of "EXPORT" has been left
439 in place in the following summary.

440 A cipher suite combines four kinds of security features, and is given a name in the SSL protocol
441 specification. Before data flows over a SSL connection, both ends attempt to negotiate a cipher suite. This
442 lets them establish an appropriate quality of protection for their communications, within the constraints of
443 the particular mechanism combinations which are available. The features associated with a cipher suite
444 are:

- 445 • The protocol, SSL or TLS.
- 446 • The type of key exchange algorithm used. SSL defines many; the ones that provide server
447 authentication are the most important ones, but anonymous key exchange is supported. (Note
448 that anonymous key exchange algorithms are subject to "man in the middle" attacks, and are **not**
449 **recommended** in the SAML context.) The "RSA" authenticated key exchange algorithm is
450 currently the most interoperable algorithm. Another important key exchange algorithm is the
451 authenticated Diffie-Hellman "DHE_DSS" key exchange, which has no patent-related
452 implementation constraints.¹
- 453 • Whether the key exchange algorithm is freely exportable from the United States of America.
454 Exportable algorithms must use short (512-bit) public keys for key exchange and short (40-bit)
455 symmetric keys for encryption. Keys of these lengths have been successfully attacked, and their
456 use is not recommended.
- 457 • The encryption algorithm used. The fastest option is the RC4 stream cipher; DES and variants
458 (DES40, 3DES-EDE) as well as AES are also supported in "cipher block chaining" (CBC) mode.
459 Other modes are also supported, refer to the TLS documentation [RFC2246].
- 460 • Null encryption is also an option in some cipher suites. Note that null encryption performs **no**
461 encryption; in such cases SSL/TLS is used only to authenticate and provide integrity protection.
462 Cipher suites with null encryption do not provide confidentiality, and **must not be used** in cases
463 where confidentiality is a requirement and is not obtained by means other than SSL/TLS.
- 464 • The digest algorithm used for the Message Authentication Code. The recommended choice is
465 SHA1.
- 466 • For example, the cipher suite named SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
467 uses SSL, uses an authenticated Diffie-Hellman key exchange (DHE_DSS), is export grade
468 (EXPORT), uses an exportable variant of the DES cipher (DES40_CBC), and uses the SHA1
469 digest algorithm in its MAC (SHA).

470 A given implementation of SSL will support a particular set of cipher suites, and some subset of those will
471 be enabled by default. Applications have a limited degree of control over the cipher suites that are used on
472 their connections; they can enable or disable any of the supported cipher suites, but cannot change the
473 cipher suites that are available.

1 ¹ The RSA algorithm patent has expired; hence this issue is mostly historical.

474 **4.5.2 SSL/TLS Recommendations**

475 SSL 2.0 must not be used due to known security weaknesses. TLS is preferred, SSL 3.0 may also be
476 used.

477 The SAML 2.0 Bindings specification outlines which cipher suites are required and recommended, making
478 normative statements. This section repeats this information for completeness, but that specification is
479 considered normative in case of inconsistency.

480 TLS-capable implementations MUST implement the TLS_RSA_WITH_3DES_EDE_CBC_SHA cipher
481 suite and MAY implement the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite.

482 FIPS [FIPS] TLS-capable implementations MUST implement the corresponding
483 TLS_RSA_FIPS_WITH_3DES_EDE_CBC_SHA cipher suite and MAY implement the corresponding
484 TLS_RSA_FIPS_AES_128_CBC_SHA cipher suite [FIPS].

485 SSL-capable implementations MUST implement the SSL_RSA_WITH_3DES_EDE_CBC_SHA cipher
486 suite.

487 FIPS [FIPS] SSL-capable implementations MUST implement the FIPS ciphersuite corresponding to the
488 SSL SSL_RSA_WITH_3DES_EDE_CBC_SHA cipher suite [FIPS].

489 However, the IETF is moving rapidly towards mandating the use of AES, which has both speed and
490 strength advantages. Forward-looking systems would be wise as well to implement support for the AES
491 cipher suites, such as:

- 492 • TLS_RSA_WITH_AES_128_CBC_SHA

5 General SAML Security Considerations

493

494 The following sections analyze the security risks in using and implementing SAML and describe
495 countermeasures to mitigate the risks.

5.1 SAML Assertions

496

497 At the level of the SAML assertion itself, there is little to be said about security concerns—most concerns
498 arise during communications in the request/response protocol, or during the attempt to use SAML by
499 means of one of the bindings. The consumer is, of course, always expected to honor the validity interval of
500 the assertion and any <OneTimeUse> elements that are present in the assertion.

501 However, one issue at the assertion level bears analysis: an assertion, once issued, is out of the control of
502 the issuer. This fact has a number of ramifications. For example, the issuer has no control over how long
503 the assertion will be persisted in the systems of the consumer; nor does the issuer have control over the
504 parties with whom the consumer will share the assertion information. These concerns are over and above
505 concerns about a malicious attacker who can see the contents of assertions that pass over the wire
506 unencrypted (or insufficiently encrypted).

507 While efforts have been made to address many of these issues within the SAML specification, nothing
508 contained in the specification will erase the requirement for careful consideration of what to put in an
509 assertion. At all times, issuers should consider the possible consequences if the information in the
510 assertion is stored on a remote site, where it can be directly misused, or exposed to potential hackers, or
511 possibly stored for more creatively fraudulent uses. Issuers should also consider the possibility that the
512 information in the assertion could be shared with other parties, or even made public, either intentionally or
513 inadvertently.

5.2 SAML Protocol

514

515 The following sections describe security considerations for the SAML request-response protocol itself,
516 apart from any threats arising from use of a particular protocol binding.

5.2.1 Denial of Service

517

518 The SAML protocol is susceptible to a denial of service (DOS) attack. Handling a SAML request is
519 potentially a very expensive operation, including parsing the request message (typically involving
520 construction of a DOM tree), database/assertion store lookup (potentially on an unindexed key),
521 construction of a response message, and potentially one or more digital signature operations. Thus, the
522 effort required by an attacker generating requests is much lower than the effort needed to handle those
523 requests.

5.2.1.1 Requiring Client Authentication at a Lower Level

524

525 Requiring clients to authenticate at some level below the SAML protocol level (for example, using the
526 SOAP over HTTP binding, with HTTP over TLS/SSL, and with a requirement for client-side certificates
527 that have a trusted Certificate Authority at their root) will provide traceability in the case of a DOS attack.

