SAML V2.0 Kerberos Attribute Profile Version 1.0

Committee Specification Draft 02

14 December 2010

Specification URIs:

This Version:

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-kerberos-csd02.html

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-kerberos-csd02.odt (Authoritative)

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-kerberos-csd02.pdf

Previous Version:

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

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

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

Latest Version:

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

http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-kerberos.odt (Authoritative)

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

Technical Committee:

OASIS Security Services (SAML) TC

Chair(s):

Thomas Hardjono, MIT

Nate Klingenstein, Internet2

Editor(s):

Josh Howlett, Individual

Thomas Hardjono, MIT

Declared XML Namespace(s):

`urn:oasis:names:tc:SAML:2.0:profiles:attribute:kerberos`

Abstract:

This specification defines an attribute profile for the Kerberos protocol.

Copyright © OASIS® 2010. All Rights Reserved.

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" 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/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 Intellectual Property Rights section of the Technical Committee web page (http://www.oasis-open.org/committees/security/ipr.php).

Citation Format:

When referencing this specification the following citation format should be used:

sstc-saml-attribute-kerberos OASIS Committee Specification Draft 02, *SAML V2.0 Kerberos Attribute Profile Version 1.0*, December 2010. http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-attribute-kerberos-csd02.odt

Copyright © OASIS® 2010. All Rights Reserved.

Notices

Copyright © OASIS® 2010. All Rights Reserved.

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 5
1.1 Terminology 5
1.2 Normative References 5
1.3 Non-Normative References 5
2 SAML 2.0 Kerberos Attribute Profile 6
2.1 Required Information 6
2.2 Profile Overview 6
2.3 SAML Attribute Naming 6
2.3.1 Attribute Name Comparison 6
2.4 Profile-Specific XML Attributes 6
2.5 SAML Attribute Values 6
2.6 Kerberos Principal Naming 6
2.7 Attribute Definition 7
2.8 Examples 7
3 Conformance 9
3.1 SAML 2.0 Kerberos Attribute Profile 9

Copyright © OASIS® 2010. All Rights Reserved.

1 Introduction

The SAML V2.0 Kerberos Attribute Profile describes a SAML attribute profile for requesting and expressing Kerberos protocol messages.

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 RFC2119.

The term *TLS* as used in this specification refers to either the Secure Sockets Layer (SSL) Protocol 3.0 [SSL3] or any version of the Transport Layer Security (TLS) Protocol [RFC2246] [RFC4346] [RFC5256]. As used in this specification, the term TLS specifically does not refer to the SSL Protocol 2.0 [SSL2].

1.2 Normative References

[NonEncKrb] R. Yount. *The Unencrypted Form Of Kerberos 5 KRB-CRED Message*. IETF Internet-Draft, December 2010. See http://tools.ietf.org/id/draft-yount-krb-cred-clear-text-01.txt

[RFC2045] N. Freed et al. *Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies,* November 1996*. See* http://www.ietf.org/rfc/rfc2045.txt

[RFC2119] S. Bradner. *Key words for use in RFCs to Indicate Requirement Levels*. IETF RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt

[RFC2246] T. Dierks, C. Allen. *The TLS Protocol Version 1.0*. IETF RFC 2246, January 1999. http://www.ietf.org/rfc/rfc2246.txt

[RFC4120] C. Neuman et al. *The Kerberos Network Authentication Service (V5)*. IETF RFC 4120, July 2005. http://www.ietf.org/rfc/rfc4120.txt

[RFC4346] T. Dierks, E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.1*. IETF RFC 4346, April 2006. http://www.ietf.org/rfc/rfc4346.txt

[RFC3061] M. Mealling. *A URN Namespace of Object Identifiers*. IETF RFC 3061, February 2001. http://www.ietf.org/rfc/rfc3061.txt

[Kerberos-XSD] J. Howlett et al., Kerberos schema. OASIS SSTC, November 2009. Document ID saml-schema-kerberos-2.0. See http://www.oasis-open.org/committees/download.php/35334/saml-schema-kerberos-2.0

