

Network Working Group
Internet-Draft
Obsoletes: [3709](#), [6170](#) (if approved)
Intended status: Standards Track
Expires: 31 August 2022

S. Santesson
IDsec Solutions
R. Housley
Vigil Security
T. Freeman
Amazon Web Services
L. Rosenthol
Adobe
27 February 2022

Internet X.509 Public Key Infrastructure: Logotypes in X.509
Certificates
draft-ietf-lamps-rfc3709bis-01

Abstract

This document specifies a certificate extension for including logotypes in public key certificates and attribute certificates. This document obsoletes [RFC 3709](#) and [RFC 6170](#).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

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."

This Internet-Draft will expire on 31 August 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components

extracted from this document must include Revised BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Revised BSD License.

Table of Contents

1.	Introduction	3
1.1.	Certificate-based Identification	4
1.2.	Selection of Certificates	5
1.3.	Combination of Verification Techniques	5
1.4.	Terminology	6
2.	Different Types of Logotypes in Certificates	6
3.	Logotype Data	7
4.	Logotype Extension	8
4.1.	Extension Format	8
4.2.	Conventions for LogotypeImageInfo	12
4.3.	Embedded Images	12
4.4.	Other Logotypes	13
4.4.1.	Loyalty Logotype	13
4.4.2.	Certificate Background Logotype	13
4.4.3.	Certificate Image Logotype	14
5.	Type of Certificates	15
6.	Use in Clients	15
7.	Image Formats	17
8.	Audio Formats	18
9.	Security Considerations	19
10.	IANA Considerations	21
11.	Acknowledgments	21
11.1.	Acknowledgments from RFC 3709	22
11.2.	Acknowledgments from RFC 6170	22
11.3.	Additional Acknowledgments	22
12.	References	22
12.1.	Normative References	22
12.2.	Informative References	24
Appendix A.	ASN.1 Modules	25
A.1.	ASN.1 Modules with 1988 Syntax	25
A.2.	ASN.1 Module with 1997 Syntax	28
Appendix B.	Examples	31
B.1.	Example from RFC 3709	31
B.2.	Issuer Logotype Example	32
B.3.	Embedded Image Example	33
B.4.	Embedded Certificate Image Example	35
Appendix C.	Changes Since RFC 3709 and RFC 6170	37

[1.](#) Introduction

This specification supplements [\[RFC5280\]](#), which profiles public-key certificates and certificate revocation lists (CRLs) for use in the Internet, and it supplements [\[RFC5755\]](#) which profiles attribute certificates for use in the Internet.

This document obsoletes [RFC 3709](#) [\[RFC3709\]](#) and [RFC 6170](#) [\[RFC6170\]](#). [Appendix C](#) provides a summary of the changes since the publication of [RFC 3709](#) and [RFC 6170](#).

The basic function of a certificate is to bind a public key to the identity of an entity (the subject). From a strictly technical viewpoint, this goal could be achieved by signing the identity of the subject together with its public key. However, the art of Public Key Infrastructure (PKI) has developed certificates far beyond this functionality in order to meet the needs of modern global networks and heterogeneous information technology structures.

Certificate users must be able to determine certificate policies, appropriate key usage, assurance level, and name form constraints. Before a relying party can make an informed decision whether a particular certificate is trustworthy and relevant for its intended usage, a certificate may be examined from several different perspectives.

Systematic processing is necessary to determine whether a particular certificate meets the predefined prerequisites for an intended usage. Much of the information contained in certificates is appropriate and effective for machine processing; however, this information is not suitable for a corresponding human trust and recognition process.

Humans prefer to structure information into categories and symbols. Most humans associate complex structures of reality with easily recognizable logotypes and marks. Humans tend to trust things that they recognize from previous experiences. Humans may examine

information to confirm their initial reaction. Very few consumers actually read all terms and conditions they agree to in accepting a service, rather they commonly act on trust derived from previous experience and recognition.

A big part of this process is branding. Service providers and product vendors invest a lot of money and resources into creating a strong relation between positive user experiences and easily recognizable trademarks, servicemarks, and logotypes.

