SAML V2.0 Profile for Token Correlation

Committee Draft 01

28 June 2010

Specification URIs:

This Version:

XXXXXX

Previous Version:

N/A

Latest Version:

Technical Committee:

OASIS Security Services TC

Chair(s):

Thomas Hardjono, MIT

Nate Klingenstein, Internet2

Editor(s):

Federico Rossini, Telecom Italia

Enrico Ronco, Telecom Italia

Declared XML Namespace(s):

`urn:oasis:names:tc:SAML:2.0:cm:token correlation profile`

Abstract:

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

This document defines the syntax to express a relation between two SAML assertion, a “main” one and a “related” one.

Status:

This is initial draft of Subject Management Protocol based on [*to add the quotation*]

Technical Committee members should send comments on this specification to the Technical Committee’s email list. Others should send comments to the Technical Committee by using the

"Send A Comment" button on the Technical Committee's web page at http://www.oasis-open.org/committeees/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 Intellectual Property Rights section of the Technical Committee 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 names "OASIS", [insert specific trademarked names, abbreviations, etc. here] are trademarks 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

In some advanced SAML use cases, in enterprise context, the execution of a business process might involve two or more logical transactions that span across one or more intermediaries.

Suppose that an intermediary is involved in almost every process and it needs to call the same services for different processes, if the authorization to call the services is granted to the intermediary without correlating this authorization to the process in execution, that would mean to authorize the intermediary to call every services, as a consequence there wouldn't be real security policy criteria and there would be reduced logging information.

This profile supply a normative extension to the [SAML2Core] in accord to the philosophy that every actor owns only the authorizations strictly necessary to do what it needs to do.

1.1 Terminology

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 IETF RFC 2119 [RFC 2119].

1.2 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

2 SAML V2.0 Token Correlation

2.1 Required Information

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

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

Description: Given below.

Updates: None.

2.2 Description

This token correlation requirement extends the message security models and enforces the security mechanism in environments where the message exchange pattern is more complex than the simple “requestor – provider” pattern.

This model should be useful when the definition and the use of a “simple” token doesn’t guarantee a sufficient level of security, since the authorization to access a specific service also depends on the fact that a previous token was released.

The syntax defined in this profile defines a new security profile, in which a SAML assertion is syntactically and semantically meaningful if it is built and presented in relation with another “related” SAML assertion; it enables to express a relation between two security SAML assertions, a “main” SAML and a “related” SAML.

The characteristics of the relation are that, when the token correlation is used,

1. the SAML assertion cannot be built and considered valid if it isn't presented together with another “related” SAML assertion,
2. The authorization is granted only in presence of both the subjects of the two SAML assertions.

2.3 Element <token-correlation>

The optional <Token-correlation> element of the section condition specifies the subject of the correlated SAML assertion; it contains an identifier.

<BaseID>, <NameID>, or <EncryptedID>[optiona].

The following schema fragment defines the <Token-correlation> element and its TokenCorrelationType complex type:

```
<element name="Token-correlation" type="saml:TokenCorrelationType"/>
  <complexType name="TokenCorrelationType">
    <choice>
        <element ref="saml:BaseID"/>
        <element ref="saml:NameID"/>
        <element ref="saml:EncryptedID"/>
    </choice>
  </complexType>
```

The element <Token-correlation>, if present, implies that a <Token-correlated> element must be present.

2.4 Element <Token-correlated>

The element <token-correlated>, contains a SAML assertion.

How can I express the type?

If the SAML authority signs the assertion, this element can be out of the assertion (it should be inserted by the SAML subject).

Where can I put the correlate SAML, in order that, if the SAML authority signs the assertion, the signature is not invalidated by putting the SAML correlated?

Processing roules

Assume the main SAML: *SAML2* and the correlated one: *SAML1*.

The requestor (that can obtain only token-correlated SAML for a specific service invocation)

- asks to the SAML authority for a SAML (SAML2); the SAML is of “token correlation” kind, it contains the condition <token-correlation>;
- after having obtained the assertion, the requestor inserts the correlated SAML (SAML1);
- the SAML1 subject ID is equal to the SAML2 token-correlation ID;
- after the other actions, such as signing, are performed, the message is sent to the service provider.