528 If the authentication is used only to provide traceability, then this does not in itself prevent the attack from
529 occurring, but does function as a deterrent.

530 If the authentication is coupled with some access control system, then DOS attacks from non-insiders is
531 effectively blocked. (Note that it is possible that overloading the client-authentication scheme could still
532 function as a denial-of-service attack on the SAML service, but that this attack needs to be dealt with in
533 the context of the client authentication scheme chosen.)

534 Whatever system of client authentication is used, it should provide the ability to resolve a unique originator
535 for each request, and should not be subject to forgery. (For example, in the traceability-only case, logging
536 the IP address is insufficient since this information can easily be spoofed.)

537 **5.2.1.2 Requiring Signed Requests**

538 In addition to the benefits gained from client authentication discussed in Section 5.2.1.1, requiring a
539 signed request also lessens the order of the asymmetry between the work done by requester and
540 responder. The additional work required of the responder to verify the signature is a relatively small
541 percentage of the total work required of the responder, while the process of calculating the digital
542 signature represents a relatively large amount of work for the requester. Narrowing this asymmetry
543 decreases the risk associated with a DOS attack.

544 Note, however, that an attacker can theoretically capture a signed message and then replay it continually,
545 getting around this requirement. This situation can be avoided by requiring the use of the XML Signature
546 element `<ds:SignatureProperties>` containing a timestamp; the timestamp can then be used to
547 determine if the signature is recent. In this case, the narrower the window of time after issue that a
548 signature is treated as valid, the higher security you have against replay denial of service attacks.

549 **5.2.1.3 Restricting Access to the Interaction URL**

550 Limiting the ability to issue a request to a SAML service at a very low level to a set of known parties
551 drastically reduces the risk of a DOS attack. In this case, only attacks originating from within the finite set
552 of known parties are possible, greatly decreasing exposure both to potentially malicious clients and to
553 DOS attacks using compromised machines as zombies.

554 There are many possible methods of limiting access, such as placing the SAML responder inside a
555 secured intranet and implementing access rules at the router level.

6 SAML Bindings Security Considerations

556

557 The security considerations in the design of the SAML request-response protocol depend to a large extent
558 on the particular protocol binding (as defined in the SAML bindings specification [SAMLBind]) that is used.
559 The bindings sanctioned by the OASIS Security Services Technical Committee are the SOAP binding,
560 Reverse SOAP Binding (PAOS), HTTP Redirect binding, HTTP Redirect/POST binding and HTTP Artifact
561 binding and SAML URI bindings.

6.1 SAML SOAP Binding

562

563 Since the SAML SOAP binding requires no authentication and has no requirements for either in-transit
564 confidentiality or message integrity, it is open to a wide variety of common attacks, which are detailed in
565 the following sections. General considerations are discussed separately from considerations related to the
566 SOAP-over-HTTP case.

6.1.1 Eavesdropping

567

568 **Threat:** Since there is no in-transit confidentiality requirement, it is possible that an eavesdropping party
569 could acquire both the SOAP message containing a request and the SOAP message containing the
570 corresponding response. This acquisition exposes both the nature of the request and the details of the
571 response, possibly including one or more assertions.

572 Exposure of the details of the request will in some cases weaken the security of the requesting party by
573 revealing details of what kinds of assertions it requires, or from whom those assertions are requested. For
574 example, if an eavesdropper can determine that site X is frequently requesting authentication assertions
575 with a given confirmation method from site Y, he may be able to use this information to aid in the
576 compromise of site X.

577 Similarly, eavesdropping on a series of authorization queries could create a “map” of resources that are
578 under the control of a given authorization authority.

579 Additionally, in some cases exposure of the request itself could constitute a violation of privacy. For
580 example, eavesdropping on a query and its response may expose that a given user is active on the
581 querying site, which could be information that should not be divulged in cases such as medical information
582 sites, political sites, and so on. Also the details of any assertions carried in the response may be
583 information that should be kept confidential. This is particularly true for responses containing attribute
584 assertions; if these attributes represent information that should not be available to entities not party to the
585 transaction (credit ratings, medical attributes, and so on), then the risk from eavesdropping is high.

586 **Countermeasures:** In cases where any of these risks is a concern, the countermeasure for
587 eavesdropping attacks is to provide some form of in-transit message confidentiality. For SOAP messages,
588 this confidentiality can be enforced either at the SOAP level or at the SOAP transport level (or some level
589 below it).

590 Adding in-transit confidentiality at the SOAP level means constructing the SOAP message such that,
591 regardless of SOAP transport, no one but the intended party will be able to access the message. The
592 general solution to this problem is likely to be XML Encryption [XMLEnc]. This specification allows
593 encryption of the SOAP message itself, which eliminates the risk of eavesdropping unless the key used in
594 the encryption has been compromised. Alternatively, deployers can depend on the SOAP transport layer,
595 or a layer beneath it, to provide in-transit confidentiality.

596 The details of how to provide this confidentiality depend on the specific SOAP transport chosen. Using
597 HTTP over TLS/SSL (described further in Section 6.1.7) is one method. Other transports will necessitate
598 other in-transit confidentiality techniques; for example, an SMTP transport might use S/MIME.

599 In some cases, a layer beneath the SOAP transport might provide the required in-transit confidentiality.
600 For example, if the request-response interaction is carried out over an IPsec tunnel, then adequate in-
601 transit confidentiality may be provided by the tunnel itself.

6.1.2 Replay

Threat: There is little vulnerability to replay attacks at the level of the SOAP binding. Replay is more of an issue in the various profiles. The primary concern about replay at the SOAP binding level is the potential for use of replay as a denial-of-service attack method.

Countermeasures: In general, the best way to prevent replay attacks is to prevent the message capture in the first place. Some of the transport-level schemes used to provide in-transit confidentiality will accomplish this goal. For example, if the SAML request-response conversation occurs over SOAP on HTTP/TLS, third parties are prevented from capturing the messages.

Note that since the potential replayer does not need to understand the message to replay it, schemes such as XML Encryption do not provide protection against replay. If an attacker can capture a SAML request that has been signed by the requester and encrypted to the responder, then the attacker can replay that request at any time without needing to be able to undo the encryption. The SAML request includes information about the issue time of the request, allowing a determination about whether replay is occurring. Alternatively, the unique key of the request (its ID) can be used to determine if this is a replay request or not.

Additional threats from the replay attack include cases where a “charge per request” model is in place. Replay could be used to run up large charges on a given account.