Branding is also pervasive in identification instruments, including identification cards, passports, driver's licenses, credit cards, gasoline cards, and loyalty cards. Identification instruments are intended to identify the holder as a particular person or as a member of the community. The community may represent the subscribers of a service or any other group. Identification instruments, in physical form, commonly use logotypes and symbols, solely to enhance human recognition and trust in the identification instrument itself. They may also include a registered trademark to allow legal recourse for unauthorized duplication.

Since certificates play an equivalent role in electronic exchanges, we examine the inclusion of logotypes in certificates. We consider certificate-based identification and certificate selection.

1.1. Certificate-based Identification

The need for human recognition depends on the manner in which certificates are used and whether certificates need to be visible to human users. If certificates are to be used in open environments and in applications that bring the user in conscious contact with the result of a certificate-based identification process, then human recognition is highly relevant, and may be a necessity.

Examples of such applications include:

- * Web server identification where a user identifies the owner of the web site.

- * Peer e-mail exchange in B2B, B2C, and private communications.
- * Exchange of medical records, and system for medical prescriptions.
- * Unstructured e-business applications (i.e., non-EDI applications).
- * Wireless client authenticating to a service provider.

Most applications provide the human user with an opportunity to view the results of a successful certificate-based identification process. When the user takes the steps necessary to view these results, the user is presented with a view of a certificate. This solution has two major problems. First, the function to view a certificate is often rather hard to find for a non-technical user. Second, the presentation of the certificate is too technical and is not user friendly. It contains no graphic symbols or logotypes to enhance human recognition.

Many investigations have shown that users of today's applications do not take the steps necessary to view certificates. This could be due to poor user interfaces. Further, many applications are structured to hide certificates from users. The application designers do not want to expose certificates to users at all.

[1.2.](#) Selection of Certificates

One situation where software applications must expose human users to certificates is when the user must select a single certificate from a portfolio of certificates. In some cases, the software application can use information within the certificates to filter the list for suitability; however, the user must be queried if more than one certificate is suitable. The human user must select one of them.

This situation is comparable to a person selecting a suitable plastic card from his wallet. In this situation, substantial assistance is provided by card color, location, and branding.

In order to provide similar support for certificate selection, the users need tools to easily recognize and distinguish certificates. Introduction of logotypes into certificates provides the necessary

graphic.

1.3. Combination of Verification Techniques

The use of logotypes will, in many cases, affect the users decision to trust and use a certificate. It is therefore important that there be a distinct and clear architectural and functional distinction between the processes and objectives of the automated certificate verification and human recognition.

Since logotypes are only aimed for human interpretation and contain data that is inappropriate for computer based verification schemes, the logotype extension MUST NOT be an active component in automated certification path validation.

Automated certification path verification determines whether the end-entity certificate can be verified according to defined policy. The algorithm for this verification is specified in [[RFC5280](#)].

The automated processing provides assurance that the certificate is valid. It does not indicate whether the subject is entitled to any particular information, or whether the subject ought to be trusted to perform a particular service. These are access control decisions. Automatic processing will make some access control decisions, but others, depending on the application context, involve the human user.

In some situations, where automated procedures have failed to establish the suitability of the certificate to the task, the human user is the final arbitrator of the post certificate verification access control decisions. In the end, the human will decide whether or not to accept an executable email attachment, to release personal information, or follow the instructions displayed by a web browser. This decision will often be based on recognition and previous experience.

The distinction between systematic processing and human processing is rather straightforward. They can be complementary. While the systematic process is focused on certification path construction and verification, the human acceptance process is focused on recognition and related previous experience.

There are some situations where systematic processing and human processing interfere with each other. These issues are discussed in the [Section 9](#).

[1.4](#). Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14](#) [[RFC2119](#)] [[RFC8174](#)] when, and only when, they appear in all capitals, as shown here.

[2](#). Different Types of Logotypes in Certificates

This specification defines the inclusion of three standard logotype types:

- * Community logotype
- * Issuer organization logotype
- * Subject organization logotype

The community logotype is the general mark for a community. It identifies a service concept for entity identification and certificate issuance. Many issuers may use a community logotype to co-brand with a global community in order to gain global recognition of its local service provision. This type of community branding is very common in the credit card business, where local independent card issuers include a globally recognized brand (such as VISA and MasterCard).

Issuer organization logotype is a logotype representing the organization identified as part of the issuer name in the certificate.

