SAML V2.0 Kerberos Subject Confirmation Method Version 1.0

Committee Draft 01

15 December 2009

Specification URIs:

This Version:

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-kerberos-subject-confirmation-method-cd-01.html

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-kerberos-subject-confirmation-method-cd-01.odt (Authoritative)

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-kerberos-subject-confirmation-method-cd-01.pdf

Previous Version:

N/A

Latest Version:

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-kerberos-subject-confirmation-method.html

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-kerberos-subject-confirmation-method.odt

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-kerberos-subject-confirmation-method.pdf

Technical Committee:

OASIS Security Services TC

Chair(s):

Hal Lockhart, Oracle, Inc.

Thomas Hardjono, MIT

Editor(s):

Josh Howlett, Individual

Thomas Hardjono, MIT

Declared XML Namespace(s):

`urn:oasis:names:tc:SAML:2.0:cm:kerberos`

Abstract:

This document defines a subject confirmation method for use with the Kerberos protocol.

Status:

This document was last revised or approved by the SSTC on the above date. The level of approval is also listed above. Check the "Latest Version" or "Latest Approved Version" location noted above for possible later revisions of this document.

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

The *SAML V2.0 Assertions and Protocols* specification defines the `<SubjectConfirmation>` element which can provide evidence that, when applied to a process known as a Method, may be used by a relying party to confirm that the message came from a system entity that is associated with the subject of an assertion. This specification defines a new subject confirmation method that uses evidence provided by the Kerberos protocol.

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

[RFC 2119] S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

[RFC 4120] C. Neuman et al. *The Kerberos Network Authentication Service (V5)*. IETF RFC 4120, July 2005. http://www.ietf.org/rfc/rfc4120.txt.

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

2 SAML V2.0 Kerberos Subject Confirmation Method

URI: urn:oasis:names:tc:SAML:2.0:cm:kerberos

The `<KerberosData>` element from the XML namespace `urn:oasis:names:tc:SAML:2.0:attribute:kerberos` MUST be present within the `<SubjectConfirmationData>` element. This element MUST contain a single instance of either the `<KerberosCname>` or the `<KerberosSname>` element. This elements MUST name the Kerberos [RFC 4120] user or service principal that is considered to be the subject of the assertion by the asserting party, subject to optional constraints on confirmation using the attributes that MAY be present in the `<SubjectConfirmationData>` element, as defined by [SAML2Core].

Example: The Kerberos user principal named "joe@EXAMPLE.ORG" can confirm itself as the subject.

```
<SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:kerberos">
   <SubjectConfirmationData>
      <KerberosData>
         <KerberosCname>
            joe@EXAMPLE.ORG
         </KerberosCname>
      </KerberosData>
   </SubjectConfirmationData>
</SubjectConfirmation>
```

3 Conformance

An asserting party implementation conforms to this profile if it can produce assertions and other SAML-defined content consistent with the normative text of section 2.

A relying party implementation conforms to this profile if it can accept assertions and other SAML-defined content consistent with the normative text of section 2.

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:

- John Bradley, Individual
- Scott Cantor, Internet2
- Duane DeCouteau, Veterans Health Administration
- Christian Guenther, Nokia Siemens Networks GmbH & Co.
- Frederick Hirsch, Nokia Corporation
- Ari Kermaier, Oracle Corporation
- Nathan Klingenstein, Internet2
- Hal Lockhart, Oracle Corporation
- Paul Madsen, NTT Corporation
- Kyle Meadors, Drummond Group Inc.
- Bob Morgan, Internet2
- Thinh Nguyenphu, Nokia Siemens Networks GmbH & Co.
- Rob Philpott, EMC Corporation
- Anil Saldhana, Red Hat
- Tom Scavo, National Center for Supercomputing Applications
- Kent Spaulding, Skyworth TTG Holdings Limited
- David Staggs, Veterans Health Administration
- Emily Xu, Sun Microsystems

The editor would also like to acknowledge the following particular individuals who contributed to the development of this document:

- Scott Cantor, Internet2
- Nathan Klingenstein, Internet2
- Tom Scavo, National Center for Supercomputing Applications
- Jeff Hodges, PayPal

Appendix B. Revision History

Document ID	Date	Committer	Comment
sstc-saml-kerberos-subject-confirmation-method-00	3 Sep 2009	J. Howlett	Initial draft
sstc-saml-attribute-kerberos-cd-01	18 Nov 2009	J. Howlett	Committee Draft 01