If **the service provider**, during the exam of the main SAML assertion (SAML2) finds the condition <token-correlation>, it searches for the correlated SAML (SAML1) in the message;

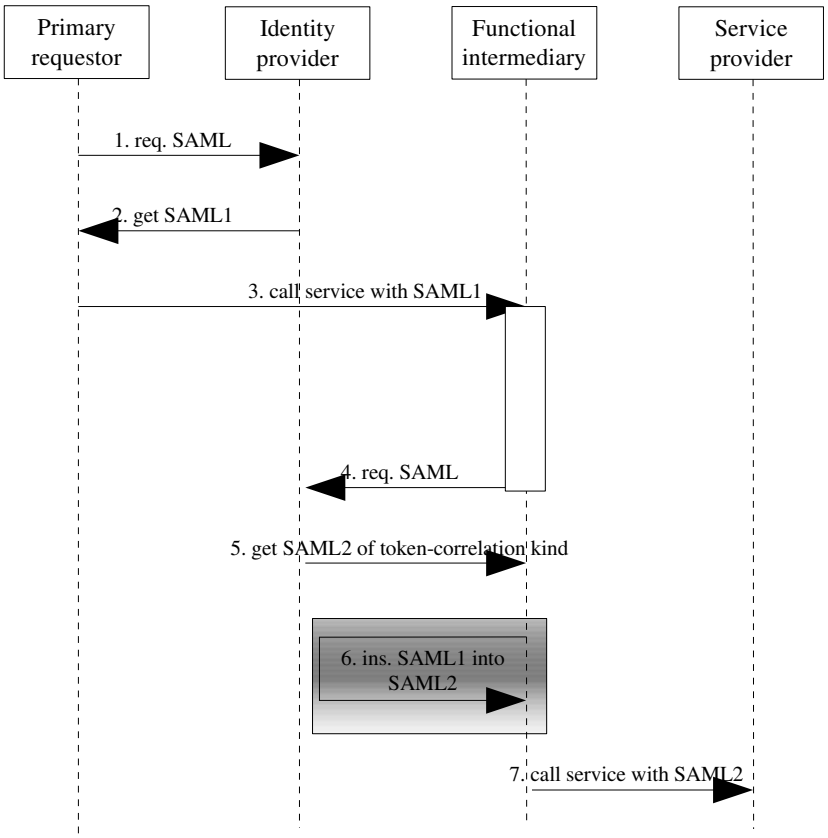
The authorization is granted if

- SAML1 is present and is authentic (released by a trusted SAML authority),

- the SAML1 subject ID is equal to the SAML2 token-correlation ID;
- all the other SAML2 conditions are verified, in accord to the SAML2 standard protocol.

Usually when <token-correlation> condition is present, the authorization should be granted to SAML2 subject only in presence of the SAML1 subject (i.e. token-correlation element).

SAML1 condition elements (for example < NotOnOrAfter>, <OneTimeUse>) could not be true any more.



3 Conformance

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Appendix A. Uses cases

Scenario/context

The business process under analysis is complex and necessitates to be orchestrated by a BPM (Business Process Management) application.

Such process is a “long-running” type process: in fact one of its tasks requires a human intervention, which can be executed within hours (or days).

This implies that the process must be handled in a different mode from the “security management” perspective.

Use case

The issue presented in this section derives from a concrete case of telecommunications services’ sales and post-sales: in particular the activation and provisioning of ADSL service to residential customers.

A consumer, e.g. a CRM application invokes a service to execute a specific business process.

A BPM (Business Process Management) application gets in charge of the orchestration/execution of such processes.

Given the fact that the process is “long-running”, the BPM shall, at a given point, suspend the orchestration/execution of the process until it will receive a specific “activity closure” event from a back office system once the appropriate technician will have terminated his manual tasks.

The following schema Figure 1 depicts a simplified transaction diagram, while Figure 2 provides a pictorial representation of the Use Case.