Subject organization logotype is a logotype representing the organization identified in the subject name in the certificate.

In addition to the standard logotype types, this specification

accommodates inclusion of other logotype types where each class of logotype is defined by an object identifier. The object identifier can be either locally defined or an identifier defined in [Section 4.4](#) of this document.

[3.](#) Logotype Data

This specification defines two types of logotype data: image data and audio data. Implementations **MUST** support image data; however, support for audio data is **OPTIONAL**.

There is no need to significantly increase the size of the certificate by including image and audio data of logotypes when a URI identifying the location to the logotype data and a one-way hash of the referenced data is included in the certificate. Embedding the logotype in the certificate (as defined in [Section 4.3](#)) can significantly increase the size of the certificate.

Several image objects, representing the same visual content in different formats, sizes, and color palates, may represent each logotype image. At least one of the image objects representing a logotype **SHOULD** contain an image within the size range of 60 pixels wide by 45 pixels high, and 200 pixels wide by 150 pixels high.

Several instances of audio data may further represent the same audio sequence in different formats, resolutions, and languages. At least one of the audio objects representing a logotype **SHOULD** have a play time between 1 and 30 seconds.

If a logotype of a certain type (as defined in [Section 1.1](#)) is represented by more than one image object, then the image objects **MUST** contain variants of roughly the same visual content. Likewise, if a logotype of a certain type is represented by more than one audio object, then the audio objects **MUST** contain variants of the same audio information. A spoken message in different languages is considered a variation of the same audio information. Compliant applications **MUST NOT** display more than one of the image objects and **MUST NOT** play more than one of the audio object for any logotype type at the same time.

logotype types. For example, it may display one subject organization logotype while also displaying a community logotype, but it MUST NOT display multiple image variants of the same community logotype.

Each logotype present in a certificate MUST be represented by at least one image data object.

Client applications SHOULD enhance processing and off-line functionality by caching logotype data.

[4.](#) Logotype Extension

This section specifies the syntax and semantics of the logotype certificate extension.

[4.1.](#) Extension Format

The logotype extension MAY be included in public key certificates [[RFC5280](#)] or attribute certificates [[RFC5755](#)]. The logotype extension MUST be identified by the following object identifier:

```
id-pe-logotype OBJECT IDENTIFIER ::=
    { iso(1) identified-organization(3) dod(6) internet(1)
      security(5) mechanisms(5) pkix(7) id-pe(1) 12 }
```

This extension MUST NOT be marked critical.

Logotype data may be referenced through either direct or indirect addressing. Client applications MUST support both direct and indirect addressing. Certificate issuing applications MUST support direct addressing, and certificate issuing applications SHOULD support indirect addressing.

The direct addressing includes information about each logotype in the certificate, and URIs point to the image and audio data object. Direct addressing supports cases where just one or a few alternative images and audio objects are referenced.

The indirect addressing includes one reference to an external hashed data structure that contains information on the type, content, and location of each image and audio object. Indirect addressing supports cases where each logotype is represented by many alternative audio or image objects.

Both direct and indirect addressing accommodate alternative URIs to obtain exactly the same item. This opportunity for replication is intended to improve availability. Therefore, if a client is unable

to fetch the item from one URI, the client SHOULD try another URI in the sequence. All direct addressing URIs SHOULD use either the HTTP scheme (<http://...>) or the HTTPS scheme (<https://...>) or the DATA scheme (<data://...>) [[RFC3986](#)]; however, the "data" URI scheme MUST NOT be used with the indirect addressing. Clients MUST support retrieval of referenced LogoTypeData with the HTTP/2 [[RFC7540](#)] and the HTTPS/2 with TLS [[RFC8740](#)]. Client applications SHOULD also support the "data" URI scheme [[RFC2397](#)] for direct addressing with embedded logotype data within the extension.

