

STATE SERVICES COMMISSION
Te Komihana O Nga Tari Kāwanatanga



THE DEPARTMENT OF INTERNAL AFFAIRS

Te Tari Taiwhenua

Amendments to Authentication Standards

State Services Commission
Department of Internal Affairs
September 2008
Version 4.0

Table of Contents

1. Introduction.....	3
2. Amendment AS06/2008 (Rev 1.0).....	4
1. Authentication Key Strengths Standard.....	4
1. All-of-government authentication services (3.2).....	4
2. Terms and definitions (4.6).....	4
3. Authentication protocols: threats and attacks (5.2).....	5
4. Requirements for online services in the Moderate Risk Category (6.9).....	5
5. Requirements for online services in the High Risk Category (6.10).....	6
2. Password Standard.....	6
1. All-of-government authentication services (3.2).....	6
2. Password construction (6.4).....	7
3. Password management (6.5).....	7
3. Guide to Authentication Standards.....	7
1. Misuse and abuse of identity (3.2).....	7
2. All-of-government authentication services (3.5).....	8
3. Definitions (Appendix A).....	8
3. Amendment AS03/2008.....	10
1. Evidence of Identity Standard.....	10
1. New Zealand Birth Certificate (Appendix A, page 105).....	10
2. New Zealand Driver Licence (Appendix A, pages 110 - 111).....	10
3. IR number (Appendix A, page 116).....	10
4. International Driving Permit (Appendix B, page 119).....	10
4. Amendment AS06/2007.....	11
1. Guide to Authentication Standards for Online Services Standard.....	11
2. Data Formats for Identity Records Standard.....	11
3. Authentication Key Strength Standard.....	11
5. SCHEDULE AS06/2008 (Rev 1.0).....	12

1. Introduction

In accordance with the provisions of the Authentication Standards, the *Authentication Standards for Online Services* Working Groups may from time to time agree to minor corrections, additional explanations, amendments or revisions of these Standards. Such changes will also be included in any subsequent re-printings of the Standards concerned.

2. Amendment AS06/2008 (Rev 1.0)

This minor revision to AS06/2008 introduces minor changes in '3. Guide to Authentication Standards'; primarily the removal of some of the definitions added in AS06/2008 that were duplications of those already contained in the Guide.

NOTE: The New Zealand Security Assertion Messaging Standard (NZ SAMS) Version 1.0 and the Data formats for Identity Records Standard Version 1.1 are shortly to be published in their entirety. Amendments to these do not appear in Amendment AS06/2008.

1. Authentication Key Strengths Standard

1. All-of-government authentication services (3.2)

Clause 3.2 (All-of-government authentication services), is hereby amended by deleting paragraph 2 and substituting it with the following:

“The GLS is a website that allows people to access government online services more conveniently by using a common authentication mechanism appropriate to the service risk category established for the service. The IVS will allow people to establish their identity once so that they do not have to establish their identity separately with each agency that uses the IVS they transact with. See 4.6 for definitions of the GLS and IVS”.

Clause 3.2 is hereby further amended by deleting paragraph 4 and substituting it with the following:

“Where agencies adopt one or more of these shared services, they must adopt the standards relating to the functions of those services. Adopting the service relieves agencies of some (but not all) obligations regarding standards adoption, since the service itself implements the standards applicable to its area of responsibility. However, significant areas of the standards under the responsibility of the agency remain, such as risk assessments and agency web site controls”.

2. Terms and definitions (4.6)

Clause 4.6 (Terms and definitions), is hereby amended by

deleting the term “*Proof of possession protocol*” and its accompanying definition from the table.

Clause 4.6 is hereby further amended by adding two new definitions under the Authentication keys section of the table as follows:

“Weak mutual authentication – Where one authenticating party can use duplicity to obtain authentication keys or data which they may later use to fraudulently authenticate themselves”.