Similarly, models where a client is allocated (or purchases) a fixed number of interactions with a system, the replay attack could exhaust these uses unless the issuer is careful to keep track of the unique key of each request.

6.1.3 Message Insertion

Threat: A fabricated request or response is inserted into the message stream. A false response such as a spurious “yes” reply to an authorization decision query or the return of false attribute information in response to an attribute query may result in inappropriate receiver action.

Countermeasures: The ability to insert a request is not a threat at the SOAP binding level. The threat of inserting a false response can be a denial of service attack, for example returning SOAP Faults for responses, but this attack would become quickly obvious. The more subtle attack of returning fabricated responses is addressed in the SAML protocol, appropriate since according to the SOAP Binding definition each SOAP response must contain a single SAML protocol response unless it contains a fault. The SAML Protocol addresses this with two mechanisms, correlation of responses to requests using the required InResponseTo attribute, making an attack harder since requests must be intercepted to generate responses, and through the support origin authentication, either via signed SAML responses or through a secured transport connection such as SSL/TLS.

6.1.4 Message Deletion

Threat: The message deletion attack would either prevent a request from reaching a responder, or would prevent the response from reaching the requester.

Countermeasures: In either case, the SOAP binding does not address this threat. In general, correlation of request and response messages may deter such an attack, for example use of the InResponseTo attribute in the StatusResponseType.

6.1.5 Message Modification

Threat: Message modification is a threat to the SOAP binding in both directions.

Modification of the request to alter the details of the request can result in significantly different results being returned, which in turn can be used by a clever attacker to compromise systems depending on the assertions returned. For example, altering the list of requested attributes in the <Attribute> elements could produce results leading to compromise or rejection of the request by the responder.

Modification of the request to alter the apparent issuer of the request could result in denial of service or incorrect routing of the response. This alteration would need to occur below the SAML level and is thus out of scope.

650 Modification of the response to alter the details of the assertions therein could result in vast degrees of
651 compromise. The simple examples of altering details of an authentication or an authorization decision
652 could lead to very serious security breaches.

653 **Countermeasures:** In order to address these potential threats, a system that guarantees in-transit
654 message integrity must be used. The SAML protocol and the SOAP binding neither require nor forbid the
655 deployment of systems that guarantee in-transit message integrity, but due to this large threat, it is **highly**
656 **recommended** that such a system be used. At the SOAP binding level, this can be accomplished by
657 digitally signing requests and responses with a system such as XML Signature [XMLSig]. The SAML
658 specification allows for such signatures; see the SAML assertion and protocol specification [SAMLCore]
659 for further information.

660 If messages are digitally signed (with a sensible key management infrastructure, see Section 4.4) then the
661 recipient has a guarantee that the message has not been altered in transit, unless the key used has been
662 compromised.

663 The goal of in-transit message integrity can also be accomplished at a lower level by using a SOAP
664 transport that provides the property of guaranteed integrity, or is based on a protocol that provides such a
665 property. SOAP over HTTP over TLS/SSL is a transport that would provide such a guarantee.

666 Encryption alone does not provide this protection, as even if the intercepted message could not be altered
667 per se, it could be replaced with a newly created one.

668 6.1.6 Man-in-the-Middle

669 **Threat:** The SOAP binding is susceptible to man-in-the-middle (MITM) attacks. In order to prevent
670 malicious entities from operating as a man in the middle (with all the perils discussed in both the
671 eavesdropping and message modification sections), some sort of bilateral authentication is required.

672 **Countermeasures:** A bilateral authentication system would allow both parties to determine that what they
673 are seeing in a conversation actually came from the other party to the conversation.

674 At the SOAP binding level, this goal could also be accomplished by digitally signing both requests and
675 responses (with all the caveats discussed in Section 6.1.5 above). This method does not prevent an
676 eavesdropper from sitting in the middle and forwarding both ways, but he is prevented from altering the
677 conversation in any way without being detected.

678 Since many applications of SOAP do not use sessions, this sort of authentication of author (as opposed to
679 authentication of sender) may need to be combined with information from the transport layer to confirm
680 that the sender and the author are the same party in order to prevent a weaker form of "MITM as
681 eavesdropper".

682 Another implementation would depend on a SOAP transport that provides, or is implemented on a lower
683 layer that provides, bilateral authentication. The example of this is again SOAP over HTTP over TLS/SSL
684 with both server- and client-side certificates required.

685 Additionally, the validity interval of the assertions returned functions as an adjustment on the degree of
686 risk from MITM attacks. The shorter the valid window of the assertion, the less damage can be done if it is
687 intercepted.

688 6.1.7 Use of SOAP over HTTP

689 Since the SOAP binding requires that conformant applications support HTTP over TLS/SSL with a number
690 of different bilateral authentication methods such as Basic over server-side SSL and certificate-backed
691 authentication over server-side SSL, these methods are always available to mitigate threats in cases
692 where other lower-level systems are not available and the above listed attacks are considered significant
693 threats.

694 This does not mean that use of HTTP over TLS with some form of bilateral authentication is mandatory. If
695 an acceptable level of protection from the various risks can be arrived at through other means (for
696 example, by an IPsec tunnel), full TLS with certificates is not required. However, in the majority of cases
697 for SOAP over HTTP, using HTTP over TLS with bilateral authentication will be the appropriate choice.

698 The HTTP Authentication RFC [RFC2617] describes possible attacks in the HTTP environment when
699 basic or message-digest authentication schemes are used.

700 Note, however, that the use of transport-level security (such as the SSL or TLS protocols under HTTP)
701 only provides confidentiality and/or integrity and/or authentication for “one hop”. For models where there
702 may be intermediaries, or the assertions in question need to live over more than one hop, the use of
703 HTTP with TLS/SSL does not provide adequate security.

704 **6.2 Reverse SOAP (PAOS) Binding**

705 **6.2.1 Denial of Service**

706 **Threat:** Remove HTTP accept header field and/or the PAOS HTTP header field causing HTTP responder
707 to ignore PAOS processing possibility.

708 **Countermeasures:** Integrity protect the HTTP message, using SSL/TLS integrity protection or other
709 adequate transport layer security mechanism.

710 **6.3 HTTP Redirect binding**

711 **6.3.1 Denial of Service**

712 **Threat:** Malicious redirects into identity or service provider targets

713 Description: A spurious entity could issue a redirect to a user agent so that the user agent would access a
714 resource that disrupts single sign-on. For example, an attacker could redirect the user agent to a logout
715 resource of a service provider causing the Principal to be logged out of all existing authentication
716 sessions.