The logotype extension MUST have the following syntax:

```
LogotypeExtn ::= SEQUENCE {
    communityLogos  [0] EXPLICIT SEQUENCE OF LogotypeInfo OPTIONAL,
    issuerLogo      [1] EXPLICIT LogotypeInfo OPTIONAL,
    subjectLogo     [2] EXPLICIT LogotypeInfo OPTIONAL,
    otherLogos      [3] EXPLICIT SEQUENCE OF OtherLogotypeInfo
                        OPTIONAL }

LogotypeInfo ::= CHOICE {
    direct          [0] LogotypeData,
    indirect        [1] LogotypeReference }

LogotypeData ::= SEQUENCE {
    image           SEQUENCE OF LogotypeImage OPTIONAL,
    audio           [1] SEQUENCE OF LogotypeAudio OPTIONAL }

LogotypeImage ::= SEQUENCE {
    imageDetails    LogotypeDetails,
    imageInfo       LogotypeImageInfo OPTIONAL }

LogotypeAudio ::= SEQUENCE {
    audioDetails    LogotypeDetails,
    audioInfo       LogotypeAudioInfo OPTIONAL }

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 }

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 5646 Language Tag

```
LogotypeImageType ::= INTEGER { grayScale(0), color(1) }
```

```
LogotypeImageResolution ::= CHOICE {  
    numBits      [1] INTEGER,    -- Resolution in bits  
    tableSize    [2] INTEGER }  -- Number of colors or grey tones
```

```
LogotypeAudioInfo ::= SEQUENCE {  
    fileSize      INTEGER,    -- In octets  
    playTime      INTEGER,    -- In milliseconds  
    channels       INTEGER,    -- 1=mono, 2=stereo, 4=quad  
    sampleRate    [3] INTEGER OPTIONAL, -- Samples per second  
    language      [4] IA5String OPTIONAL } -- RFC 5646 Language Tag
```

```
OtherLogotypeInfo ::= SEQUENCE {  
    logotypeType  OBJECT IDENTIFIER,  
    info          LogotypeInfo }
```

```
LogotypeReference ::= SEQUENCE {  
    refStructHash SEQUENCE SIZE (1..MAX) OF HashAlgAndValue,  
    refStructURI  SEQUENCE SIZE (1..MAX) OF IA5String }  
    -- Places to get the same LogotypeData  
    -- image or audio object
```

