INTERNET-DRAFT   Stefan Santesson (3xA Security)
Intended Status: Proposed Standard   Russ Housley (Vigil Security)
Updates: 3709 (once approved)   Siddharth Bajaj (VeriSign)
Expires: August 19, 2011   Leonard Rosenthol (Adobe)
                                                          February 15, 2011

Internet X.509 Public Key Infrastructure - Certificate Image
<draft-ietf-pkix-certimage-11>

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 public key certificate as defined in RFC 5280 [RFC5280] by defining a new otherLogos image type according to RFC 3709 [RFC3709].

Table of Contents

1. Introduction 3
   1.2. Terminology 4
2. Certificate Image 4
3. LogotypeImageInfo 5
4. Embedded images 6
5. Certificate Image Formats 7
   5.1. PDF 7
   5.2. SVG 7
   5.3. PNG 8
6. Security Considerations 9
7. Acknowledgements 10
8. IANA Considerations 10
9. References 10
   9.1. Normative References 10
   9.2. Informative References 11
Appendix A - ASN.1 Module 12
Appendix B - Example 13
Authors' Addresses 14

1. Introduction

This standard specifies how to bind a Certificate Image to a certificate (defined in [RFC5280]), providing a visual representation of that 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 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 3 }
```

When present the Certificate Image MUST be 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 that represents a complete visual representation of the certificate. However, The visual representation of Subject and Issuer information from the certificate MUST have the same meaning as the textual representation of that information in the certificate itself.

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
```

Note: The referenced RFC 3066 in the structure above (from RFC 3709) is obsolete and is currently replaced by RFC 5646 [RFC5646]. The language tag may carry information about the the language used to express any textual elements within the image as well as any audio information associated with the image.

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.

The resolution parameter is redundant for all image formats that are relevant for certificate images and MUST NOT be specified.

4. Embedded images

The certificate image otherLogos type defined in this specification and all logotype types defined in RFC 3709 [RFC3709] 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 media type 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 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.

5. Certificate Image Formats

Implementations of this specification MUST support JPEG and GIF as defined in RFC 3709 [RFC3709]. In addition to these mandatory to implement formats, this specification specifies the use of PDF, SVG and PNG as image formats.

5.1. 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
```

5.2. SVG

A Certificate Image MAY be provided in the form of a Scalable Vector Graphic (SVG) image, which MUST follow the SVG Tiny profile [SVGT] with the following amendments:

- The SVG image MUST NOT contain any IRI references to information stored outside of the SVG image of type B, C or D according to section 14.1.4 of SVG Tiny 1.2 [SVGT]

- The SVG image MUST NOT contain any 'script' element according to section 15.2 of SVG Tiny 1.2 [SVGT]

- The XML structure in the SVG file MUST use <LF> (linefeed 0x0A) as end-of-line (EOL) character when calculating a hash over the SVG image.

The referenced SVG file MAY be provided in GZIP [RFC1952] compressed form as an SVGZ file according to section 1.2 in SVG 1.1 [SVG]. Hash over the SVGZ file is calculated over the decompressed SVG content with canonicalized EOL characters (<LF>) as specified above.

The following MIME media type, defined in Appendix M of [SVGT], MUST be included as mediaType in LogotypeDetails for all SVG and SVGZ images:

image/svg+xml

When the SVG image is embedded using the "data" URL scheme as defined in section 4, SVG image data MUST be provided in SVGZ (GZIP compressed) form (i.e. it MUST NOT be provided in uncompressed SVG form).

Compliant implementations of this specification SHOULD be able to process SVG images that are formatted according to this section.

5.3. 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

6. Security Considerations

This document is based on and inherits all security considerations from RFC 3709 [RFC3709]. In particular, RFC 3709 discusses several issues a Certificate Authority should take into consideration when evaluating a request to issue a certificate with a certificate image.

Images incorporated according to RFC 3709 provide an additional possibility for a CA with bad intentions or bad security procedures to include false, conflicting or malicious information to relying parties. A bad performing CA may for example;

- include information in graphical form that is in conflict with information in provided text based attributes or other name forms, and;

- include malicious data that could exploit known security bugs in common software libraries used to render graphical images.

This underlines the necessity for CAs to provide reliable services and the relying party's responsibility and need to carefully select which CA that is trusted to provide public key certificates.

This also underlines the general necessity for relying parties to use up-to-date software libraries to render or dereference data from external sources (such as certificates) to minimize risks related to processing potentially malicious data before the data has been adequately verified and validated.

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. Clients SHOULD verify that SVGT images meets all requirements of section 5.2 and reject images that contain references to external data.

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.

Certificates, and hence their cert images, are commonly public objects and as such usually will not contain privacy sensitive

information. However, when a cert image that is referenced from a certificate contains privacy sensitive information appropriate security controls should be in place to protect the privacy of that information. Details of such controls are outside the scope of this document.

7. Acknowledgements The Authors recognize valuable contributions from members of the PKIX work group, the CA Browser Forum and James Manger

for review and sample data.

8. IANA Considerations

This document requires no actions from IANA.

9. References

9.1. Normative References

[RFC1952] P. Deutsch, "GZIP file format specification version 4.3", RFC 1952, May 1996

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

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

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

[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

[RFC5646] A. Phillips, M. Davis, "Tags for Identifying Languages", RFC 5646, September 2009

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

[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

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

[SVG] W3C Recommendation, "Scalable Vector Graphics (SVG) 1.1 Specification", January 2003

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

9.2. Informative References

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

Appendix A - ASN.1 Module