“Strong mutual authentication – Where two authenticating parties can authenticate reliably without revealing any authentication keys or data that may be used subsequently to fraudulently authenticate by posing as the other party. With strong mutual authentication the authentication process provides confidence in the other parties claimed identity, but does not leave either

party with any information that may later be used to impersonate the other party”.

Clause 4.6 is hereby further amended by deleting the definition of one-time password and substituting it with the following:

“One-time password systems utilise a series of passwords in the authentication process. Each password of the series is called a one-time password as they are all distinct and unpredictable (or at least distinct and unpredictable with a very high probability). Many methods are based on a static shared base secret that is used to generate the distinct authentication secrets. Other common methods use collections of passwords that are distributed to customers”.

3. Authentication protocols: threats and attacks (5.2)

Clause 5.2 (Authentication protocols: threats and attacks), is hereby amended by deleting bullet point 3 and substituting it with the following:

“Man-in-the-middle and verifier impersonation attacks can be resisted in a limited way by using similar protections as described above for eavesdropper and session hijacking attacks, this is effectively weak mutual authentication. Combining the channel encryption with additional cryptographic techniques improves protection against these attacks and is effectively strong mutual authentication (for example, using a mutual handshake exchange based around cryptography and cryptographic keys held by the customer and the verifier, such as TLS in authentication mode, achieves strong mutual authentication)”.

4. Requirements for online services in the Moderate Risk Category (6.9)

Clause 6.9 (Requirements for online services in the Moderate Risk Category), is hereby amended by deleting the entire clause and substituting it with the following:

“When the online service is in the Moderate Risk Category, agencies MUST:

- *Use at least two-factor authentication to authenticate the customer, using one of the following authentication keys:
 - a) *a one-time password system combined with a password*
 - b) *a one-time password device that requires per-session local activation with a password or biometric*
 - c) *a software token that requires per-session local activation with a password or biometric.**
- *Protect the authentication exchange using GCSB approved encryption technology conforming to the requirements of SIGS and NZSIT 402.*
- *Ensure the authentication process is resistant to replay, eavesdropper and session hijacking attacks.*

- *Use weak mutual authentication in cases where a one-time password is used to authenticate the customer (refer 5.2).*
- *Use strong mutual authentication in cases where a software token is used to authenticate the customer (refer 5.2)”.*

5. Requirements for online services in the High Risk Category (6.10)

Clause 6.10 (Requirements for online services in the High Risk Category), is hereby amended by deleting the entire clause and substituting it with the following:

“When the online service is in the High Risk Category, agencies MUST:

- *Use at least two-factor authentication to authenticate the customer.*
- *Authenticate the customer using (at least) a hardware token that requires per-session local activation with a password or biometric.*
- *Protect the authentication exchange using GCSB approved encryption technology conforming to the requirements of SIGS and NZSIT 402.*
- *Ensure the authentication process is resistant to replay, eavesdropper and session hijacking attacks.*
- *Use strong mutual authentication (refer 5.2)”.*

2. Password Standard

1. All-of-government authentication services (3.2)

Clause 3.2 (All-of-government authentication services), is hereby amended by deleting paragraph 2 and substituting it with the following:

“The GLS is a website that will allow people to access government online services more conveniently by using a common authentication mechanism appropriate to the service risk category established for the service. The IVS will allow people to establish their identity once so that they do not have to establish their identity separately with each agency that uses the IVS they transact with. See 4.6 for definitions of the GLS and IVS”.

Clause 3.2 is hereby further amended by deleting paragraphs 4 and 5 and substituting them with the following:

“Where agencies adopt one or more of these shared services, they must adopt the standards relating to the functions of those services. Adopting the service relieves agencies of some (but not all) obligations regarding standards adoption, since the service itself implements the standards applicable to its area of responsibility. However, significant areas of the standards under the responsibility of the agency remain, such as risk assessments and agency web site controls”.