```
HashAlgAndValue ::= SEQUENCE {  
    hashAlg      AlgorithmIdentifier,  
    hashValue    OCTET STRING }
```

When using indirect addressing, the URI (refStructURI) pointing to the external data structure MUST point to a binary file containing the DER-encoded data with the syntax LogotypeData.

At least one of the optional elements in the LogotypeExtn structure MUST be present. Avoid the use of otherLogos whenever possible.

When using direct addressing, at least one of the optional elements in the LogotypeData structure MUST be present.

The LogotypeReference and LogotypeDetails structures explicitly identify one or more one-way hash functions employed to authenticate

referenced image or audio objects. CAs MUST include a hash value for each referenced object, calculated on the whole object. CAs SHOULD include a hash value that computed with the one-way hash function associated with the certificate signature, and CAs MAY include other hash values. Clients MUST compute a one-way hash value using one of the identified functions, and clients MUST discard the logotype data if the computed hash value does not match the hash value in the certificate extension.

A MIME type is used to specify the format of the image or audio object containing the logotype data. The `mediaType` field MUST contain a string that is constructed according to the ABNF [\[RFC5234\]](#) provided in [Section 4.2 of \[RFC6838\]](#). MIME types MAY include parameters.

Image format requirements are specified in [Section 7](#), and audio format requirements are specified in [Section 8](#).

When language is specified, the language tag MUST use the [\[RFC5646\]](#) syntax.

Logotype types defined in this specification are:

Community Logotype: If `communityLogos` is present, the logotypes MUST represent one or more communities with which the certificate issuer is affiliated. The `communityLogos` MAY be present in an end entity certificate, a CA certificate, or an attribute certificate. The `communityLogos` contains a sequence of Community Logotypes, each representing a different community. If more than one Community logotype is present, they MUST be placed in order of preferred appearance. Some clients MAY choose to display a subset of the present community logos; therefore the placement within the sequence aids the client selection. The most preferred logotype MUST be first in the sequence, and the least preferred logotype MUST be last in the sequence.

Issuer Organization Logotype: If `issuerLogo` is present, the logotype MUST represent the issuer's organization. The logotype MUST be consistent with, and require the presence of, an organization name stored in the organization attribute in the issuer field (for either a public key certificate or attribute

certificate). The issuerLogo MAY be present in an end entity certificate, a CA certificate, or an attribute certificate.

Subject Organization Logotype: If subjectLogo is present, the logotype MUST represent the subject's organization. The logotype MUST be consistent with, and require the presence of, an organization name stored in the organization attribute in the subject field (for either a public key certificate or attribute certificate). The subjectLogo MAY be present in an end entity certificate, a CA certificate, or an attribute certificate.

The relationship between the subject organization and the subject organization logotype, and the relationship between the issuer and either the issuer organization logotype or the community logotype, are relationships asserted by the issuer. The policies and practices employed by the issuer to check subject organization logotypes or claims its issuer and community logotypes is outside the scope of this document.

[4.2.](#) Conventions for LogotypeImageInfo

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

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

The resolution field is redundant for all logotype image formats listed in [Section 7](#). The optional resolution field SHOULD be omitted when the image format already contains this information.

[4.3.](#) Embedded Images

If the logotype image is provided through direct addressing, then the image MAY be stored within the logotype certificate extension using the "data" scheme [[RFC2397](#)]. The syntax of the "data" URI scheme defined 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" URI 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" URI scheme is processed as a data source rather than as a URL, the image data is typically not limited by any URL length limit settings 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 from being used as intended.

[4.4.](#) Other Logotypes

Logotypes identified by otherLogos (as defined in [Section 4.1](#)) can be used to enhance the display of logotypes and marks that represent partners, products, services, or any other characteristic associated with the certificate or its intended application environment when the standard logotype types are insufficient.

The conditions and contexts of the intended use of these logotypes

are defined at the discretion of the local client application.

Three other logotype types are defined in the follow subsections.

[4.4.1.](#) Loyalty Logotype

When a loyalty logotype appears in the otherLogos, it MUST be identified by the id-logo-loyalty object identifier.

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

id-logo-loyalty OBJECT IDENTIFIER ::= { id-logo 1 }

A loyalty logotype, if present, MUST contain a logotype associated with a loyalty program related to the certificate or its use. The relation between the certificate and the identified loyalty program is beyond the scope of this document. The logotype extension MAY contain more than one Loyalty logotype.

[4.4.2.](#) Certificate Background Logotype

When a certificate background logotype appears in the otherLogos, it MUST be identified by the id-logo-background object identifier.

id-logo-background OBJECT IDENTIFIER ::= { id-logo 2 }

The certificate background logotype, if present, MUST contain a graphical image intended as a background image for the certificate, and/or a general audio sequence for the certificate. The background image MUST allow black text to be clearly read when placed on top of the background image. The logotype extension MUST NOT contain more than one certificate background logotype.

[4.4.3.](#) Certificate Image Logotype