717 **Countermeasures:** Access to resources that produce side effects could be specified with a transient
718 qualifier that must correspond to the current authentication session. Alternatively, a confirmation dialog
719 could be interposed that relies on a transient qualifier with similar semantics.

720 **6.4 HTTP Redirect/POST binding**

721 This section utilizes materials from [ShibMarlena and [Rescorla-Sec] and is derived from material in the
722 SAML 1.1 Bindings and Profiles specification [SAML11Bind].

723 **6.4.1 Stolen Assertion**

724 **Threat:** If an eavesdropper can copy the real user’s SAML response and included assertions, then the
725 eavesdropper could construct an appropriate POST body and be able to impersonate the user at the
726 destination site.

727 **Countermeasures:** Confidentiality MUST be provided whenever a response is communicated between a
728 site and the user’s browser. This provides protection against an eavesdropper obtaining a real user’s
729 SAML response and assertions.

730 If an eavesdropper defeats the measures used to ensure confidentiality, additional countermeasures are
731 available:

- 732 • The Identity Provider and Service Provider sites SHOULD make some reasonable effort to
733 ensure that clock settings at both sites differ by at most a few minutes. Many forms of time
734 synchronization service are available, both over the Internet and from proprietary sources.
- 735 • When a non-SSO SAML profile uses the POST binding it must ensure that the receiver can
736 perform timely subject confirmation. To this end, a SAML authentication assertion for the
737 principal MUST be included in the POSTed form response.
- 738 • Values for `NotBefore` and `NotOnOrAfter` attributes of SSO assertions SHOULD have the
739 shortest possible validity period consistent with successful communication of the assertion from
740 Identity Provider to Service Provider site. This is typically on the order of a few minutes. This
741 ensures that a stolen assertion can only be used successfully within a small time window.
- 742 • The Service Provider site MUST check the validity period of all assertions obtained from the

743 Identity Provider site and reject expired assertions. A Service Provider site MAY choose to
744 implement a stricter test of validity for SSO assertions, such as requiring the assertion's
745 `IssueInstant` or `AuthnInstant` attribute value to be within a few minutes of the time at
746 which the assertion is received at the Service Provider site.

747 • If a received authentication statement includes a `<saml:SubjectLocality>` element with the
748 IP address of the user, the Service Provider site MAY check the browser IP address against the
749 IP address contained in the authentication statement.

750 6.4.2 Man In the Middle Attack

751 **Threat:** Since the Service Provider site obtains bearer SAML assertions from the user by means of an
752 HTML form, a malicious site could impersonate the user at some new Service Provider site. The new
753 Service Provider site would believe the malicious site to be the subject of the assertion.

754 **Countermeasures:** The Service Provider site MUST check the Recipient attribute of the SAML response
755 to ensure that its value matches the `https://<assertion consumer host name and path>`. As the
756 response is digitally signed, the `Recipient` value cannot be altered by the malicious site.

757 6.4.3 Forged Assertion

758 **Threat:** A malicious user, or the browser user, could forge or alter a SAML assertion.

759 **Countermeasures:** The browser/POST profile requires the SAML response carrying SAML assertions to
760 be signed, thus providing both message integrity and authentication. The Service Provider site MUST
761 verify the signature and authenticate the issuer.

762 6.4.4 Browser State Exposure

763 **Threat:** The browser/POST profile involves uploading of assertions from the web browser to a Service
764 Provider site. This information is available as part of the web browser state and is usually stored in
765 persistent storage on the user system in a completely unsecured fashion. The threat here is that the
766 assertion may be "reused" at some later point in time.

767 **Countermeasures:** Assertions communicated using this profile must always have short lifetimes and
768 should have a `<OneTimeUse>` SAML assertion `<Conditions>` element. Service Provider sites are
769 expected to ensure that the assertions are not re-used.

770 6.4.5 Replay

771 **Threat:** Replay attacks amount to resubmission of the form in order to access a protected resource
772 fraudulently.

773 **Countermeasures:** The profile mandates that the assertions transferred have the one-use property at the
774 Service Provider site, preventing replay attacks from succeeding.

775 6.4.6 Modification or Exposure of state information

776 **Threat:** Relay state tampering or fabrication

777 Some of the messages may carry a `<RelayState>` element, which is recommended to be integrity-
778 protected by the producer and optionally confidentiality- protected. If these practices are not followed, an
779 adversary could trigger unwanted side effects. In addition, by not confidentiality-protecting the value of this
780 element, a legitimate system entity could inadvertently expose information to the identity provider or a
781 passive attacker.

782 **Countermeasure:** Follow the recommended practice of confidentiality- and integrity- protecting the
783 RelayState data. Note: Because the value of this element is both produced and consumed by the same
784 system entity, symmetric cryptographic primitives could be utilized

785 6.5 HTTP Artifact Binding

786 This section utilizes materials from [ShibMarlena and [Rescorla-Sec] and is derived from material in the
787 SAML 1.1 Bindings and Profiles specification [SAML11Bind].

788 6.5.1 Stolen Artifact

789 **Threat:** If an eavesdropper can copy the real user's SAML artifact, then the eavesdropper could construct
790 a URL with the real user's SAML artifact and be able to impersonate the user at the destination site.

791 **Countermeasures:** Confidentiality **MUST** be provided whenever an artifact is communicated between a
792 site and the user's browser. This provides protection against an eavesdropper gaining access to a real
793 user's SAML artifact.

794 If an eavesdropper defeats the measures used to ensure confidentiality, additional countermeasures are
795 available:

- 796 • The source and destination sites **SHOULD** make some reasonable effort to ensure that clock
797 settings at both sites differ by at most a few minutes. Many forms of time synchronization service
798 are available, both over the Internet and from proprietary sources.
- 799 • The source site **SHOULD** track the time difference between when a SAML artifact is generated
800 and placed on a URL line and when a `<samlp:Request>` message carrying the artifact is
801 received from the destination. A maximum time limit of a few minutes is recommended. Should
802 an assertion be requested by a destination site query beyond this time limit, the source site
803 **MUST** not provide the assertions to the destination site.
- 804 • It is possible for the source site to create SSO assertions either when the corresponding SAML
805 artifact is created or when a `<samlp:Request>` message carrying the artifact is received from
806 the destination. The validity period of the assertion **SHOULD** be set appropriately in each case:
807 longer for the former, shorter for the latter.
- 808 • Values for `NotBefore` and `NotOnOrAfter` attributes of SSO assertions **SHOULD** have the
809 shortest possible validity period consistent with successful communication of the assertion from
810 source to destination site. This is typically on the order of a few minutes. This ensures that a
811 stolen artifact can only be used successfully within a small time window.
- 812 • The destination site **MUST** check the validity period of all assertions obtained from the source
813 site and reject expired assertions. A destination site **MAY** choose to implement a stricter test of
814 validity for SSO assertions, such as requiring the assertion's `IssueInstant` or `AuthnInstant`
815 attribute value to be within a few minutes of the time at which the assertion is received at the
816 destination site.
- 817 • If a received authentication statement includes a `<saml:SubjectLocality>` element with the
818 IP address of the user, the destination site **MAY** check the browser IP address against the IP
819 address contained in the authentication statement.