[RFC5256] T. Dierks, E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.2*. IETF RFC 5246, August 2008. http://www.ietf.org/rfc/rfc5246.txt

[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

[SSL3] A. Freier, P. Karlton, P. Kocher. *The SSL Protocol Version 3.0*. Netscape Communications Corp., November 18, 1996. http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt

1.3 Non-Normative References

[SSL2] K. Hickman. *The SSL Protocol*. Netscape Communications Corp., February 9, 1995. http://www.mozilla.org/projects/security/pki/nss/ssl/draft02.html

Copyright © OASIS® 2010. All Rights Reserved. Standards Track Work Product

2 SAML 2.0 Kerberos Attribute Profile

2.1 Required Information

Identification: `urn:oasis:names:tc:SAML:2.0:profiles:attribute:kerberos`

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

Description: Given below.

Updates: None.

2.2 Profile Overview

This specification describes a SAML attribute profile that can be used to request and express Kerberos protocol messages. In this version of the specification, this is constrained to the Kerberos KRB-CRED message type. The mechanisms that are used to generate the Kerberos message are outside the scope of this document and are described by [RFC4120].

2.3 SAML Attribute Naming

The `NameFormat` XML attribute in `<Attribute>` elements MUST be `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.

2.3.1 Attribute Name Comparison

Two `<Attribute>` elements refer to the same SAML attribute if and only if their `Name` XML attribute values are equivalent in the sense of [RFC3061]. The `FriendlyName` attribute plays no role in the comparison.

2.4 Profile-Specific XML Attributes

No additional XML attributes are defined for use with the `<Attribute>` element.

2.5 SAML Attribute Values

The value of this attribute is a Kerberos message that is expressed using the `<KerberosData>` element defined in the XML namespace `urn:oasis:names:tc:SAML:2.0:attribute:kerberos`.

When comparing attribute values for equality, an attribute value which does not contain a `<KerberosMessage>` element MUST be considered equivalent to any other value. This rule is necessary to satisfy the equality condition stipulated in section 3.3.2.3 of [SAML2Core], in the case where the attribute is used within the `<AttributeQuery>` element.

2.6 Kerberos Principal Naming

The naming of Kerberos principals MUST adhere to the rules specified in section 2.1 of [RFC1964].

Copyright © OASIS® 2010. All Rights Reserved.

2.7 Attribute Definition

This profile currently defines a single multi-valued attribute named “krb-cred”.

Name: urn:oasis:names:tc:SAML:2.0:profiles:attribute:kerberos:krb-cred

An `<AttributeValue>` element MUST contain a single `<KerberosData>` element from the XML namespace `urn:oasis:names:tc:SAML:2.0:attribute:kerberos`. For purposes of human readability, there may also be a requirement for some applications to carry an optional string name together with the URI. The optional XML attribute `FriendlyName` (defined in [SAML2Core]) MAY be used for this purpose.

When used to request a Kerberos KRB-CRED message, this element MUST include a single instance of the `<KerberosSname>` element and MAY include at most a single instance of the `<KerberosCname>` element, naming the intended service and client principals respectively.

When used to express a Kerberos KRB-CRED message, this element MUST include single instances of the `<KerberosSname>` and `<KerberosCame>` elements naming the service and client principals identified in the KRB-CRED message and a single instance of the `<KerberosMessage>` element whose value takes the base64-encoded [RFC2045] representation of the KRB-CRED message and whose `KerberosMsgType` attribute MUST take a value of “KRB_CRED”.

The issuer SHOULD attempt to satisfy the client principal named by the requester, if given, but MAY use any other client principal (for example, if a local policy forbids or requires a particular client principal for a service).

The KRB-CRED message issued in a `<KerberosMessage>` element MUST conform to section 5.8 of [RFC4120].

The KRB-CRED message contains sensitive information related to Kerberos credentials being transferred, such as their secret session keys, client and server principal names, and validity period. Posession of this information, along with the ticket itself, would allow an attacker to impersonate the client named in the ticket. As a result, this information must be carefully safeguarded.