When a certificate image logotype appears in the otherLogos, it MUST be identified by the id-logo-background object identifier.

id-logo-certImage OBJECT IDENTIFIER ::= { id-logo 3 }

The certificate image logotype, if present, aids human interpretation of a certificate by providing meaningful visual information to the user interface (UI). Typical situations when a human needs to examine the visual representation of a certificate are:

- * A person establishes a 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.

The 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 the problem of labeling that data in the UI and informing the human about the exact nature (semantics) of that data. It is also challenging for the application to determine which identification attributes are important to display and how to organize them in a logical order.

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 to 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 that 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, graphical symbols, and elements -- represents a complete visual representation of the certificate. However, the visual representation of Certificate Subject and Certificate 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.

[5.](#) Type of Certificates

Logotypes **MAY** be included in public key certificates and attribute certificates at the discretion of the certificate issuer; however, logotypes **MUST NOT** be part of certification path validation or any type of automated processing. The sole purpose of logotypes is to enhance the display of a particular certificate, regardless of its position in a certification path.

[6.](#) Use in Clients

All PKI implementations require relying party software to have some mechanism to determine whether a trusted CA issues a particular certificate. This is an issue for certification path validation, including consistent policy and name checking.

After a certification path is successfully validated, the replying party trusts the information that the CA includes in the certificate, including any certificate extensions. The client software can choose to make use of such information, or the client software can ignore it. If the client is unable to support a provided logotype, the

client MUST NOT report an error, rather the client MUST behave as though no logotype extension was included in the certificate. Current standards do not provide any mechanism for cross-certifying CAs to constrain subordinate CAs from including private extensions (see [Section 9](#)).

Consequently, if relying party software accepts a CA, then it should be prepared to (unquestioningly) display the associated logotypes to its human user, given that it is configured to do so. Information about the logotypes is provided so that the replying party software can select the one that will best meet the needs of the human user. This choice depends on the abilities of the human user, as well as the capabilities of the platform on which the replying party software is running. If none of the provided logotypes meets the needs of the human user or matches the capabilities of the platform, then the logotypes can be ignored.

A client MAY, subject to local policy, choose to display none, one, or any number of the logotypes in the logotype extension. In many cases, a client will be used in an environment with a good network connection and also used in an environment with little or no network connectivity. For example, a laptop computer can be docked with a high-speed LAN connection, or it can be disconnected from the network altogether. In recognition of this situation, the client MUST include the ability to disable the fetching of logotypes. However, locally cached logotypes can still be displayed when the user disables the fetching of additional logotypes.

A client MAY, subject to local policy, choose any combination of audio and image presentation for each logotype. That is, the client MAY display an image with or without playing a sound, and it MAY play a sound with or without displaying an image. A client MUST NOT play more than one logotype audio sequence at the same time.

The logotype is to be displayed in conjunction with other identity information contained in the certificate. The logotype is not a replacement for this identity information.

Care is needed when designing replying party software to ensure that an appropriate context of logotype information is provided. This is especially difficult with audio logotypes. It is important that the human user be able to recognize the context of the logotype, even if other audio streams are being played.

If the relying party software is unable to successfully validate a particular certificate, then it MUST NOT display any logotype data associated with that certificate.

7. Image Formats

Animated images SHOULD NOT be used.

The following table lists many common image formats and their corresponding MIME type. The table also indicates which of the image formats must be supported by implementations. The filename extensions commonly used for each of these formats is also provided. Implementations MAY support other image formats.

Format	MIME Type	.ext	References	Implement?
JPEG	image/jpeg	.jpg .jpeg	[JPEG] [RFC2046]	MUST support
GIF	image/gif	.gif	[GIF] [RFC2046]	MUST support
SVG	image/ svg+xml	.svg	[SVGT] [SVGR]	SHOULD support
SVG + GZIP	image/ svg+xml+gzip	.svgz .svg.gz	[SVGT] [SVGZR]	MUST support
PNG	image/png	.png	[ISO15948] [PNGR]	SHOULD support
PDF	application/ pdf	.pdf	[ISO32000] [ISO19005] [RFC8118]	MAY support

Table 1: Image Formats

NOTE: The image/svg+xml-compressed media type is widely implemented, but it has not yet been registered with IANA.

When a Scalable Vector Graphics (SVG) image is used, whether the image is compressed or not, the SVG Tiny profile [[SVGT](#)] MUST be

followed, with these additional restrictions:

- * The SVG image MUST NOT contain any Internationalized Resource Identifier (IRI) references to information stored outside of the SVG image of type B, C, or D, according to Section 14.1.4 of [\[SVGT\]](#).

- * The SVG image MUST NOT contain any 'script' element, according to Section 15.2 of [\[SVGT\]](#).
- * The XML structure in the SVG file MUST use linefeed (0x0A) as the end-of-line (EOL) character when calculating a hash over the SVG image.

When a GZIP-compressed SVG image is fetched with HTTP, the client will receive response that includes these headers:

```
Content-Type: image/svg+xml
Content-Encoding: gzip
```

In this case, the octet stream of type image/svg+xml is compressed with GZIP [\[RFC1952\]](#) as specified in [\[SVGR\]](#).

When a uncompressed SVG image is fetched with HTTP, the client will receive response with the same Content-Type header, but no Content-Encoding header.

Whether the SVG image is GZIP-compressed or uncompressed, the hash value for the SVG image is calculated over the uncompressed SVG content with canonicalized EOL characters as specified above.

When a SVG image is embedded in the certificate extension using the "data" URL scheme, the SVG image data MUST be provided in GZIP-compressed form, and the XML structure, prior to compression, SHOULD use linefeed (0x0A) as the end-of-line (EOL) character.

When a bitmapped image is used, the PNG [\[ISO15948\]](#) format SHOULD be used.

When a Portable Document Format (PDF) document according to

[[ISO32000](#)] is used, it MUST also be formatted according to the profile PDF/A [[ISO19005](#)].

[8.](#) Audio Formats

Implementations that support audio MUST support the MP3 audio format [[MP3](#)] with a MIME type of "audio/mpeg" [[RFC3003](#)]. Implementations MAY support other audio formats.

[9.](#) Security Considerations

Implementations that simultaneously display multiple logotype types (subject organization, issuer, community, or other), MUST ensure that there is no ambiguity as to the binding between the image and the type of logotype that the image represents. "Logotype type" is defined in [Section 1.1](#), and it refers to the type of entity or affiliation represented by the logotype, not the of binary format if the image or audio.

Logotypes are very difficult to securely and accurately define. Names are also difficult in this regard, but logotypes are even worse. It is quite difficult to specify what is, and what is not, a legitimate logotype of an organization. There is an entire legal structure around this issue, and it will not be repeated here. However, issuers should be aware of the implications of including images associated with a trademark or servicemark before doing so. As logotypes can be difficult (and sometimes expensive) to verify, the possibility of errors related to assigning wrong logotypes to organizations is increased.

This is not a new issue for electronic identification instruments. It is already dealt with in a number of similar situations in the physical world, including physical employee identification cards. In addition, there are situations where identification of logotypes is rather simple and straightforward, such as logotypes for well-known

industries and institutes. These issues should not stop those service providers who want to issue logotypes from doing so, where relevant.

It is impossible to prevent fraudulent creation of certificates by dishonest or badly performing issuers, containing names and logotypes that the issuer has no claim to or has failed to check correctly. Such certificates could be created in an attempt to socially engineer a user into accepting a certificate. The premise used for the logotype work is thus that logotype graphics in a certificate are trusted only if the certificate is successfully validated within a valid path. It is thus imperative that the representation of any certificate that fails to validate is not enhanced in any way by using the logotype data.

This underlines the necessity for CAs to provide reliable services, and the relying party's responsibility and need to carefully select which CAs are 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, including logotype data in certificates, to minimize risks related to processing potentially malicious data before it has been adequately verified and validated.

Referenced image objects 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 an external source by incorporating a reference to an external file that contains the image. If this feature were used within a logotype image, the hash of the image would only cover the URI reference to the external image file, but not the referenced image data. Clients SHOULD verify that SVG images meet all requirements listed in [Section 7](#) and reject images that contain references to external data.

Logotype data is fetched from a server when it is needed. By watching activity on the network, an observer can determine which clients are making use of certificates that contain particular

logotype data. This observation can potentially introduce privacy issues. Since clients are expected to locally cache logotype data, network traffic to the server containing the logotype data will not be generated every time the certificate is used. In cases where logotype data is not cached, monitoring would reveal usage frequency. In cases where logotype data is cached, monitoring would reveal when a certain logotype image or audio sequence is used for the first time.

CAs issuing certificates with embedded logotype 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 a case, the accepted image may contain data that could help an attacker to obtain colliding certificates with identical certificate signatures.

Certificates, and hence their logotype images, are commonly public objects and as such usually will not contain privacy-sensitive information. However, when a logotype 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.

