SAML V2.0 Profile for Mandator Credentials

Specification URIs:

This Version:

Previous Version:

Latest Version:

Technical Committee:

OASIS Security Services TC

Chair(s):

Hal Lockhart, Oracle Corporation
Thomas Hardjono, MIT

Editors:

Federico Rossini, Telecom Italia

Contributors:

Declared XML Namespace(s):

`urn:oasis:names:tc:SAML:2.0:mgmt`

Abstract:

Based on Telecom Italia proposal of the Telecom SOA Requirement **[*SOA-TEL req*]**.

The protocol here described makes possible to add other security credentials in the SAML assertions.

Status

This is initial draft of the mandator credential profile based on Telecom Italia requirement (OASIS Telecom SOA Requirements Version 1.0, http://docs.oasis-open.org/soa-tel/t-soa-req1.0/cd01/t-soa-req-01-cd-02.pdf) and use case (OASIS Telecom SOA Use Case and Issues Version 1.0, http://docs.oasis-open.org/soa-tel/t-soa-uci/v1.0/cs01/t-soa-uc-cs-01.pdf)

TC members should send comments on this specification to the TC's email list.
Others should send comments to the TC by using the "Send A Comment" button on the TC's web page at http://www.oasis-open.org/committees/security.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the IPR section of the TC web page (http://www.oasis-open.org/committees/security/ipr.php).

The non-normative errata page for this specification is located at http://www.oasis-open.org/committees/security.

Notices

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

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

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

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and

implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see http://www.oasis-open.org/who/trademark.php for above guidance.

Table of Contents

1 Introduction

The following specification makes possible to insert into a SAML assertion additional security credentials.

1.1 Notation

This specification uses normative text. The keywords "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this specification are to be interpreted as described in :

> …they MUST only be used where it is actually required for interoperation or to limit behavior which has potential for causing harm (e.g., limiting retransmissions)…

These keywords are thus capitalized when used to unambiguously specify requirements over protocol and application features and behavior that affect the interoperability and security of implementations. When these words are not capitalized, they are meant in their natural-language sense.

```
Listings of XML schemas appear like this.
```

```
Example code listings appear like this.
```

Conventional XML namespace prefixes are used throughout the listings in this specification to stand for their respective namespaces as follows, whether or not a namespace declaration is present in the example:

Prefix	XML Namespace	Comments
`saml:`	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace defined in the SAML V2.0 core specification [SAML2Core].
`ds:`	http://www.w3.org/2000/09/xmldsig#	This is the XML Signature namespace [XMLSig].
`xs:`	http://www.w3.org/2001/XMLSchema	This is the XML Schema namespace .
`xsi:`	http://www.w3.org/2001/XMLSchema-instance	This is the XML Schema namespace for schema-related markup that appears in XML instances .

This specification uses the following typographical conventions in text: `<SAMLElement>`, `<ns:ForeignElement>`, `Attribute`, **Datatype**, `OtherCode`.

1.2 Terminology

1.3 Normative References

[*SOA-TEL req*] Ronco et al. *Telecom SOA Requirements Version 1.0* OASIS SOA-TEL TC, Date. http://docs.oasis-open.org/soa-tel/t-soa-req1.0/cd01/t-soa-req-01-cd-02.pdf .

[*SOA-TEL UC*] Ronco et al. *Telecom SOA Use Cases and Issues 1.0* OASIS SOA-TEL TC, Date. http://docs.oasis-open.org/soa-tel/t-soa-uci/v1.0/cs01/t-soa-uc-cs-01.pdf.

[SAML2Core] OASIS Standard, *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0.* March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[SAML2Prof] OASIS Standard, *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0.* March 2005. http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

1.4 Non-normative References

2 Mandator credential specification

2.1 Required Information

Identification: urn:oasis:names:tc:SAML:2.0:mandator????

Contact information: security-services-comment@lists.oasis-open.org

Description: Given below.

Updates: None.

2.2 Description

The following specification makes possible to insert into a SAML assertion additional security credentials.

The extra security credentials make possible to execute additional security routines.

The extra security credentials usually represent the user requestor (the actor who started the business process).

2.3 Assumptions

2.4 Elements <Mandator>

The mandator element contains additional security credentials, to be used by the services invoked.

Usually the element is designed to carry the credentials of the user who started the process which the service invocation belongs to.

The mandator element is a sub element of the <Statement> element, it is optional.