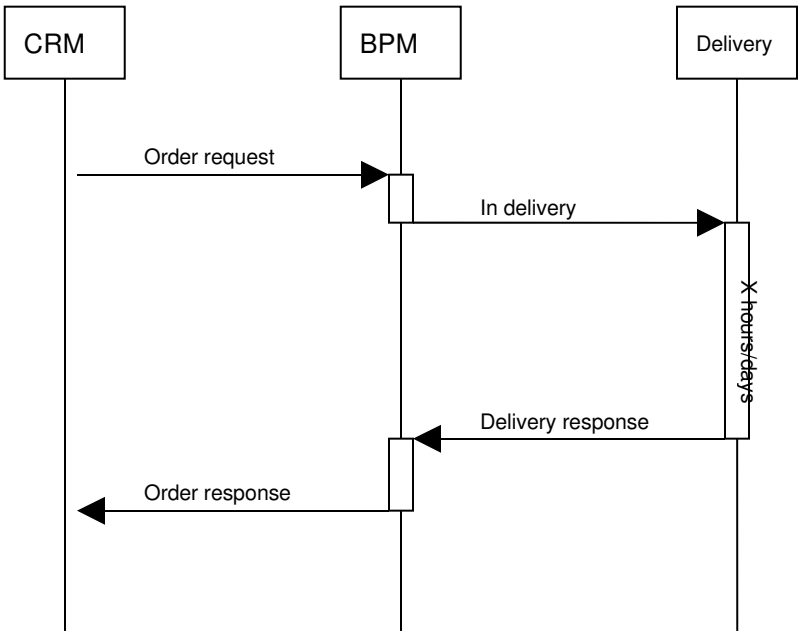


Figure 1: Simplified transaction diagram for the "SAML token correlation" use case