2. Password construction (6.4)

Clause 6.4 (Password construction) sub-clause 6.4.2, is hereby amended by deleting the sub-clause and substituting it with the following:

“Passwords MUST be a minimum of seven (7) characters. Passwords SHOULD contain characters from at least three (3) of the following sets:”

1. Lowercase characters (a-z).
2. Uppercase characters (A-Z).
3. Digits (0-9).
4. Punctuation and special characters (for example, !@#%&^*).

These requirements MUST be enforced by the system”.

3. Password management (6.5)

Clause 6.5 (Password management), is hereby amended by deleting sub-clause 6.5.1 and substituting it with the following:

“6.5.1(A) Agencies MUST:

- *Protect passwords in storage and during the online authentication exchange. (Requirements for the authentication exchange protection of passwords are detailed in the Authentication Key Strengths Standard.)*
- *Require the customer to change an initial logon or a reset password immediately following authentication with that password”.*

“6.5.1(B) Agencies SHOULD:

- *Require passwords to be changed at least every 90 days.*
- *Retain a password history of at least the last six (6) passwords used by a customer.*
- *Ensure that the customer does not use a password from their password history”.*

Clause 6.5 is hereby further amended by deleting sub-clause 6.5.5 and substituting it with the following:

“6.5.5 Agencies MUST ensure that the full password is not visible on the screen when entered”.

3. Guide to Authentication Standards

1. Misuse and abuse of identity (3.2)

Clause 3.2 (Misuse and abuse of identity), is hereby amended by

deleting the word *“stolen”*, where it appears in two instances, and substituting them with the word *“assumed”*.

Clause 3.2 is hereby further amended by adding to the bullet-points the following:

“ . *damage to credibility of process* ”.

2. All-of-government authentication services (3.5)

Clause 3.5 (All-of-government authentication services), is hereby amended by deleting paragraph 2 and substituting it with the following:

“The GLS is a website that allows people to access government online services more conveniently by using a common authentication mechanism appropriate to the service risk category established for the service. The IVS will allow people to establish their identity once so that they do not have to establish their identity separately with each agency that uses the IVS they transact with. See Appendix A for definitions of the GLS and IVS”.

Clause 3.5 is hereby further amended by deleting paragraph 4 and substituting it with the following:

“Where agencies adopt one or more of these shared services, they must adopt the standards relating to the functions of those services. Adopting the service relieves agencies of some (but not all) obligations regarding standards adoption, since the service itself implements the standards applicable to its area of responsibility. However, significant areas of the standards under the responsibility of the agency remain, such as risk assessments and agency web site controls”.

3. Definitions (Appendix A)

Appendix A (Definitions), is hereby amended by

deleting the term “*Proof of possession protocol*” and its accompanying definition from the table.

Appendix A is hereby further amended by adding two new definitions as follows:

“Weak mutual authentication – Where one authenticating party can use duplicity to obtain authentication keys or data which they may later use to fraudulently authenticate themselves”.

“Strong mutual authentication – Where two authenticating parties can authenticate reliably without revealing any authentication keys or data that may be used subsequently to fraudulently authenticate by posing as the other party. With strong mutual authentication the authentication process provides confidence in the other parties claimed identity, but does not leave either party with any information that may later be used to impersonate the other party”.

Appendix A is hereby further amended by deleting the definition of one-time password and substituting it with the following:

“One-time password systems utilise a series of passwords in the authentication process. Each password of the series is called a one-time password as they are all distinct and unpredictable (or at least distinct and unpredictable with a very high probability). Many methods are based on a static shares base secret that is used to generate the distinct authentication secrets. Other common methods use collections of passwords that are distributed to customers”.

Appendix A – (Definitions) is hereby amended by

deleting from the Definition of ‘Identity – misuse and abuse’, the word “*stolen*” and substituting it with the word “*assumed*”.

Appendix A is hereby further amended by

deleting from the Definition of ‘Identity theft’, the words “*Theft or*”.

