Domain Authorization for PIDF-LO
draft-thomson-domain-auth-01.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress".

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire in December 2005.

Copyright Notice

Copyright (C) The Internet Society (2005). All Rights Reserved.

Abstract

This document describes a standard method for digitally signing Presence Information Data Format Location Object (PIDF-LO) documents using a subset of the XML Digital Signature specification. A digital signature enables the user of a signed PIDF-LO document to attribute that information to an authorized source within the domain of the target entity. A schema is defined for including a domain authorization element in the PIDF-LO and a set of XML Path Language (XPath) filters for selecting the correct elements for signing.
Table of Contents
1 Introduction

Users of location information may desire to be able to attribute this information to an authorized entity. This entity may not have provided the information, but they must be able to vouch for its accuracy. In most cases this will mean that the trusted entity resides within the same domain, or access network, as the target entity.

This specification describes a means by which a domain authority may assume responsibility for the validity of the location information provided in a Presence Information Data Format Location Object (PIDF-LO [I-D.ietf-geopriv-pidf-lo]). A standard form is described whereby a domain authority may digitally sign the PIDF-LO document. This signature ensures that a user of the PIDF-LO can verify that the presentity identified is at the described location within certain time bounds.

Only selected data are signed within a PIDF, allowing a user freedom to change other parts of the document without affecting the signature. A signature only applies to a single tuple element, allowing separate tuples to be unsigned, or to be signed separately. Elements such as notes, contact information and the privacy preferences described in [I-D.ietf-geopriv-pidf-lo] are not signed to allow for modification. The signed elements are restricted to:

the presentity identifier: the entity attribute of the presence element.
timestamp: the timestamp associated with the location information
location-info: the actual location information
expires: the time at which the signature expires, this datum is added by this specification

1.1 Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

The term presentity is used as defined in RFC 2778 [RFC2778].

The term location user is used to refer to the entity that is consuming location information. In the context of RFC 2778 [RFC2778], the location user may be a watcher.

The term domain authority is used to refer to the entity that assumes responsibility for the accuracy of the information provided in the PIDF-LO.
2 The Domain Authorization Element

This specification describes a new namespace for a domain authorization element. This element contains the digital signature described in RFC 3275 [RFC3275] and an expiry time for the signature.

The domain-auth element is added to the tuple element that contains the geopriv element. Separate tuple elements are signed separately. The XML Schema definition for the domain-auth element is included in Section 4.1.

The digital signature signs the PIDF-LO document that includes only the tuple element that the domain-auth element is included within. Section 3.1 describes the specific means by which the correct elements are selected.

2.1 'expires' attribute

The expires attribute defines the expiry time for the domain authorization provided. A user of the PIDF-LO document MUST consider the document to be unsigned beyond the expiry time.
3 Signature Elements

The XML Signature specification [RFC3275] describes a means to sign XML documents. The Signature element consists of three major parts:
1. a description of the signed elements, which may be an entire document, or selected parts of a document
2. a digital signature
3. information on the key used to sign the document

3.1 PIDF-LO Document Transform

Since the content of XML documents is indeterminate based on similar data sets, RFC 3275 [RFC3275] describes a set of transforms that may be applied to a document before applying a digital signature.

The input PIDF-LO document MUST be canonicalized using either Canonical XML (http://www.w3.org/TR/2001/REC-xml-c14n-20010315) or Exclusive Canonical XML (http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718) [W3C.REC-xml-exc-c14n-20020718]. Note that both of these canonicalization methods remove comments from the source document.

The signature form selected for this document is an enveloped signature. Therefore the enveloped signature transform (http://www.w3.org/2000/09/xmldsig#enveloped-signature) MUST be applied to the document.

A filter is applied to the input document in order to select the correct elements for signing. It is RECOMMENDED that the transformed document is also a valid PIDF-LO. In addition, the transform should exclude tuple elements other than the element that is directly signed. This ensures that other content may be included in other tuple elements, including other digital signatures.

The following elements MUST be selected:
• the presence element, which includes the entity attribute
• the location-info element and all of its contents
• the timestamp element associated with the signed tuple element
• the domain-auth element

The minimum set of elements required to ensure that the signed document is a valid PIDF-LO SHOULD also be included.

The XML Path Language (XPath) filter defined in Section 4.2 meets the above criteria. For convenience, and to reduce the size of a signed PIDF-LO document, this transform may be identified by the URN urn:ietf:params:xml:ns:pidf:geopriv10:domain-auth#PIDF-LO.

Note that any elements from other namespaces included within the domain-auth element are selected by this XPath filter. This ensures that additions to this element are covered by the digital signature.

