INTERNET-DRAFT
Intended Status: Proposed Standard
Updates: 3709 (once approved)
Expires: June 7, 2010

Stefan Santesson (3xA Security)
Russ Housley (Vigil Security)
Siddharth Bajaj (VeriSign)
Leonard Rosenthol (Adobe)

December 4, 2009

Internet X.509 Public Key Infrastructure - Certificate Image
<draft-ietf-pkix-certimage-04>

Status of this Memo

Copyright and License Notice

Abstract

This document specifies a method to bind a visual representation of a certificate in the form of a certificate image to a [RFC5280] public key certificate by defining a new otherLogos image type according to [RFC3709].

Table of Contents

1. Introduction

This standard specifies how to bind a Certificate Image, providing a visual representation of a certificate, to that [RFC5280] certificate using the Logotype extension defined in [RFC3709], specifying the Certificate Image as a new otherLogos type.

The purpose of the Certificate image is to aid human interpretation of a certificate by providing meaningful visual information to the user interface.

Typical situations when a human needs to examine the visual representation of a certificate are:

- A person establishes secured channel with an authenticated service. The person needs to determine the identity of the service based on the authenticated credentials.

- A person validates the signature on critical information, such as signed executable code, and needs to determine the identity of the signer based on the signer’s certificate.

- A person is required to select an appropriate certificate to be used when authenticating to a service or Identity Management infrastructure. The person needs to see the available certificates in order to distinguish between them in the selection process.

Display of a certificate information to humans is challenging due to lack of well defined semantics for critical identity attributes. Unless the application has out of band knowledge about a particular certificate, the application will not know the exact nature of the data stored in common identification attributes such as serialNumber, organizationName, country, etc. Consequently the application can display the actual data, but faces problem to label that data in the UI, informing the human about the exact nature (semantics) of that data. It is also challenging for the application to determine which identification attribute that are important to display and how to organize them in a logical order.

RFC 3709 [RFC3709] defines a certificate extension for binding images to a certificate, such as community logo and issuer logo, enhancing display of certificate information. The syntax is extensible and allows inclusion of new image types using the other-Logos structure. This standard defines how to include a complete certificate image using the extensibility mechanism of RFC 3709.

1.2 Terminology

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].

2 Certificate Image

This section defines the Certificate Image as a new otherLogos type according to section 4.1 of [RFC3709].

The Certificate Image otherLogos type is identified by the Object Identifier (OID) id-logo-certimage.

```
id-pkix  OBJECT IDENTIFIER  ::=
     { iso(1) identified-organization(3) dod(6) internet(1)
     security(5) mechanisms(5) pkix(7) }

id-logo OBJECT IDENTIFIER ::= { id-pkix 20 }

id-logo-certimage OBJECT IDENTIFIER ::= { id-logo TBD }
```

//* Note: TBD is to be replaced by a real OID before publication of this draft *//

When present the Certificate Image MUST represent a complete visual representation of the certificate. This means that the display of this certificate image represents all information about the certificate that the issuer subjectively defines as relevant to show a typical human user within the typical intended use of the certificate, giving adequate information about at least the following three aspects of the certificate:

- Certificate Context
- Certificate Issuer
- Certificate Subject

Certificate Context information is visual marks and/or textual information which helps the typical user to understand the typical usage and/or purpose of the certificate

It is up to the issuer to decide what information in the form of text and graphical symbols and elements, which represents a complete visual representation of the certificate.

Applications providing a Graphical User Interface (GUI) to the certificate user MAY present a Certificate Image according to this standard in any given application interface, as the only visual representation of a certificate.

3 LogotypeImageInfo

The optional LogotypeImageInfo structure is defined in [RFC3709] and is included here for convenience:

```
LogotypeImageInfo ::= SEQUENCE {
  type          [0] LogotypeImageType DEFAULT color,
  fileSize      INTEGER,  -- In octets
  xSize         INTEGER,  -- Horizontal size in pixels
  ySize         INTEGER,  -- Vertical size in pixels
  resolution    LogotypeImageResolution OPTIONAL,
  language      [4] IA5String OPTIONAL }  -- RFC 3066 Language Tag
```

When the optional LogotypeImageInfo is included with a certificate image, the parameters shall be used with the following semantics and restrictions.

xSize and ySize represents recommended display size for the image. When a value of 0 (zero) is present, no recommended display size specified. When non-zero values are present and these values differ from corresponding size values in the referenced image file, then the referenced image SHOULD be scaled to fit within the size parameters of LogotypeImageInfo, while keeping x and y ratio intact.

Resolution MUST NOT be specified.

4 Certificate Image Formats

4.1 PDF

A Certificate Image MAY be provided in the form of a Portable Document Format (PDF) document according to [ISO32000] following the conventions defined in this section. When a certificate image is formatted as a PDF document, it MUST also be formatted according to the profile PDF/A [ISO19005].

When including a PDF document as Certificate Image, the following MIME media type as specified in [RFC3778] MUST be used as mediaType in LogotypeDetails:

application/pdf

4.2 SVG

A Certificate Image MAY be provided in the form of a Scalable Vector Graphic (SVG) image, which MUST follow the SVG Tiny profile [SVGT1.2]

The following MIME media type defined in Appendix M of [SVGT1.2] MUST be used as mediaType in LogotypeDetails for SVG images:

image/svg+xml

The SVG image file MUST NOT incorporate any external image data by reference to an external SVG document, or by reference to an external media source other than SVG. Doing so would incorporate image data that is not covered by the logotypeHash value of the image. Certificate using applications MUST reject any image that violates this rule.