```
   CERT-IMAGE-MODULE { iso(1) identified-organization(3) dod(6)
       internet(1)  security(5) mechanisms(5) pkix(7) id-mod(0)
       id-mod-logotype-certimage(68) }

   DEFINITIONS EXPLICIT TAGS ::=
   BEGIN

     EXPORTS ALL;   -- export all items from this module

       id-logo-certImage  OBJECT IDENTIFIER  ::=
             { iso(1) identified-organization(3) dod(6) internet(1)
             security(5) mechanisms(5) pkix(7) id-logo(20) 3 }


   END
```

Appendix B - Example

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

```
data:image/svg+xml;base64,
H4sIAAAAAAAAAO1aW3OjxhJ+968gbKXKrhJo7jCy5WTtvZSrUptT65yTZ4xGElkE
KkCWvb8+PYAkQEKSLe3amxz5RfQMQ1++7v4a+eKXh0lo3KskDeKob2IbmYaK/HgQ
RKO++d8/PliuaaSZFw28MI5U34xi85fLk4ufLMu4TpSXqYExD7KxcRN9SX1vqozT
cZZNe93ufD63g1Jox8moe2ZY1uXJyUV6PzoxDAOeG6U9uOiblTvmNN9LEEJdWDOX
O3fuqtmgBfNgkI3hEqGf8+uxCkbjrCK4D9T8Kn7om8hABkPIoKi4Mxj0zWuVZMEw
8MFC42bijZR5CUsXAzVM9ZZi04cgzOCx+RIsDvPLYhnU7psWshGm1OEcCXMhf8zl
mBKMqLMSL9S1EREOx0v5Um2bCEaQw5crfhzGiRVE8MxpHHoZWG8VKoC30s8fr5Y7
ta7FCpXILdXVCquP3ixNAy+6CmdLxQ0I+OCdug/yI/smsQmRpKJSeWDtZioxQKdb
eqJbPG2jX56nNiZPVRvbTDLqYLZLb7ZR74uujnX+bbSKeOg9qgQvAj5anJwlXpQO
42TSN/OvYJY6RbagnEtKSAeC52DsCn5WM+52DMmRLkVp9hhCiqVZEn9RvTco/6zM
TpSfrUwp8cJKzNbBwpDNK2KN8cqlRmAzmvpwgVxpVt2ZqwMuCbUyBAv3XF9YySxU
vSiOvqokPi881psl4embFcbOlj49VHGrLgHdCa9qWXH9xMuS4OEUdxD8YZu7iDAh
O5U4WNhhNsOSs7ON9kvcbj9ClG60FpOatWEQqfrZWgJn09rZOsZW6QtSNZDANcY1
o8vd8dTzgww8gOzaHbhvCqfuN31ITYAbAm2VruaRarFYL51X1eyR87oePa3GPoZv
MKXFcIzIk8yu79dWU8HtdcPtlzLd2d90hp9mem1/afpribjc32xHPBHqzTvaTH+h
mGO0IY5Hy/PmHS9i/EV3VHTI0cb2SNba4xqhiobxqq9l6qHSHqDkO26j4Fc7xYZ6
b3MgWFyIvO4TGzPOMJVQ7JG0iUuIgK/gESEpx826fwXHDZa6aG3SqRet9hS7ciGE