3.2 Algorithms

As recommended in RFC 3275 [RFC3275], implementations of this specification MUST provide the following algorithms:

<table>
<thead>
<tr>
<th>digest algorithm:</th>
<th>The SHA1 digest, as identified by the URN <a href="http://www.w3.org/2000/09/xmldsig#sha1">http://www.w3.org/2000/09/xmldsig#sha1</a>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>signature algorithm:</td>
<td>DSA with SHA1, as identified by the URN <a href="http://www.w3.org/2000/09/xmldsig#dsa-sha1">http://www.w3.org/2000/09/xmldsig#dsa-sha1</a>.</td>
</tr>
<tr>
<td>canonicalization method:</td>
<td>Canonical XML [RFC3076], as identified by the URN</td>
</tr>
</tbody>
</table>
transforms: The enveloped signature transform, as identified by the URN http://www.w3.org/2000/09/xmldsig#enveloped-signature and the transform defined in Section 4.2, as identified by the URN urn:ietf:params:xml:ns:pidf:geopriv10:domain-auth.

It is also RECOMMENDED that the following are also supported:


canonicalization method: Exclusive Canonical XML, as identified by the URN http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718/ [W3C.REC-xml-exc-c14n-20020718].

3.3 Signature Key Data

RFC 3275 [RFC3275] describes a number of methods for describing the key used to sign the document. For this specification, the KeyInfo element MUST be provided in the Signature element.

The domain authority MUST also describe a means to retrieve an X.509 certificate that includes the key used to sign the document. This can be either by including an X509Certificate element, or by referencing another certificate.

A reference to a certificate within the same document may be made using the X509SubjectName element or a fragment identifier URI. A fragment identifier URI might be applicable where multiple signatures are applied to different parts of the document. External certificate sources SHOULD be described by URI only in the RetrievalMethod element. It is RECOMMENDED that the scheme for the RetrievalMethod URI indicates a secure protocol, such as HTTPS.

The domain authority MAY include additional information in the KeyInfo element that could assist the location user in validating the certificate. For example a certificate chain and certificate revocation list may be added. However, this specification does not specify how the location user validates the certificate.
4 XML Definitions

4.1 XML Schema

The following XML schema describes the domain-auth element. This schema defines a new namespace:

<?xml version="1.0"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
attributeFormDefault="unqualified">
  <xsd:import namespace="http://www.w3.org/2000/09/xmldsig#"/>
  <xsd:annotation>
    <xsd:documentation>
      This schema defines a means for providing authentication to a PIDF-LO. This schema is also accompanied by a set of transforms that should be applied to the signed PIDF-LO.
    </xsd:documentation>
  </xsd:annotation>

  <xsd:element name="domain-auth">
    <xsd:annotation>
      <xsd:documentation>
        The domain authorization that is applied to the PIDF-LO. This element should be included within the scope of a &lt;tuple&gt; element.
      </xsd:documentation>
    </xsd:annotation>
    <xsd:complexType>
      <xsd:complexContent>
        <xsd:restriction base="xsd:anyType">
          <xsd:sequence>
            <xsd:element ref="dsig:Signature"/>
            <xsd:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
          </xsd:sequence>
          <xsd:attribute name="expires" use="required" type="xsd:dateTime">
            <xsd:annotation>
              <xsd:documentation>
                The expiry time associated with the authorization.
              </xsd:documentation>
            </xsd:annotation>
          </xsd:attribute>
        </xsd:restriction>
      </xsd:complexContent>
    </xsd:complexType>
  </xsd:element>
</xsd:schema>

4.2 XPath Filter

The following XPath transform follows the recommendations in RFC 3275 [RFC3275] to select the elements for signing. This specification defines a new URN for this transform:

<?xml version="1.0"?>
<dsig:Transform id="PIDF-LO"
Algorithm="http://www.w3.org/TR/1999/REC-xpath-19991116"/>
<!-- Select elements -->
{(count(self::pidf:presence | here()/ancestor::pidf:presence[1]) = 1)
  or (count(self::pidf:tuple | here()/ancestor::pidf:tuple[1]) = 1)
  or ((count(ancestor::pidf:tuple[1]
    | here()/ancestor::pidf:tuple[1]) = 1)
    and (self::pidf:status or ancestor-or-self::pidf:timestamp
    or self::gp:geopriv or self::gp:usage-rules
    or ancestor-or-self::gp:location-info))
  or (count(self::da:domain-auth
    | here()/ancestor::da:domain-auth[1]) = 1)
}
</dsig:XPath>
</dsig:Transform>
5 Examples