The XML structure in the SVG file MUST use <LF> (linefeed 0x0A) as end-of-line (EOL) character when calculating the hash over the SVG file. The referenced SVG file may be provided in compressed form, for example as SVG.GZ or SVGZ. It is outside the scope of this specification to specify any such compression algorithm. However, after decompression the EOL characters of the SVG file MUST be normalized according to this section before computing the hash of the SVG file.

4.2 PNG

If a certificate image is provided as a bit mapped image, the PNG [ISO15948] format SHOULD be used.

PNG images are identified by the following mediaType in LogotypeDetails:

image/png

5 Embedded images

The certificate image otherLogos type MAY be stored within the logotype extension using the "data" URL scheme defined in RFC 2397 [RFC2397] if the logotype image is provided through direct addressing, i.e. the image is referenced using the LogotypeDetails structure.

The syntax of Logotype details defined in RFC 3709 is included here for convenience:

```
LogotypeDetails ::= SEQUENCE {
   mediaType       IA5String, -- MIME media type name and optional
                              -- parameters
   logotypeHash    SEQUENCE SIZE (1..MAX) OF HashAlgAndValue,
   logotypeURI     SEQUENCE SIZE (1..MAX) OF IA5String }
```

The syntax of the "data" URL Scheme defined in RFC 2397 is included here for convenience:

```
dataurl    := "data:" [ mediatype ] [ ";base64" ] "," data
mediatype  := [ type "/" subtype ] *( ";" parameter ) data
 := *urlchar parameter  := attribute "=" value
```

When including the image data in the logotype extension using the "data" URL scheme the following conventions apply.

- the value of mediaType in LogotypeDetails MUST be identical to the mediatype value in the "data" URL.
- The hash of the image MUST be included in logotypeHash and MUST be calculated over the same data as it would have been, had the image been referenced through a link to an external resource.

Note: As the "data" URL scheme is processed as a data source rather than as a URL, the image data is typically not limited by any URL length limit setting that otherwise apply to URLs in general.

Note: Implementations need to be cautious about the the size of images included in a certificate in order to ensure that the size of the certificate does not prevent the certificate to be used as intended.

6 Security Considerations

This document is based on and inherits all security considerations from RFC 3709 [RFC3709].

Referenced image files are hashed in order to bind the image to the signature of the certificate. Some image types, such as SVG allow part of the image to be collected from external source by incorporating a reference to an external image file. If this feature were used within a certificate image file, the hash of the image file would only cover the URI reference to the external image file, but not the referenced image data. To ensure that the hash of the certificate image covers the whole image, implementations of this standard MUST reject images that incorporate parts of the image by reference to external image files.

CAs issuing certificate with embedded certificate images should be cautious when accepting graphics from the certificate requestor for inclusion in the certificate if the hash algorithm used to sign the certificate is vulnerable to collision attacks. In such case the accepted image may contain data that could help an attacker to obtain colliding certificates with identical certificate signatures.

7 IANA Considerations

This document requires no actions from IANA.

8 References

8.1 Normative References

[RFC2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008

[RFC3709] S. Santesson, R. Housley, T. Freeman, "Internet X.509 Public Key Infrastructure Logotypes in X.509 Certificates", RFC 3709, February 2004

[RFC2397] L. Masinter, ’The "data" URL scheme’ RFC 2397, August 1998

[ISO32000] ISO 32000-1:2008, "Document management - Portable document format" -- Part 1: PDF 1.7, April 2008

[ISO19005] ISO 19005-1:2005, "Document Management - Electronic document file format for long term preservation - Part 1: Use of PDF 1.4 (PDF/A-1)", 2005

[ISO15948] ISO/IEC 15948:2004, "Information technology - Computer graphics and image processing -- Portable Network Graphics (PNG): Functional specification", 2004

[SVGT1.2] W3C Recommendation, "Scalable Vector Graphics (SVG) Tiny 1.2 Specification", December 2008

8.2 Informative References

[RFC3778] E. Taft, J. Pravetz, S. Zilles, L. Masinter "The application/pdf Media Type", RFC 3778, May 2004

Appendix A - "data" URL example

The following example stores an embedded SVG image using the "data" URL scheme.

```

cvMjAwMC9zdmciIHdpZHRoPSI0MDEiIGhlaWdodD0iODAxIiB2ZXJzaW9uPSIxLj
AiPg0KPHBhdGggc3R5bGU9ImZpbGw6bm9uZTsgc3Ryb2tlOiMwMDAwMDA7IHN0cm
9rZS13aWR0aDoxMDsiDQpkPSJNNDUsNWE0MCw0MCAwIDAgMSAtNDAsNDB2MzEwYT
QwLDQwIDAgMCAxIDQwLDQwaDMxMGE0MCw0MCAwIDAgMSA0MCwtNDB2LTMxMGE0MC
w0MCAwIDAgMSAtNDAsLTQweiIvPg0KPC9zdmc+DQo=
```

This example stores the following SVG image:

```
<svg xmlns="http://www.w3.org/2000/svg" width="401" height="801"
 version="1.0">
  <path style="fill:none; stroke:#000000; stroke-width:10;"
   d="M45,5a40,40 0 0 1 -40,40v310a40,40 0 0 1 40,40h310a40,
   40 0 0 1 40,-40v-310a40,40 0 0 1 -40,-40z"/>
</svg>
```

Authors' Addresses

Stefan Santesson
3xA Security (AAA-sec.com)
Bjornstorp 744
247 98 Genarp
Sweden
EMail: sts@aaa-sec.com

Russell Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA
EMail: housley@vigilsec.com

Siddharth Bajaj
VeriSign
685 East Middlefield rd
Mountain view, CA 94043
USA
Email: sbajaj@verisign.com

Leonard Rosenthol
3533 Sunset Way
Huntingdon Valley, PA 19006
USA
Email: leonardr@adobe.com