820 6.5.2 Attacks on the SAML Protocol Message Exchange

821 **Threat:** The message exchange used by the Service Provider to obtain an assertion from the Identity
822 Provider could be attacked in a variety of ways, including artifact or assertion theft, replay, message
823 insertion or modification, and MITM (man-in-the-middle attack).

824 **Countermeasures:** The requirement for the use of a SAML protocol binding with the properties of
825 bilateral authentication, message integrity, and confidentiality defends against these attacks.

826 6.5.3 Malicious Destination Site

827 **Threat:** Since the Service Provider obtains artifacts from the user, a malicious site could impersonate the
828 user at some new Service Provider site. The new Service Provider site would obtain assertions from the
829 Identity Provider site and believe the malicious site to be the user.

830 **Countermeasures:** The new Service Provider site will need to authenticate itself to the Identity Provider

831 site so as to obtain the SAML assertions corresponding to the SAML artifacts. There are two cases to
832 consider:

- 833 1. If the new Service Provider site has no relationship with the Identity Provider site, it will be unable to
834 authenticate and this step will fail.
- 835 2. If the new Service Provider site has an existing relationship with the Identity Provider site, the
836 Identity Provider site will determine that assertions are being requested by a site other than that to
837 which the artifacts were originally sent. In such a case, the Identity Provider site MUST not provide
838 the assertions to the new Service Provider site.

839 **6.5.4 Forged SAML Artifact**

840 **Threat:** A malicious user could forge a SAML artifact.

841 **Countermeasures:** The Bindings specification provides specific recommendations regarding the
842 construction of a SAML artifact such that it is infeasible to guess or construct the value of a current, valid,
843 and outstanding assertion handle. A malicious user could attempt to repeatedly “guess” a valid SAML
844 artifact value (one that corresponds to an existing assertion at a Identity Provider site), but given the size
845 of the value space, this action would likely require a very large number of failed attempts. An Identity
846 Provider site SHOULD implement measures to ensure that repeated attempts at querying against non-
847 existent artifacts result in an alarm.

848 **6.5.5 Browser State Exposure**

849 **Threat:** The SAML browser/artifact profile involves “downloading” of SAML artifacts to the web browser
850 from an Identity Provider site. This information is available as part of the web browser state and is usually
851 stored in persistent storage on the user system in a completely unsecured fashion. The threat here is that
852 the artifact may be “reused” at some later point in time.

853 **Countermeasures:** The “one-use” property of SAML artifacts ensures that they cannot be reused from a
854 browser. Due to the recommended short lifetimes of artifacts and mandatory SSO assertions, it is difficult
855 to steal an artifact and reuse it from some other browser at a later time.

856 **6.5.6 Replay**

857 **Threat:** Reuse of an artifact by repeating protocol messages

858 **Countermeasures:** The threat of replay as a reuse of an artifact is addressed by the requirement that
859 each artifact is a one-time-use item. Systems should track cases where multiple requests are made
860 referencing the same artifact, as this situation may represent intrusion attempts.

861 The threat of replay on the original request that results in the assertion generation is not addressed by
862 SAML, but should be mitigated by the original authentication process.

863 **6.6 SAML URI Binding**

864 **6.6.1 Substitution**

865 **Threat:** Substitution of assertion with another by substitution of URI reference. Given that a URI is
866 opaque to the receiver it is hard to validate the integrity.

867 **Countermeasures:** Where this is a concern, transport layer integrity protection such as with SSL/TLS is
868 required.

869 7 SAML Profile Security Considerations

870 The SAML profiles specification [SAMLProf] defines profiles of SAML, which are sets of rules describing
871 how to embed SAML assertions into and extract them from a framework or protocol.

872 7.1 Web Browser Single Sign-On (SSO) Profiles

873 Note that user authentication at the source site is explicitly out of scope, as are issues related to this
874 source site authentication. The key notion is that the source system entity must be able to ascertain that
875 the authenticated client system entity that it is interacting with is the same as the one in the next
876 interaction step. One way to accomplish this is for these initial steps to be performed using TLS as a
877 session layer underneath the protocol being used for this initial interaction (likely HTTP).

878 7.1.1 SSO Profile

879 7.1.1.1 Eavesdropping

880 **Threat:** The possibility of eavesdropping exists in all web browser cases.

881 **Countermeasures:** In cases where confidentiality is required (bearing in mind that any assertion that is
882 not sent securely, along with the requests associated with it, is available to the malicious eavesdropper),
883 HTTP traffic needs to take place over a transport that ensures confidentiality. HTTP over TLS/SSL
884 [RFC2246] and the IP Security Protocol [IPsec] meet this requirement.

885 The following sections provide more detail on the eavesdropping threat.

886 7.1.1.2 Theft of the User Authentication Information

887 **Threat:** In the case where the subject authenticates to the source site by revealing reusable
888 authentication information, for example, in the form of a password, theft of the authentication information
889 will enable an adversary to impersonate the subject.

890 **Countermeasures:** In order to avoid this problem, the connection between the subject's browser and the
891 source site must implement a confidentiality safeguard. In addition, steps must be taken by either the
892 subject or the destination site to ensure that the source site is genuinely the expected and trusted source
893 site before revealing the authentication information. Using HTTP over TLS can be used to address this
894 concern.

895 7.1.1.3 Theft of the Bearer Token

896 **Threat:** In the case where the authentication assertion contains the assertion bearer's authentication
897 protocol identifier, theft of the artifact will enable an adversary to impersonate the subject.