The mandator element contains an identifier:

<BaseID>, <NameID>, or <EncryptedID> [Optional]

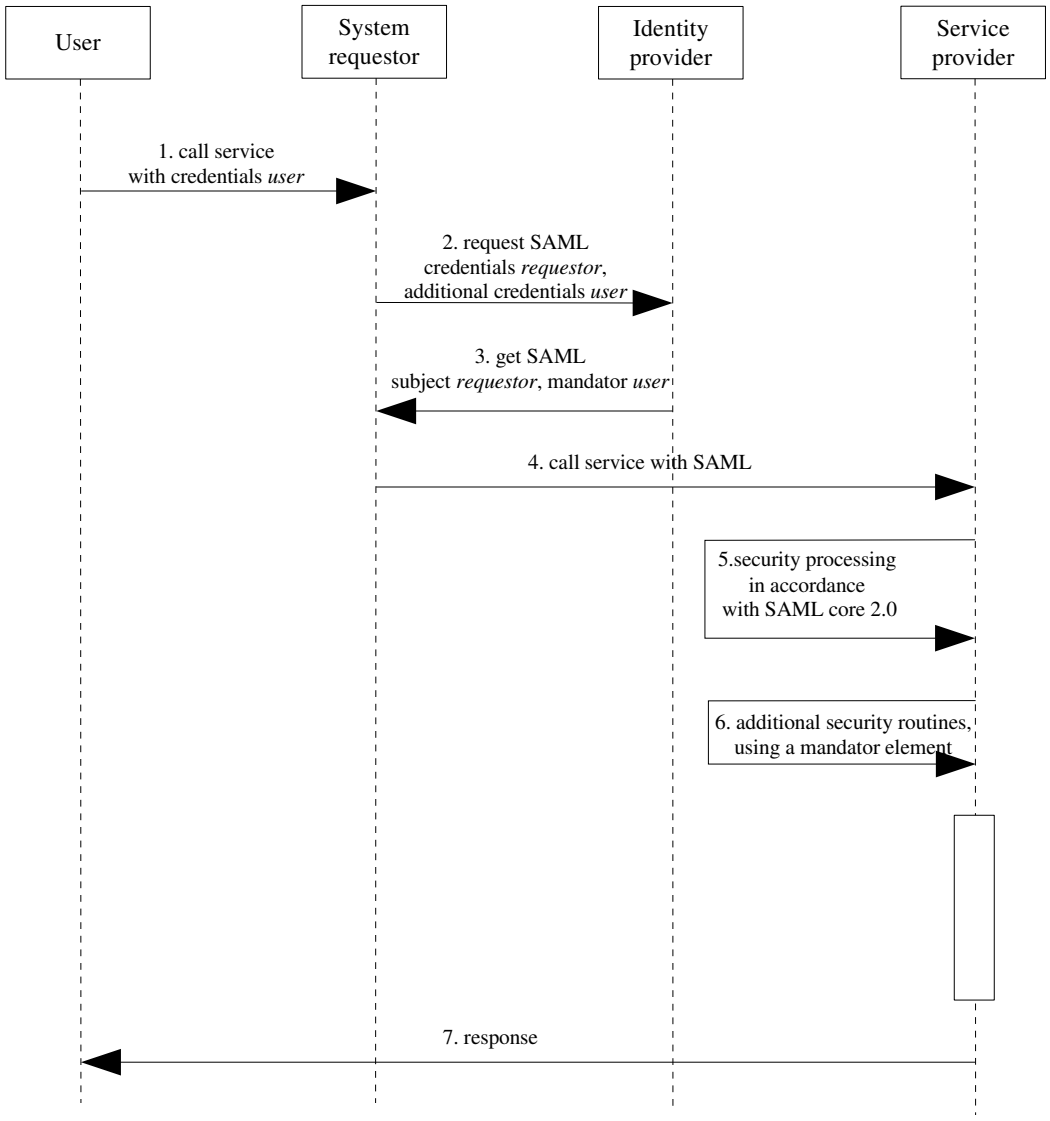
The following schema fragment defines the <Mandator> element and its MandatorType complex type:

```
<element name="Mandator" type="saml:MandatorType"/>
<complexType name="MandatorType">
<choice>
<element ref="saml:BaseID"/>
<element ref="saml:NameID"/>
<element ref="saml:EncryptedID"/>
</choice>
</complexType>
```

2.5 Processing Rules

The credentials carried in the <mandator> element is intended for additional security functionalities, different from those that implement the standard processing rules of a SAML assertion, its use never overlaps with that of the credentials present in the subject field of the SAML assertion.