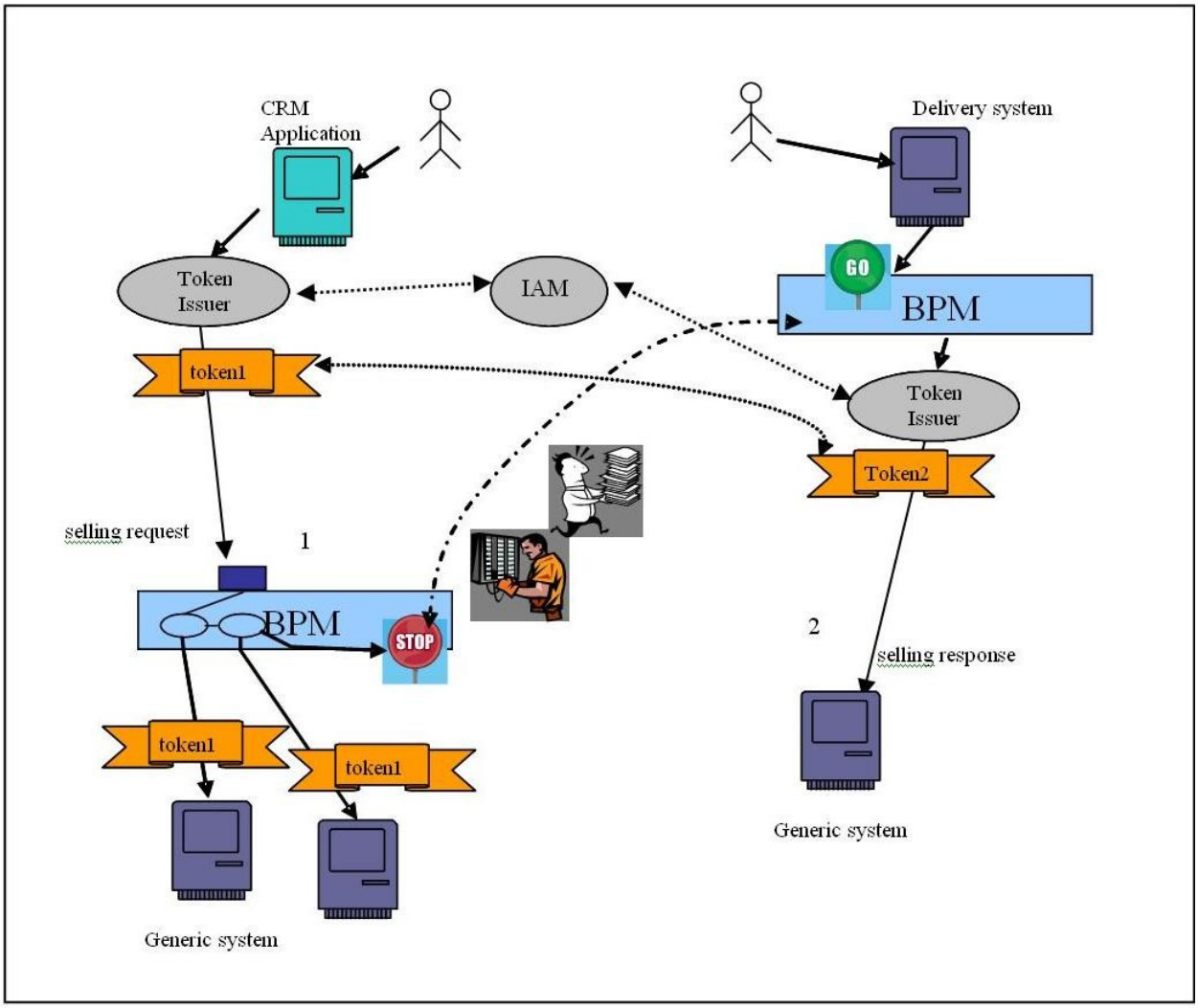


Figure 2: "SAML token correlation" use case: pictorial representation

Use Case steps.

- The CRM sends an ADSL activation request.
- The consumer (CRM) provides its credentials to a Security provider and obtains a SAML assertion, *"SAML1"*. The SAML assertion is associated to the initial message and has limited duration, since extending it would mean to have a weaker security policy.
- The BPM Security Enforcement Point, interacting with the policy decision point (IAM) (Identity Access Manager) applies the authentication and authorization policies.
- The BPM orchestrates the process interacting with the various services exposed by the involved systems within the company infrastructure. All interactions are executed with the *"SAML1"* as security token.
- When appropriate, the BPM invokes a service exposed by a Delivery system to obtain a physical configuration within the central office. At this stage the BPM suspends the execution of the business process (the duration of the task may require hours or days) awaiting for the reception of a specific "activity closure" event.

- The Delivery System activates the technical configuration task.
- A human intervention is performed within the central office.
- Once this task is terminated, the technician reports the “activity closure” on the Delivery system, which generates the “activity closure” event for the BPM.
- The BPM resumes the suspended process, invoking the “next step” in the ADSL activation process.
- The BPM requests the security provider to generate a new SAML, *“SAML2”*, since the previous is not valid any more.
- The remaining portion of the process is executed utilizing SAML2.

The BPM is responsible for the orchestration/execution of the process, and is the entity which is entitled to request the generation of the new SAML *“SAML2”*, so the subject of SAML2 is different from the system that started the process.

It is important for the “security architecture”, that an element of the middleware infrastructure (the BPM) use SAML assertions which are “correlated” (or “directly coupled”) to the real entity which requires the initiation of the business process (i.e. the CRM application, thus the CRM sales representative) and to the business process itself.

It enforces the security level that the BPM requests to the SAML Issuer to generate a SAML assertion “associated” to the *“SAML1”,* and to maintains evidence of that correlation, in order to authorize the BPM itself, once security checks are validated by the IAM, to invoke all pending services within the second part of the process, because such invocations are “really” part of a “security authorized” business process.

Appendix B. Acknowledgments

The following individuals have participated in the creation of this specification and are gratefully acknowledged

Participants:

- [Participant name, affiliation | Individual member]
- [Participant name, affiliation | Individual member]
- [Participant name, affiliation | Individual member]

Appendix A. Revision History

Document ID	Date	Committer	Comment