898 **Countermeasures:** Each of the following methods decreases the likelihood of this happening:

- 899 • The destination site implements a confidentiality safeguard on its connection with the subject's
900 browser.
- 901 • The subject or destination site ensures (out of band) that the source site implements a
902 confidentiality safeguard on its connection with the subject's browser.
- 903 • The destination site verifies that the subject's browser was directly redirected by a source site
904 that directly authenticated the subject.
- 905 • The source site refuses to respond to more than one request for an assertion corresponding to
906 the same assertion ID.
- 907 • If the assertion contains a condition element of type **AudienceRestrictionType** that identifies a
908 specific domain, then the destination site verifies that it is a member of that domain.

- 909 • The connection between the destination site and the source site, over which the assertion ID is
910 passed, is implemented with a confidentiality safeguard.
- 911 • The destination site, in its communication with the source site, over which the assertion ID is
912 passed, must verify that the source site is genuinely the expected and trusted source site.

913 **7.1.1.4 Replay**

914 The possibility of a replay attack exists for this set of profiles. A replay attack can be used either to attempt
915 to deny service or to retrieve information fraudulently. The specific countermeasures depend on which
916 specific binding is used and are discussed above

917 **7.1.1.5 Message Insertion**

918 Message insertion attacks are discussed in the section on bindings.

919 **7.1.1.6 Message Deletion**

920 **Threat:** Deleting a message during any step of the interactions between the browser, SAML assertion
921 issuer, and SAML assertion consumer will cause the interaction to fail. It results in a denial of some
922 service but does not increase the exposure of any information.

923 **Countermeasures:** Use of an integrity protected transport channel addresses the threat of message
924 deletion when no intermediaries are present.

925 **7.1.1.7 Message Modification**

926 **Threat:** The possibility of alteration of the messages in the stream exists for this set of profiles. Some
927 potential undesirable results are as follows:

- 928 • Alteration of the initial request can result in rejection at the SAML issuer, or creation of an artifact
929 targeted at a different resource than the one requested
- 930 • Alteration of the artifact can result in denial of service at the SAML consumer.
- 931 • Alteration of the assertions themselves while in transit could result in all kinds of bad results (if
932 they are unsigned) or denial of service (if they are signed and the consumer rejects them).

933 **Countermeasures:**

934 To avoid message modification, the traffic needs to be transported by means of a system that guarantees
935 message integrity from endpoint to endpoint.

936 For the web browser-based profiles, the recommended method of providing message integrity in transit is
937 the use of HTTP over TLS/SSL with a cipher suite that provides data integrity checking.

938 **7.1.1.8 Man-in-the-Middle**

939 **Threat:** Man-in-the-middle attacks are particularly pernicious for this set of profiles. The MITM can relay
940 requests, capture the returned assertion (or artifact), and relay back a false one. Then the original user
941 cannot access the resource in question, but the MITM can do so using the captured resource.

942 **Countermeasures:** Preventing this threat requires a number of countermeasures. First, using a system
943 that provides strong bilateral authentication will make it much more difficult for a MITM to insert himself
944 into the conversation.

945 However the possibility still exists of a MITM who is purely acting as a bidirectional port forwarder, and
946 eavesdropping on the information with the intent to capture the returned assertion or handler (and possibly
947 alter the final return to the requester). Putting a confidentiality system in place will prevent eavesdropping.
948 Putting a data integrity system in place will prevent alteration of the message during port forwarding.

949 For this set of profiles, all the requirements of strong bilateral session authentication, confidentiality, and
950 data integrity can be met by the use of HTTP over TLS/SSL if the TLS/SSL layer uses an appropriate
951 cipher suite (strong enough encryption to provide confidentiality, and supporting data integrity) and
952 requires X509v3 certificates for authentication.

953 **7.1.1.9 Impersonation without Reauthentication**

954 **Threat:** Rogue user attempts to impersonate currently logged-in legitimate Principal and thereby gain
955 access to protected resources.

956 Once a Principal is successfully logged into an identity provider, subsequent <AuthnRequest> messages
957 from different service providers concerning that Principal will not necessarily cause the Principal to be
958 reauthenticated. Principals must, however, be authenticated unless the identity provider can determine
959 that an <AuthnRequest> is associated not only with the Principal's identity, but also with a validly
960 authenticated identity provider session for that Principal.

961 **Countermeasures:** In implementations where this threat is a concern, identity providers MUST maintain
962 state information concerning active sessions, and MUST validate the correspondence between an
963 <AuthnRequest> and an active session before issuing a <Response> without first authenticating the
964 Principal. Cookies posted by identity providers MAY be used to support this validation process, though
965 Liberty does not mandate a cookie-based approach.

966 **7.1.2 Enhanced Client and Proxy Profile**

967 **7.1.2.1 Man in the Middle**

968 **Threat:** Intercept AuthnRequest and Response SOAP messages, allowing subsequent Principal
969 impersonation.

970 A spurious system entity can interject itself as a man-in-the-middle (MITM) between the enhanced client
971 and a legitimate service provider, where it acts in the service provider role in interactions with the
972 enhanced client and in the enhanced client role in interactions with the legitimate service provider. In this
973 way, as a first step, the MITM is able to intercept the service provider's AuthnRequest and substitute any
974 URL of its choosing for the responseConsumerServiceURL value in the PAOS header block before
975 forwarding the AuthnRequest on to the enhanced client. Typically, the MITM will insert a URL value that
976 points back to itself. Then, if the enhanced client subsequently receives an Response from the identity
977 provider and subsequently sends the contained Response to the responseConsumerServiceURL
978 received from the MITM, the MITM will be able to masquerade as the Principal at the legitimate service
979 provider.

980 **Countermeasure:** The identity provider specifies to the enhanced client the address to which the
981 enhanced client must send the Response. The responseConsumerServiceURL in the PAOS header is
982 only used for error responses from the enhanced client – as specified in the profile.

983 **7.1.2.2 Denial of Service**

984 **Threat:** Change an AuthnRequest SOAP request so that it cannot be processed, such as by changing the
985 PAOS header block service attribute value to an unknown value or by changing the ECP header block
986 ProviderID or IDPList to cause the request to fail.

987 **Countermeasures:** Provide integrity protection for the SOAP message, by using SOAP Message Security
988 or SSL/TLS.

989 **7.1.3 Identity Provider Discovery Profile**

990 **Threat:** Cookie poisoning attack, where parameters within the cookie are modified, to cause discovery of
991 an fraudulent identity provider for example.

992 **Countermeasures:** The specific mechanism of using a common domain limits the feasibility of this threat.