Appendix A is hereby further amended by

adding the following Term and Definition:

“Party - Party means a person in this Standard. However, the CIQ v3.0 Specifications use the term party to mean a person or an organisation”.

Appendix A is hereby further amended by

adding the Terms and Definitions as detailed in the attached [Schedule](#).

(Explanation – these additional terms and definitions were introduced as a result of the subsequent publishing of the New Zealand Security Assertion Messaging Standard, v1.0 June 2008).

3. Amendment AS03/2008

1. Evidence of Identity Standard

1. New Zealand Birth Certificate (Appendix A, page 105)

Standard fit is hereby amended by replacing the last sentence in paragraph 2 (“*Birth certificates contain a warning to the effect that ‘this certificate is not evidence of the person presenting it’.*”) with:

“A birth certificate is not evidence of identity of the person presenting it.”

2. New Zealand Driver Licence (Appendix A, pages 110 - 111)

Validity is hereby amended by:

changing “*ten years*” to “*up to eleven years*”.

Issuance process is hereby amended by:

replacing “*primary identification*” in both lines 2 and 4 of paragraph 1 with “*evidence of identity*”

deleting “*or overseas driver licence*” in line 5 of paragraph 1.

Legislation is hereby amended by:

adding “*Land Transport (Driver Licensing) Rule 1999*”.

Further information is hereby amended by:

replacing “www.ltsa.govt.nz” with “www.landtransport.govt.nz”.

3. IR number (Appendix A, page 116)

Purpose is hereby amended by:

deleting the second sentence, ie. “*All individuals receiving income in New Zealand are required to have an IR number.*”

4. International Driving Permit (Appendix B, page 119)

Sentence 2 under bullet point 2 (“*The IDP is valid for 12 months from the date of issue.*”) is hereby replaced with:

“New Zealand is a signatory to the 1949 United Nations Convention on Road Traffic. This permits New Zealand issued IDPs to have a maximum period of 12 months. A number of countries have since signed the 1968 United Nations Convention on Road Traffic, as a result they are authorised to issue IDPs with a maximum period of validity of five years.”

4. Amendment AS06/2007

1. Guide to Authentication Standards for Online Services Standard

Clause 3.3 (Internet-related misuse and abuse of identity) is hereby amended to replace the words contained in parentheses at line 3 of paragraph 2 as follows:

“(such as monetary, or information theft through the unlawful assumption of another person’s details)”

2. Data Formats for Identity Records Standard

Clause 6.4.3 (PersonInfo container) is hereby amended to add the following note after Figure 6:

“Note. XML Spy representations may restrict the ability to show all elements e.g. Gender, mother's name, etc in the above diagram, but may be seen in Appendix E.”

Figure 6 is hereby amended to replace:

the titles of the BirthInfo sub-containers from “*Birth:nfoE:ment*” to “*BirthInfoElement*”, and “*BirthP:ace*” to “*BirthPlace*”.

3. Authentication Key Strength Standard

Clause 6.7 (Requirements for online services in the Nil/Negligible Risk Category) is hereby amended to add the following to the Note:

“Customer experience and/or other reasons may lead agencies to use the same password across the Low and Nil/Negligible Risk categories. In this case all requirements of Clause 6.8 must be followed even for services in the Nil/Negligible Risk Category”