turVnJj2YMEHN04TlarkXtXWaw1kCB/fP1809yH3XYTqTted7vLKi77cvLvo5o+8
LJXqah+1O0wbSl3ZdBsDIaOcbPYeMPNQkxTXYdApXQwdEzPKEJNNH1VD98fjdBOK
4iiz0uCr6mHQRAAxB941fTgv5HoPYCyZeGEhufcSoF9ZTTbPGUBNBM5RmT9eynI/
EoWABxcbht4kCB97b+G0cO8Yus+K4fENGeaftTzbZNl/gBvHkRca6uadAdEzbgYq
KkMCXPdpYGmghEtbSsxJkybfzu7+Ak5kfEi8CYQ9yMLWuB/LLc8NKcYvHtI6Z19L
60223aTpDKbnLDaemOykSYg525zhq1HEcjtYimZe5xok3zPCSyqNNuJ8z3CzFw/3
hgxuJvQi9rQwF7dCIGkP/45Guxgovmcy1pt6iaC8n2+cYpduEIUbyJa2D6yFSf26
pI5u7EDvdhgTO0gAYQj6Fy+HP8pdaGUudH4gBIRRKTsUGhwVWLotefBJp8HbDI67
m0Gn+58Xzra3OgIdTltheWEwinpp5iXZuSaBVjHOwg7+8/k8CbIgGlmTeKB6YWJl
d+VNkT+Ok+KufaHPnkdA6iofFSfHsb9MKN/1XUfsLKZr1HRjfX3/4E2mIRS2ZJZm
RkGrjBWVgb5pvJ1loAKc8bQKDMSKI0xxA6cS2dJFePvLCWQ7QlDEWI5TyAsJ4MT6
JQUWwFUd4nQwkwB4l7XVa51txnU8mQYh9I8lYNOtWMXQ5fUH8e8P2gMY17ru/xL0
5qiF8H6OvYEBM2XHuIVSRg3Gjdss9r+M43ACsj/fv3v/SXvt92T0xuAcY0IsShk7
BqKBxgOZd1rYxQrQxHVdhzYATWwkBaIO62BObbQFz9dgvQdMs9ZFXke95Qcwy39b
vVXWxAvCnhFAGH/NCvjavverKuqw7ceT3El/qrue/hGnIu+W231vJxdqMpDFmFJ/
pTCqA22xadXcf/PuVLirYjIAMJdMx3DpIk4QWXORhAEa5mZeg1Utx4osc2zHJc0m
DonmEtvF1KX1hbVZHduI6V26W5SPrOVUOa3Hk0kcNchMbm9FvU24r5NsadbXdmH/
W08MUu41Kud211HULH8twRG2S/R7o2ZwMAHeKBg+SnBulVbz02xyB4XvgPAQ8mOG
5zq4D3zjsxoFsLsgYYUznhWytnwCKmVz5gp5jJBBZ/Wi4GvJGA8IGf9BQwalOZ4A
XOOhcapp9NkzY0URrf9oUdJmaWOMHXac2jeLsuTxoDC5P2iYStMhStX02h6rZVPd
p2fmA/H2nrlqle2Dfws+9Mwj0FoqS2YTwaELt8FjOf8LQpmAiX/x4y/BrqAdC6o3
iLn+qucqrofotqa56xXA0uSjs9CdsKQHFvxXzUa3E1C25Q3ax1kE1G8E1Um/I093
4b0Ve0Qyx1lv/VjaSAhOvi34ClJgrLGC1wS/A5vXPxR+WFKOOOYWzLnkOdCjMEwR
4WCyBj0GMCIuF98Wei3k5jUh78B+/A9F3u1cDe6AjBlvr46LO0FtKij+1u22ydNe
EeIaHPX/iFshTu3LJ6u/XF3o/9G9PPkbr+DaC2ssAAA=
```

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