993 **7.1.4 Single Logout Profile**

994 **Threat:** Passive attacker can collect a Principal's name identifier

995 During the initial steps, a passive attacker can collect the <LogoutRequest> information when it is issued
996 in the redirect. Exposing these data poses a privacy threat.

997 **Countermeasures:** All exchanges should be conducted over a secure transport such as SSL or TLS.

998 **Threat:** Unsigned <LogoutRequest> message

999 An Unsigned <LogoutRequest> could be injected by a spurious system entity thus denying service to
1000 the Principal. Assuming that the NameID can be deduced or derived then it is conceivable that the user
1001 agent could be directed to deliver a fabricated <LogoutRequest> message.

1002 **Countermeasures:** Sign the <LogoutRequest> message. The identity provider can also verify the
1003 identity of a Principal in the absence of a signed request.

1004 **7.2 Name Identifier Management Profiles**

1005 **Threat:** Allow system entities to correlate information or otherwise inappropriately expose identity
1006 information, harming privacy.

1007 **Countermeasures:** IDP must take care to use different name identifiers with different service providers
1008 for same principal. The IDP SHOULD encrypt the name identifier it returns to the service provider,
1009 allowing subsequent interactions to use an opaque identifier.

1010 **7.3 Attribute Profiles**

1011 Threats related to bindings associated with attribute profiles are discussed above. No additional profile-
1012 specific threats are known.

1013

8 Summary

1014 Security and privacy must be addressed in a systemic manner, considering human issues such as social
1015 engineering attacks, policy issues, key management and trust management, secure implementation and
1016 other factors outside the scope of this document. Security technical solutions have a cost, so
1017 requirements and policy alternatives must also be considered, as must legal and regulatory requirements.

1018 This non-normative document summarizes general security issues and approaches as well as specific
1019 threats and countermeasures for the use of SAML assertions, protocols, bindings and profiles in a secure
1020 manner that maintains privacy. Normative requirements are specified in the normative SAML
1021 specifications.

9 References

1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071

The following are cited in the text of this document:

- [Anonymity]** A. Pfitzmann et al. *Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology*. See http://marit.koehntopp.de/pub/anon/Anon_Terminology.pdf.
- [FIPS]** FIPS SSL Cipher Suites. See <http://www.mozilla.org/projects/security/pki/nss/ssl/fips-ssl-ciphersuites.html>.
- [FreeHaven]** The Free Haven Project: Distributed Anonymous Storage Service
Roger Dingledine & Michael J. Freedman & David Molnar
<http://www.freehaven.net/paper/node6.html>
<http://www.freehaven.net/paper/node7.html>
- [IPsec]** IETF IP Security Protocol Working Group, <http://www.ietf.org/html.charters/ipsec-charter.html>.
- [LibBestPractices]** C. Varney et al. *Privacy and Security Best Practices* Version 2.0. Liberty Alliance Project, November 2003. See http://www.projectliberty.org/specs/final_privacy_security_best_practices.pdf.
- [OCSP]** M. Myers, et al. *X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol – OCSP*. IETF RFC 2560, June 1999, See <http://ietf.org/rfc/rfc2560.txt>.
- [Pooling]** David G. Post. *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*. See <http://www.cli.org/DPost/paper8.htm>.
- [Rescorla-Sec]** E. Rescorla et al. *Guidelines for Writing RFC Text on Security Considerations*, IETF RFC 3552, July 2003. See <http://www.ietf.org/rfc/rfc3552.txt>.
- [RFC2246]** T. Dierks, C. Allen. *The TLS Protocol Version 1.0*. IETF RFC 2246, January 1999. See <http://www.ietf.org/rfc/rfc2246.txt>.
- [RFC2617]** J. Franks et al. *HTTP Authentication: Basic and Digest Access Authentication*. IETF RFC 2617, June 1999. See <http://www.ietf.org/rfc/rfc2617.txt>.
- [SAML11Bind]** P. Mishra et al. *Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1*. OASIS SSTC, September 2003. Document ID oasis-sstc-saml-bindings-1.1. See <http://www.oasis-open.org/committees/security/>.
- [SAMLBind]** S. Cantor et al. *Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-bindings-2.0-os. See <http://www.oasis-open.org/committees/security/>.
- [SAMLCore]** S. Cantor et al. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-core-2.0-os. See <http://www.oasis-open.org/committees/security/>.
- [SAMLGloss]** J. Hodges et al. *Glossary for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-glossary-2.0-os. See <http://www.oasis-open.org/committees/security/>.
- [SAMLProf]** S. Cantor et al. *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*. OASIS SSTC, March 2005. Document ID saml-profiles-2.0-os. See <http://www.oasis-open.org/committees/security/>.
- [ShibMarlena]** Marlena Erdos, *Shibboleth Architecture DRAFT v05*. Shibboleth. See <http://shibboleth.internet2.edu/draft-internet2-shibboleth-arch-v05.html>.
- [SRMPPres]** Shai Kariv. *Message Queuing: Messaging Over The Internet*. See <http://www.microsoft.com/israel/events/teched/presentations/EN308.zip>
- [SSL3]** *The SSL Protocol Version 3.0*. See <http://wp.netscape.com/eng/ssl3/draft302.txt>.
- [WSS]** Web Services Security specifications (WSS), OASIS. See <http://www.oasis-open.org/committees/wss>.
- [WSS-SAML]** P. Hallam-Baker et al. *Web Services Security: SAML Token Profile*, OASIS,

- 1072 March 2003, <http://www.oasis-open.org/committees/wss>.
- 1073 **[XKMS]** P. Hallam-Baker. *XML Key Management Specification (XKMS 2.0)*. World Wide
1074 Web Consortium Candidate Recommendation, April 2004. See
1075 <http://www.w3.org/TR/xkms2/>.
- 1076 **[XMLEnc]** D. Eastlake et al. *XML Encryption Syntax and Processing*. World Wide Web
1077 Consortium. See <http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/>.
- 1078 **[XMLSig]** D. Eastlake et al. *XML-Signature Syntax and Processing*. World Wide Web
1079 Consortium, February 2002. See <http://www.w3.org/TR/xmlsig-core/>.
- 1080 The following additional documents are recommended reading:
- 1081 **[ebXML-MSS]** *Message Service Specification V2.0*. ebXML, April 2002. See [http://www.oasis-](http://www.oasis-open.org/committees/download.php/272/ebMS_v2_0.pdf)
1082 [open.org/committees/download.php/272/ebMS_v2_0.pdf](http://www.oasis-open.org/committees/download.php/272/ebMS_v2_0.pdf). The information about
1083 the security module is the material of interest.
- 1084 **[ebXML-Risk]** *ebXML Technical Architecture Risk Assessment v1.0*. ebXML, 2001. See
1085 <http://www.ebxml.org/specs/secRISK.pdf>.
- 1086 **[Prudent]** Prudent Engineering Practice for Cryptographic Protocols. See
1087 <http://citeseer.nj.nec.com/abadi96prudent.html>.
- 1088 **[Robustness]** Robustness principles for public key protocols. See
1089 <http://citeseer.nj.nec.com/2927.html>.