A sample, demonstrating a simple form of the signed PIDF-LO document is shown below.

```xml
<?xml version="1.0"?>
<pres entity="pres:user@example.com"
xmlns="urn:ietf:params:xml:ns:pidf"
xmlns:gml="http://opengis.net/gml"
xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10">
  <tuple id="pidflo1a786c3">
    <status>
      <gp:geopriv>
        <gp:location-info>
          <gml:position>
            <gml:Point srsName="urn:EPSG:geographicCRS:4979">
              <gml:pos>-34.407 150.88001 34</gml:pos>
            </gml:Point>
        </gml:position>
        <gp:usage-rules>
          <gp:retransmission-allowed>no</gp:retransmission-allowed>
          <gp:retention-expiry>2004-12-01T21:28:43+10:00</gp:retention-expiry>
        </gp:usage-rules>
      </gp:geopriv>
    </status>
    <da:domain-auth
      expires="2005-05-18T15:28:56.061+10:00"
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
          <ds:CanonicalizationMethod
            Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
          <ds:SignatureMethod
            Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <ds:Reference URI="/"/>
          <ds:Transforms/>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        </ds:SignedInfo>
        <ds:SignatureValue>
          iaEl9uK3VjpYci13oF+uyVmB12SA2HEsuJu8TtkwDcJ6f0886uU17gqmr
          U3xBv7y9H8jJse9KQf/tKQxhmOrg2TfG7/OMOqajrjtJgIi4na5YaH1co
          LAWNW1hb+iCMHvkAGxB+2cVzZQsf6Fo0nw8qNH3wBzNMFq1LcnaxyhYf
          /fI=
        </ds:SignatureValue>
      </ds:Signature>
    </da:domain-auth>
  </tuple>
</pres>
```
Note that the digest and signatures are only included to serve as an example. Several elements are included in the above example that should not be signed by the domain authority, as described in Section 3.1, in particular usage-rules and note-well.

The transform described in Section 3.1 removes extraneous elements, resulting in the following PIDF-LO, which only includes the signed elements (in this example whitespace has been added for readability):

```
<pres xmlns="urn:ietf:params:xml:ns:pidf"
      xmlns:gml="http://opengis.net/gml"
      xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
      entity="pres:user@example.com">
  <tuple id="pidflo1a786c3">
    <status>
      <gp:geopriv>
        <gp:location-info>
          <gml:position>
            <gml:Point srsName="urn:EPSG:geographicCRS:4979">
              <gml:pos>-34.407 150.88001 34</gml:pos>
            </gml:Point>
          </gml:position>
        </gp:location-info>
        </gp:usage-rules>
      </gp:geopriv>
    </status>
    <da:domain-auth
  </tuple>
</presence>
```
6 Security Considerations

The security limitations of this specification are no more significant than those already identified in RFC 3275 [RFC3275]. In particular the rules **Only What is Signed is Secure, Only What is "Seen" Should be Signed**, and **"See" What is Signed SHOULD be applied**.

It is RECOMMENDED that where certitude of information is important that only the signed information is transmitted or stored, that is, the PIDF-LO document formed by performing the transform described in Section 3.1. This ensures that no additional information may be misconstrued as being verifiable. This is particular applicable if the contents of the PIDF-LO document are displayed on screen.

A degree of trust must exist between the domain authority and the location user. It is the responsibility of the location user to verify the identity of the domain authority and assert the appropriate level of trust. If the location user is unable to validate the identity of the domain authority for any reason, then the PIDF-LO document MUST be considered unsigned.
7 IANA Considerations

7.1 URN Sub-Namespace Registration for

This document registers a new XML namespace, as per the guidelines in [RFC3688].

URI: The URI for this namespace is
Registrant Contact: IETF, GEOPRIV working group, (geopriv@ietf.org),
Martin Thomson (martin.thomson@nortel.com).
XML:
BEGIN
<?xml version="1.0"?>
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML Basic 1.0//EN"
"http://www.w3.org/TR/xhtml-basic/xhtml-basic10.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<title>GEOPRIV Domain Authorization Extensions</title>
</head>
<body>
<h1>Domain Authorization Extensions</h1>
<p>See <a href="[URL of published RFC]">RFCXXXX</a>.</p>
</body>
</html>
END
8 References


Author's Addresses

Martin Thomson
Nortel
PO Box U87
University of Wollongong, NSW 2500
AU
Phone: +61 2 4254 7515
EMail: martin.thomson@nortel.com
URI: http://www.nortel.com/

James Winterbottom
Nortel
PO Box U87
University of Wollongong, NSW 2500
AU
Phone: +61 2 4223 3038
EMail: winterb@nortel.com
URI: http://www.nortel.com/
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat 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 specification can be obtained from the IETF on-line IPR repository at <http://www.w3.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2005).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

1 mailto:ietf-ipr@ietf.org