5. SCHEDULE AS06/2008 (Rev 1.0)

Term	Definition
Asserting party [SAML]	Informally, an instance of a SAML authority.
Assertion [SAML]	A piece of data produced by a SAML authority regarding either an act of authentication performed on a subject, attribute information about the subject, or authorisation data applying to the subject with respect to a specified resource.
Attribute [SAML]	A distinct characteristic of an object (in SAML, of a subject). An object's attributes are said to describe it. Attributes are often represented as pairs of attribute name and attributes values...often referred to as attribute pairs. [edited]
Attribute assertion [SAML]	An assertion that conveys information about attributes of a subject.
Attribute authority [SAML]	A system entity that produces attribute assertions.
Authorisation [SAML]	The process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource. Usually, authorisation is in the context of authentication. Once a subject is authenticated, it may be authorised to perform different types of access.
Back channel [SAML]	Direct communications between two system entities without 'redirecting' messages through another system entity such as an HTTP client (e.g. a user agent). See also front channel.
Binding, Protocol binding [SAML]	Generically, a specification of the mapping of some given protocol's messages, and perhaps message exchange patterns, onto another protocol, in a concrete fashion. For example, the mapping of the SAML <AuthnRequest> message onto HTTP is one example of a binding. The mapping of that same SAML message onto SOAP is another binding. In the SAML context, each binding is given a name in the pattern 'SAML xxx binding.'
Cookie [Webopedia]	A piece of information stored in a browser by a web server, which is then sent back to the web server each time the browser requests a page from that server.

Term	Definition
Entity, System entity [SAML] [SSC]	<p>An active element of a computer/network system. For example, an automated process or set of processes, a subsystem, a person or group of persons that incorporates a distinct set of functionality. (RFC2828)</p> <p>NOTE –NZ SAMS also refers to ‘machine entity’ to make an entity such as a computer distinct from an entity that encompasses a person or group of persons</p>
Federated identity [SAML] [SSC]	<p>A principal’s identity is said to be federated between a set of providers when there is an agreement between the providers on a set of identifiers and/or attributes to use to refer to the principal.</p> <p>Identity Federation – the act of creating a federated identity on behalf of a principal.</p> <p>NOTE –NZ SAMS uses the terms:</p> <p>NOTE –‘Federated identifier’ to mean the identifier unique to an individual’s identity paired with the particular service agency with which the individual transacts.</p> <p>NOTE –‘Federated logon tag’ to mean the name given to the federated identifier used in the GLS implementation.</p>
Federation [SAML]	<p>This term is used in two senses in SAML:</p> <ul style="list-style-type: none"> (a) The act of establishing a relationship between two entities (b) An association comprising any number of service providers and identity providers.
Front channel [SAML]	<p>The ‘communications channel’ that can be effected between two HTTP-speaking servers by employing ‘HTTP redirect’ messages and thus passing messages between each via a user agent, e.g. a web browser, or any other HTTP client (RFC2616). See also back channel.</p>
Government Shared Network (GSN) [SSC]	<p>The Government Shared Network (GSN) enables government agencies to collaborate securely and more cost effectively. The shared network improves the delivery of information and services to the New Zealand public. Phase 1 includes interagency linking, wide area network links, internet services and remote access services.</p>

Term	Definition
Identifier [SAML]	<p>This term is used in two senses in SAML:</p> <p>(a) One that identifies.</p> <p>(b) A data object (for example, a string) mapped to a system entity, which uniquely refers to the system entity. A system entity may have multiple distinct identifiers referring to it.</p> <p>An identifier is essentially a ‘distinguished attribute’ of an entity. See also Attribute.</p>
Identity Provider (IdP) [SAML]	<p>A kind of service provider that creates, maintains, and manages identity information for principals and provides principal authentication to other service providers within a federation, such as with web browser profiles.</p> <p>Provider: a generic way to refer to both identity providers and service providers.</p> <p>(An example of an identity provider is the Government Logon Service.)</p> <p>Note: In the nomenclature of actors enumerated in the Assertions and Protocols specification [SAMLCore] the identity provider is synonymous with a ‘SAML Authority.’</p>
igovt	<p>The brand for the All-of-government Authentication Programme all-of-government shared services, i.e. the Government Logon Service, Identity Verification Service, and Future Services.</p>
Logon, Sign-on [edited] [SAML]	<p>The process whereby a service user presents credentials to an Authentication Authority, establishes a simple session, and optionally establishes a rich session.</p> <p>(Logout, Logoff, Sign-off: The process whereby a service user signifies desire to terminate a simple session or rich session.)</p>
NIST [Webopedia]	<p>National Institute of Science and Technology</p>
Party [SAML]	<p>Informally, one or more principals participating in some process or communication, such as receiving an assertion or accessing a resource.</p>