1090 Appendix A. Acknowledgments

1091 The editors would like to acknowledge the contributions of the OASIS Security Services Technical
1092 Committee, whose voting members at the time of publication were:

- 1093 • Conor Cahill, AOL
- 1094 • John Hughes, Atos Origin
- 1095 • Hal Lockhart, BEA Systems
- 1096 • Mike Beach, Boeing
- 1097 • Rebekah Metz, Booz Allen Hamilton
- 1098 • Rick Randall, Booz Allen Hamilton
- 1099 • Ronald Jacobson, Computer Associates
- 1100 • Gavenraj Sodhi, Computer Associates
- 1101 • Thomas Wisniewski, Entrust
- 1102 • Carolina Canales-Valenzuela, Ericsson
- 1103 • Dana Kaufman, Forum Systems
- 1104 • Irving Reid, Hewlett-Packard
- 1105 • Guy Denton, IBM
- 1106 • Heather Hinton, IBM
- 1107 • Maryann Hondo, IBM
- 1108 • Michael McIntosh, IBM
- 1109 • Anthony Nadalin, IBM
- 1110 • Nick Ragouzis, Individual
- 1111 • Scott Cantor, Internet2
- 1112 • Bob Morgan, Internet2
- 1113 • Peter Davis, Neustar
- 1114 • Jeff Hodges, Neustar
- 1115 • Frederick Hirsch, Nokia
- 1116 • Senthil Sengodan, Nokia
- 1117 • Abbie Barbir, Nortel Networks
- 1118 • Scott Kiestler, Novell
- 1119 • Cameron Morris, Novell
- 1120 • Paul Madsen, NTT
- 1121 • Steve Anderson, OpenNetwork
- 1122 • Ari Kermaier, Oracle
- 1123 • Vamsi Motukuru, Oracle
- 1124 • Darren Platt, Ping Identity
- 1125 • Prateek Mishra, Principal Identity
- 1126 • Jim Lien, RSA Security
- 1127 • John Linn, RSA Security
- 1128 • Rob Philpott, RSA Security
- 1129 • Dipak Chopra, SAP
- 1130 • Jahan Moreh, Sigaba
- 1131 • Bhavna Bhatnagar, Sun Microsystems
- 1132 • Eve Maler, Sun Microsystems

- 1133 • Ronald Monzillo, Sun Microsystems
- 1134 • Emily Xu, Sun Microsystems
- 1135 • Greg Whitehead, Trustgenix

1136 The editors also would like to acknowledge the following former SSTC members for their contributions to
1137 this or previous versions of the OASIS Security Assertions Markup Language Standard:

- 1138 • Stephen Farrell, Baltimore Technologies
- 1139 • David Orchard, BEA Systems
- 1140 • Krishna Sankar, Cisco Systems
- 1141 • Zahid Ahmed, CommerceOne
- 1142 • Tim Alsop, CyberSafe Limited
- 1143 • Carlisle Adams, Entrust
- 1144 • Tim Moses, Entrust
- 1145 • Nigel Edwards, Hewlett-Packard
- 1146 • Joe Pato, Hewlett-Packard
- 1147 • Bob Blakley, IBM
- 1148 • Marlena Erdos, IBM
- 1149 • Marc Chanliau, Netegrity
- 1150 • Chris McLaren, Netegrity
- 1151 • Lynne Rosenthal, NIST
- 1152 • Mark Skall, NIST
- 1153 • Charles Knouse, Oblix
- 1154 • Simon Godik, Overxeer
- 1155 • Charles Norwood, SAIC
- 1156 • Evan Prodromou, Securant
- 1157 • Robert Griffin, RSA Security (former editor)
- 1158 • Sai Allarvarpu, Sun Microsystems
- 1159 • Gary Ellison, Sun Microsystems
- 1160 • Chris Ferris, Sun Microsystems
- 1161 • Mike Myers, Traceroute Security
- 1162 • Phillip Hallam-Baker, VeriSign (former editor)
- 1163 • James Vanderbeek, Vodafone
- 1164 • Mark O'Neill, Vordel
- 1165 • Tony Palmer, Vordel

1166 Finally, the editors wish to acknowledge the following people for their contributions of material used as
1167 input to the OASIS Security Assertions Markup Language specifications:

- 1168 • Thomas Gross, IBM
- 1169 • Birgit Pfitzmann, IBM

1170 **Appendix B. Notices**

1171 OASIS takes no position regarding the validity or scope of any intellectual property or other rights that
1172 might be claimed to pertain to the implementation or use of the technology described in this document or
1173 the extent to which any license under such rights might or might not be available; neither does it represent
1174 that it has made any effort to identify any such rights. Information on OASIS's procedures with respect to
1175 rights in OASIS specifications can be found at the OASIS website. Copies of claims of rights made
1176 available for publication and any assurances of licenses to be made available, or the result of an attempt
1177 made to obtain a general license or permission for the use of such proprietary rights by implementors or
1178 users of this specification, can be obtained from the OASIS Executive Director.

1179 OASIS invites any interested party to bring to its attention any copyrights, patents or patent applications, or
1180 other proprietary rights which may cover technology that may be required to implement this specification.
1181 Please address the information to the OASIS Executive Director.

1182 **Copyright © OASIS Open 2005. All Rights Reserved.**

1183 This document and translations of it may be copied and furnished to others, and derivative works that
1184 comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and
1185 distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and
1186 this paragraph are included on all such copies and derivative works. However, this document itself may
1187 not be modified in any way, such as by removing the copyright notice or references to OASIS, except as
1188 needed for the purpose of developing OASIS specifications, in which case the procedures for copyrights
1189 defined in the OASIS Intellectual Property Rights document must be followed, or as required to translate it
1190 into languages other than English.

1191 The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors
1192 or assigns.

1193 This document and the information contained herein is provided on an "AS IS" basis and OASIS
1194 DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY
1195 WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR
1196 ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.