The processing rules depends from the security context that has required the additional credential.



3 Conformance

Appendix A. Use Cases

The use case is that of a Web Service exposed by an Application Provider, and the scenarios is a Customer Care portal accessed by both operator customers and personnel (Call Center Operators), each of them having different “rights” on accessed data.

Customer Care portal accessed by both operator customers and personnel (Call Center Operators)

C1 is a Portal for Customer Caring that consumes a Web Service (WS-A) for retrieving profile information. It is used by both Customers (for Self Caring) and Call Center Operators.

Some of the available information such as: incoming and outgoing calls, personal information or credit cards details are ruled by privacy policies.

Obviously WS-A and all its operations are accessible by C1, but information provided as result or specific details depend on the original requester: a Customer could have full access on all information and details available on its profile while a Call Center Operator could be granted to view only a subset such data (i.e. partial call numbers, filtered credit cards details, etc.).

In the following scenarios C1 invokes WS-A for retrieving the list of incoming call numbers for specific customers:

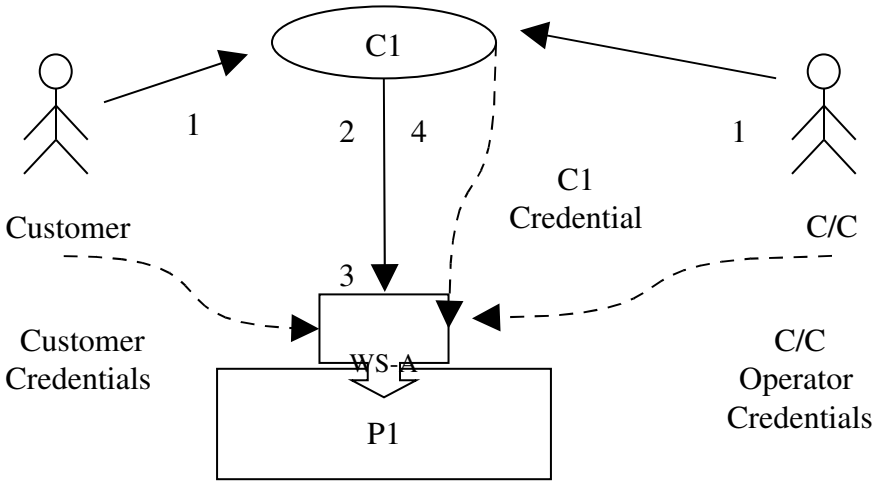


Figure 1: User ID Forwarding – “Customer care” use case

Scenario 1 (Operator’s Customers)

- A Customer accesses C1 to view the list of outcoming calls by using his Credentials.
- C1 invokes a Web Service (WS-A) exposed by P1 passing the Customer's credentials in a SAML Assertion, the subject of the SAML assertion is C1.
- WS-A handles the invocation message and apply the security policies: in particular it verifies if C1 is authenticated & authorized to access the WS-A using the C1 credentials.
- P1 (Provider) runs the business logic.
- WS-A receives the result from P1 and applies all the privacy policies in order to then return the data to C1, in particular using the other credentials (the user credentials) verifies that the user can read the entire results, so returns it to C1.
- C1 shows the entire results to Customers such as:
  03/27/09 11:39 3355799553 05:37
  03/27/09 12:03 3359955125 10:57.

Scenario 2 (Call Center Operator)

- A Call Center Operator accesses to view the list of incoming call numbers for a specific customer by using his Credentials.
- C1 invokes WS-A passing his credentials and the Operator's credentials in a SAML Assertion, the subject of the SAML assertion is C1.
- WS-A handles the invocation message and apply the security policies: in particular it verifies if C1 is authenticated & authorized to access the WS-A using the C1 credentials.
- P1 (Provider) runs the business logic.
- WS-A receives the result from P1 and applies all the privacy policies in order to then return the data to C1, in particular using the other credentials (the user credentials) verifies that the user can read only a part of the data, so returns it to C1 only this part. In particular only the first part of the phone number.
- C1 shows the results obtained from WS-A to C/C Operator such as:
  03/27/09 11:39 3355799XXX 05:37
  03/27/09 12:03 3359955XXX 10:57

Appendix A. Acknowledgments

The editor would like to acknowledge the contributions of the OASIS Security Services (SAML) Technical Committee, whose voting members at the time of publication were:

•TBD

Appendix A. Revision History

Document ID	Date	Committer	Comment