Term	Definition
Principal [SAML]	<p>A system entity whose identity can be authenticated.</p> <p>(Principal identity: A representation of a principal's identity, typically an identifier.)</p>
Profile [SAML]	<p>A set of rules for one of several purposes; each set is given a name in the pattern 'xxx profile of SAML' or 'xxx SAML profile.'</p> <p>Included are:</p> <ul style="list-style-type: none"> (a) Rules for how to embed assertions into and extract them from a protocol or other context of use. (b) Rules for using SAML protocol messages in a particular context of use. (c) Rules for mapping attributes expressed in SAML to another attribute representation system. Such a set of rules is known as an 'attribute profile.'
Proxy [SAML]	<p>An entity authorised to act for another.</p> <p>This includes:</p> <ul style="list-style-type: none"> (a) Authority or power to act for another. (b) A document giving such authority.
Relying party [SAML]	<p>A system entity that decides to take an action based on information from another system entity. For example, a SAML relying party depends on receiving assertions from an asserting party (a SAML authority) about a subject. (See also the definition of 'asserting party' above.</p> <p>NOTE —In the nomenclature of actors enumerated in the Assertions and Protocols document, section 3.4 [SAMLCore] the relying party is the request issuer and the service provider.</p>
Requester, SAML requester [SAML]	<p>A system entity that utilises the SAML protocol to request services from another system entity (a SAML authority, a responder). The term 'client' for this notion is not used because many system entities simultaneously or serially act as both clients and servers. In cases where the SOAP binding for SAML is being used, the SAML requester is architecturally distinct from the initial SOAP sender.</p>

Term	Definition
Resource [SAML]	<p>Data contained in an information system (for example, in the form of files, information in memory, etc), as well as:</p> <ul style="list-style-type: none"> (a) A service provided by a system. (b) An item of system equipment (in other words, a system component such as hardware, firmware, software, or other documentation). (c) A facility that houses system operations and equipment. <p>[RFC2828]</p> <p>SAML uses resource in the first two senses, and refers to resources by means of URI references.</p>
Responder, SAML responder [SAML]	<p>A system entity (a SAML authority) that utilises the SAML protocol to respond to a request for services from another system entity (a requester). The term ‘server’ for this notion is not used because many system entities simultaneously or serially act as both clients and servers. In cases where the SOAP binding for SAML is being used, the SAML responder is architecturally distinct from the ultimate SOAP receiver.</p>
Security [SAML]	<p>A collection of safeguards that ensure the confidentiality of information, protect the systems or networks used to process it, and control access to them. Security typically encompasses the concepts of secrecy, confidentiality, integrity, and availability. It is intended to ensure that a system resists potentially correlated attacks.</p>
SAML artifact [SAML]	<p>A small, fixed-size, structured data object pointing to a typically larger, variably-sized SAML protocol message. SAML artifacts are designed to be embedded in URLs and conveyed in HTTP messages, such as HTTP response messages with ‘3xx Redirection’ status codes, and subsequent HTTP GET messages. In this way, a service provider may indirectly, via a user agent, convey a SAML artifact to another provider, who may subsequently dereference the SAML artifact via a direct interaction with the supplying provider, and obtain the SAML protocol message. Various characteristics of the HTTP protocol and user agent implementations provided the impetus for concocting this approach. The HTTP Artifact binding section of [SAMLBind] defines both the SAML Artifact format and the SAML HTTP protocol binding incorporating it.</p>