The definition of the KRB-CRED message in section 5.8 of [RFC4120] provides for protection of the confidentiality and integrity of the sensitive portions of the KRB-CRED message when it is passed in the context of a previous Kerberos authentication, by encrypting those portions in a key derived from the shared Kerberos session key. When the issuer and recipient of this attribute share an appropriate Kerberos authentication context, it SHOULD be used to protect the KRB-CRED message as described in [RFC4120].

However, the issuer and recipient of a SAML attribute often do not share an Kerberos authentication context. To facilitate use of this attribute in such cases, the non-encrypted form of the KRB-CRED message [NonEncKrb] may be used. When the non-encrypted form is used, the confidentiality and integrity of the message MUST be protected by alternate means such as Transport Layer Security (TLS) or the `<EncryptedAttribute>` element.

To facilitate interoperability, implementations of this profile MUST support sending and receiving the non-encrypted form of the KRB-CRED message, and MUST support protection of this attribute by use of the `<EncryptedAttribute>` element.

2.8 Examples

A SAML requester issues a request to a SAML attribute authority for a Kerberos KRB-CRED message:

```
<saml:Attribute
        xmlns:kerberos="urn:oasis:names:tc:SAML:2.0:attribute:kerberos"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
```


Copyright © OASIS® 2010. All Rights Reserved. Standards Track Work Product

```
        Name="urn:oasis:names:tc:SAML:2.0:profiles:attribute:kerberos:krb-
cred">
   <saml:AttributeValue>
      <kerberos:KerberosData>
         <kerberos:KerberosCname>
            joe@EXAMPLE.ORG
         </kerberos:KerberosCname>
         <kerberos:KerberosSname>
            http/www@EXAMPLE.ORG
         </kerberos:KerberosSname>
      </kerberos:KerberosData>
   </saml:AttributeValue>
</saml:Attribute>
```

A SAML attribute authority returns a Kerberos KRB-CRED message:

```
<saml:Attribute
        xmlns:kerberos="urn:oasis:names:tc:SAML:2.0:attribute:kerberos"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="urn:oasis:names:tc:SAML:2.0:profiles:attribute:kerberos:krb-
cred"
   <saml:AttributeValue>
      <kerberos:KerberosData>
         <kerberos:KerberosCname>
            joe@EXAMPLE.ORG
         </kerberos:KerberosCname>
         <kerberos:KerberosSname>
            http/www@EXAMPLE.ORG
         </kerberos:KerberosSname>
         <kerberos:KerberosMessage KerberosMsgType=”KRB_CRED”>
            ...base64 representation of a KRB-CRED message...
         </kerberos:Message>
      </kerberos:KerberosData>
   </saml:AttributeValue>
</saml:Attribute>
```


Copyright © OASIS® 2010. All Rights Reserved. Standards Track Work Product

3 Conformance

3.1 SAML 2.0 Kerberos Attribute Profile

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 .

Copyright © OASIS® 2010. All Rights Reserved.

Appendix A. Acknowledgments

The editor would like to acknowledge the contributions of the OASIS Security Services (SAML) Technical Committee:

- 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:

- Russell Yount, CMU
- Jeffrey Hutzelman, CMU
- Scott Cantor, Internet2
- Nathan Klingenstein, Internet2
- Tom Scavo, National Center for Supercomputing Applications
- Jeff Hodges, PayPal

Copyright © OASIS® 2010. All Rights Reserved.

Appendix B. Revision History

Document ID	Date	Committer	Comment
sstc-saml-attribute-kerberos-draft-01	7 Aug 2009	J. Howlett	Initial draft
sstc-saml-attribute-kerberos-draft-02	3 Sep 2009	J. Howlett	Response to comments
sstc-saml-attribute-kerberos-cd-01	18 Nov 2009	J. Howlett	Committee Draft 01
sstc-saml-attribute-kerberos-draft-03	24 Sep 2010	J. Howlett	Response to comments
sstc-saml-attribute-kerberos-draft-04	3 Dec 2010	J. Howlett	Response to comments

Copyright © OASIS® 2010. All Rights Reserved. Standards Track Work Product