



XMPP

XEP-0233: Domain-Based Service Names in XMPP SASL Negotiation

Matthew Miller

<mailto:linuxwolf@outer-planes.net>

<xmpp:linuxwolf@outer-planes.net>

Peter Saint-Andre

<mailto:stpeter@jabber.org>

<xmpp:stpeter@jabber.org>

<https://stpeter.im/>

Joe Hildebrand

<mailto:jhildebr@cisco.com>

<xmpp:hildjj@jabber.org>

2011-08-26

Version 0.4

Status	Type	Short Name
Experimental	Standards Track	NOT YET ASSIGNED

This specification defines a method by a connecting client can learn the domain-based service name of a Kerberos acceptor principal for SASL authentication using the GSSAPI mechanism.

Legal

Copyright

This XMPP Extension Protocol is copyright © 1999 - 2011 by the [XMPP Standards Foundation](#) (XSF).

Permissions

Permission is hereby granted, free of charge, to any person obtaining a copy of this specification (the "Specification"), to make use of the Specification without restriction, including without limitation the rights to implement the Specification in a software program, deploy the Specification in a network service, and copy, modify, merge, publish, translate, distribute, sublicense, or sell copies of the Specification, and to permit persons to whom the Specification is furnished to do so, subject to the condition that the foregoing copyright notice and this permission notice shall be included in all copies or substantial portions of the Specification. Unless separate permission is granted, modified works that are redistributed shall not contain misleading information regarding the authors, title, number, or publisher of the Specification, and shall not claim endorsement of the modified works by the authors, any organization or project to which the authors belong, or the XMPP Standards Foundation.

Warranty

NOTE WELL: This Specification is provided on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE.

Liability

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall the XMPP Standards Foundation or any author of this Specification be liable for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising from, out of, or in connection with the Specification or the implementation, deployment, or other use of the Specification (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if the XMPP Standards Foundation or such author has been advised of the possibility of such damages.

Conformance

This XMPP Extension Protocol has been contributed in full conformance with the XSF's Intellectual Property Rights Policy (a copy of which can be found at <http://xmpp.org/about-xmpp/xsf/xsf-ipr-policy/> or obtained by writing to XMPP Standards Foundation, 1899 Wynkoop Street, Suite 600, Denver, CO 80202 USA).

Contents

1	Introduction	1
2	Protocol	1
3	Security Considerations	2
4	IANA Considerations	2
5	XMPP Registrar Considerations	2
5.1	Protocol Namespaces	2
5.2	Protocol Versioning	3
6	XML Schema	3
7	Acknowledgements	3

1 Introduction

In environments that make use of Kerberos V5 ([RFC 4120](http://tools.ietf.org/html/rfc4120)¹) and negotiation of Simple Authentication and Security Layer or SASL ([RFC 4422](http://tools.ietf.org/html/rfc4422)²) over XMPP, a connecting client often needs to know the identity of the Kerberos acceptor principal so that it can obtain a proper ticket for authentication. This scenario was not addressed in [RFC 3920](http://tools.ietf.org/html/rfc3920)³ or [RFC 6120](http://tools.ietf.org/html/rfc6120)⁴. However, the problem can be solved using the concept of domain-based service names ([RFC 5178](http://tools.ietf.org/html/rfc5178)⁵). In particular, when an XMPP server uses the Kerberos V5 ("GSSAPI") SASL mechanism ([RFC 4752](http://tools.ietf.org/html/rfc4752)⁶), it can communicate the identity of the acceptor principal as a Kerberos V5 service principal name ([RFC 5179](http://tools.ietf.org/html/rfc5179)⁷). This document defines an XMPP method for such communication.

2 Protocol

The acceptor principal's hostname is communicated by including a child element of the <mechanisms/> element during SASL negotiation, as allowed by RFC 6120 (see Section 6.3.5 and the schema for the 'urn:ietf:params:xml:ns:xmpp-sasl' namespace in Appendix A.4). In the case of the Kerberos V5 SASL mechanism, the child element is a <hostname/> element qualified by the 'urn:xmpp:domain-based-name:1' namespace (see [Protocol Namespaces](#) regarding issuance of one or more permanent namespaces). The XML character data of the <hostname/> element specifies the fully-qualified name of the acceptor principal. The client then generates a domain-based service name from the provided hostname, following the format specified in RFC 5179 (i.e., "protocol/hostname/domainname@REALM") and setting the values as follows:

- The protocol string MUST be "xmpp".
- The hostname string MUST be the XML character data of the <hostname/> element.
- The domainname string MUST be the canonical name of the service, such as typically communicated in the 'to' address of the initial stream header.
- The REALM string SHOULD be determined according to the network policies in effect (usually the domain name, in an uppercase mapping).