Term	Definition
SAML authority [SAML]	<p>An abstract system entity in the SAML domain model that issues assertions. See also ‘attribute authority,’ (and ‘authentication authority’ and ‘policy decision point’ (PDP) in the OASIS SAML v2.0 Glossary [edited].</p> <p>NOTE –In the nomenclature of actors enumerated in the Assertions and Protocols document [SAMLCore] the SAML authority is usually synonymous with ‘identity provider.’</p>
Security context [SAML]	<p>With respect to an individual SAML protocol message, the message’s security context is the semantic union of the message’s security header blocks (if any) along with other security mechanisms that may be employed in the message’s delivery to a recipient. With respect to the latter, examples are security mechanisms employed at lower network stack layers such as HTTP, TLS/SSL, IPSEC, etc.</p> <p>With respect to a system entity, ‘Alice’, interacting with another system entity, ‘Bob’, a security context is nominally the semantic union of all employed security mechanisms across all network connections between Alice and Bob. Alice and Bob may each individually be, for example, a provider or a user agent. This notion of security context is similar to the notion of ‘security contexts’ as employed in RFC2743, and in the Distributed Computing Environment (DCE), for example.</p>
Service provider (SP) [SAML]	<p>A role donned [taken] by a system entity where the system entity provides services to principals or other system entities.</p> <p>In the context of this Standard, it is a government agency providing online services.</p> <p>NOTE –In the nomenclature of actors enumerated in the Assertions and Protocols document, section 3.4 [SAMLCore]. The service provider is the request issuer and the relying party.</p>
Service risk category (SRC) [SSC]	<p>Each service risk category is defined based on the identity-related risk of a service and is detailed in the <i>Evidence of Identity Standard</i> [EOIS].</p>
Session [SAML]	<p>A lasting interaction between system entities, often involving a principal, typified by the maintenance of some state of the interaction for the duration of the interaction.</p>

Term	Definition
Single sign-on (SSO) [Webopedia]	<p>An authentication process in a client/server relationship where the user, or client, can enter one name and password and have access to more than one application or access to a number of resources within an enterprise. Single sign-on takes away the need for the user to enter further authentications when switching from one application to another.</p> <p>Single sign-on is also spelled single sign on or single sign-on and abbreviated as SSO.</p>
Single sign-off [Wikipedia]	<p>Single sign-off is the reverse of single sign-on, where a single action of signing out terminates access to multiple software systems.</p>
SOAP [Webopedia]	<p>Short for Simple Object Access Protocol, a lightweight XML-based messaging protocol used to encode the information in Web Service request and response messages before sending them over a network. SOAP messages are independent of any operating system or protocol and may be transported using a variety of internet protocols, including SMTP, MIME, and HTTP.</p>
Subject [SAML]	<p>A principal in the context of a security domain. SAML assertions make declarations about subjects.</p>
Uniform Resource Identifier (URI) [Webopedia]	<p>Uniform Resource Identifier is the generic term for all types of names and addresses that refer to objects on the World Wide Web. (Uniform Resource Locator (URL) is one type of URI.)</p>
Web Services [Webopedia]	<p>A term used to describe a standardised way of integrating Web-based applications using the XML, SOAP, WSDL and UDDI open standards over IP.</p>
W3C [Webopedia]	<p>Short for World Wide Web Consortium, an international consortium of companies involved with the Internet and the Web. The W3C was founded in 1994 by Tim Berners-Lee, the original architect of the World Wide Web. The organisation's purpose is to develop open standards so that the Web evolves in a single direction rather than being splintered among competing factions.</p>

Term	Definition
XML Attribute [SAML]	<p>An XML data structure that is embedded in the start-tag of an XML element and that has a name and a value. For example, the italicised portion below is an instance of an XML attribute:</p> <pre data-bbox="592 443 1190 472"><Address <i>AddressID="A12345"</i>>...</Address></pre>
XML Element [SAML]	<p>An XML data structure that is hierarchically arranged among other such structures in an XML document and is indicated by either a start-tag and end-tag or an empty tag. For example :</p> <pre data-bbox="592 667 1007 734"><AssertionConsumerService>... </AssertionConsumerService></pre>

END OF DOCUMENT