¹RFC 4120: The Kerberos Network Authentication Service (V5) <<http://tools.ietf.org/html/rfc4120>>.

²RFC 4422: Simple Authentication and Security Layer (SASL) <<http://tools.ietf.org/html/rfc4422>>.

³RFC 3920: Extensible Messaging and Presence Protocol (XMPP): Core <<http://tools.ietf.org/html/rfc3920>>.

⁴RFC 6120: Extensible Messaging and Presence Protocol (XMPP): Core <<http://tools.ietf.org/html/rfc6120>>.

⁵RFC 5178: Generic Security Service Application Program Interface (GSS-API) Internationalization and Domain-Based Service Names and Name Type <<http://tools.ietf.org/html/rfc5178>>.

⁶RFC 4752: The Kerberos V5 ("GSSAPI") Simple Authentication and Security Layer (SASL) Mechanism <<http://tools.ietf.org/html/rfc4752>>.

⁷RFC 5179: Generic Security Service Application Program Interface (GSS-API) Domain-Based Service Names Mapping for the Kerberos V GSS Mechanism <<http://tools.ietf.org/html/rfc5179>>.

Consider the example of an XMPP service whose canonical name is "example.com". A user might make use of an acceptor principal located at "auth42.us.example.com". The hostname would be communicated as follows.

Listing 1: Communicating the hostname

```
<mechanisms xmlns='urn:ietf:params:xml:ns:xmpp-sasl'>
  <mechanism>GSSAPI</mechanism>
  <mechanism>DIGEST-MD5</mechanism>
  <hostname xmlns='urn:xmpp:domain-based-name:1'>auth42.us.example.com
    </hostname>
</mechanisms>
```

The client would then attempt to obtain a ticket for the domain-based principal "xmpp-auth42.us.example.com/example.com@EXAMPLE.COM".

3 Security Considerations

The communication of acceptor principal hostname during SASL negotiation is not known to introduce new security vulnerabilities, as long as it is done after the underlying channel has been secured using Transport Layer Security (TLS; [RFC 5246](#)⁸) as described for XMPP in RFC 6120. For additional security considerations, refer to RFC5178 and RFC 5179.

4 IANA Considerations

This document requires no interaction with the [Internet Assigned Numbers Authority \(IANA\)](#)⁹.

5 XMPP Registrar Considerations

5.1 Protocol Namespaces

This specification defines the following XML namespace:

- urn:xmpp:domain-based-name:1

⁸RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2 <<http://tools.ietf.org/html/rfc5246>>.

⁹The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols, such as port numbers and URI schemes. For further information, see <<http://www.iana.org/>>.

Upon advancement of this specification from a status of Experimental to a status of Draft, the XMPP Registrar ¹⁰ shall add the foregoing namespace to the registry located at <http://xmpp.org/registrar/namespaces.html>, as described in Section 4 of XMPP Registrar Function ¹¹.

5.2 Protocol Versioning

If the protocol defined in this specification undergoes a revision that is not fully backwards-compatible with an older version, the XMPP Registrar shall increment the protocol version number found at the end of the XML namespaces defined herein, as described in Section 4 of XEP-0053.

6 XML Schema

```
<?xml version='1.0' encoding='UTF-8'?>
<xs:schema
  xmlns:xs='http://www.w3.org/2001/XMLSchema'
  targetNamespace='urn:xmpp:domain-based-name:1'
  xmlns='urn:xmpp:domain-based-name:1'
  elementFormDefault='qualified'>
  <xs:element name='hostname' type='xs:string' />
</xs:schema>
```

7 Acknowledgements

Thanks to Owen Friel, Shane Hannon, Seamus Kerrigan, Eliot Lear, Alexey Melnikov, and Klaas Wierenga for their comments.

¹⁰The XMPP Registrar maintains a list of reserved protocol namespaces as well as registries of parameters used in the context of XMPP extension protocols approved by the XMPP Standards Foundation. For further information, see <http://xmpp.org/registrar/>.

¹¹XEP-0053: XMPP Registrar Function <http://xmpp.org/extensions/xep-0053.html>.