Certification paths may also impose name constraints that are systematically checked during certification path processing, which, in theory, may be circumvented by logotypes.

Certificate path processing as defined in [[RFC5280](#)] does not constrain the inclusion of logotype data in certificates. A parent CA can constrain certification path validation such that subordinate CAs cannot issue valid certificates to end-entities outside a limited name space or outside specific certificate policies. A malicious CA can comply with these name and policy requirements and still include inappropriate logotypes in the certificates that it issues. These certificates will pass the certification path validation algorithm, which means the client will trust the logotypes in the certificates. Since there is no technical mechanism to prevent or control subordinate CAs from including the logotype extension or its contents, where appropriate, a parent CA could employ a legal

agreement to impose a suitable restriction on the subordinate CA. This situation is not unique to the logotype extension.

The controls available to a parent CA to protect itself from rogue subordinate CAs are non-technical. They include:

- * Contractual agreements of suitable behavior, including terms of liability in case of material breach.
- * Control mechanisms and procedures to monitor and follow-up behavior of subordinate CAs.
- * Use of certificate policies to declare an assurance level of logotype data, as well as to guide applications on how to treat and display logotypes.
- * Use of revocation functions to revoke any misbehaving CA.

There is not a simple, straightforward, and absolute technical solution. Rather, involved parties must settle some aspects of PKI outside the scope of technical controls. As such, issuers need to clearly identify and communicate the associated risks.

[10.](#) IANA Considerations

For the new ASN.1 Module in [Appendix A.2](#), IANA is requested to assign an object identifier (OID) for the module identifier. The OID for the module should be allocated in the "SMI Security for PKIX Module Identifier" registry (1.3.6.1.5.5.7.0).

[11.](#) Acknowledgments

[11.1.](#) Acknowledgments from [RFC 3709](#)

This document is the result of contributions from many professionals. The authors appreciate contributions from all members of the IETF PKIX Working Group. We extend a special thanks to Al Arsenault,

David Cross, Tim Polk, Russel Weiser, Terry Hayes, Alex Deacon, Andrew Hoag, Randy Sabett, Denis Pinkas, Magnus Nystrom, Ryan Hurst, and Phil Griffin for their efforts and support.

Russ Housley thanks the management at RSA Laboratories, especially Burt Kaliski, who supported the development of this specification. The vast majority of the work on this specification was done while Russ was employed at RSA Laboratories.

11.2. Acknowledgments from [RFC 6170](#)

The authors recognize valuable contributions from members of the PKIX working group, the CA Browser Forum, and James Manger, for their review and sample data.

11.3. Additional Acknowledgments

Combining [RFC 3709](#) and [RFC 6170](#) has produced an improved specification. The authors appreciate contributions from all members of the IETF LAMPS Working Group. We extend a special thanks to Alexey Melnikov for his guidance on media types. We extend a special thanks to Corey Bonnell for his careful review and comments.

12. References

12.1. Normative References

- [GIF] CompuServe Incorporated, "Graphics Interchange Format", Version 89a, 31 July 1990, <<https://www.w3.org/Graphics/GIF/spec-gif89a.txt>>.
- [ISO15948] ISO/IEC, "Information technology -- Computer graphics and image processing -- Portable Network Graphics (PNG): Functional specification", ISO/IEC 15948:2004, 2004.
- [JPEG] ITU-T, "Information technology -- Digital compression and coding of continuous-tone still images: JPEG File Interchange Format (JFIF)", ITU-T Recommendation T.871, ISO/IEC 10918-5:2013, May 2011.
- [MP3] ISO/IEC, "Information technology -- Generic coding of moving pictures and associated audio information -- Part 3: Audio", ISO/IEC 13818-3:1998, 1998.

- [NEW-ASN1] ITU-T, "Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, ISO/IEC 8824-1:2021, February 2021, <<https://www.itu.int/rec/T-REC-X.680>>.
- [RFC1952] Deutsch, P., "GZIP file format specification version 4.3", [RFC 1952](#), DOI 10.17487/RFC1952, May 1996, <<https://www.rfc-editor.org/info/rfc1952>>.
- [RFC2046] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", [RFC 2046](#), DOI 10.17487/RFC2046, November 1996, <<https://www.rfc-editor.org/info/rfc2046>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC2397] Masinter, L., "The "data" URL scheme", [RFC 2397](#), DOI 10.17487/RFC2397, August 1998, <<https://www.rfc-editor.org/info/rfc2397>>.
- [RFC3003] Nilsson, M., "The audio/mpeg Media Type", [RFC 3003](#), DOI 10.17487/RFC3003, November 2000, <<https://www.rfc-editor.org/info/rfc3003>>.
- [RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, [RFC 3986](#), DOI 10.17487/RFC3986, January 2005, <<https://www.rfc-editor.org/info/rfc3986>>.
- [RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, [RFC 5234](#), DOI 10.17487/RFC5234, January 2008, <<https://www.rfc-editor.org/info/rfc5234>>.
- [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](#), DOI 10.17487/RFC5280, May 2008, <<https://www.rfc-editor.org/info/rfc5280>>.
- [RFC5646] Phillips, A., Ed. and M. Davis, Ed., "Tags for Identifying Languages", [BCP 47](#), [RFC 5646](#), DOI 10.17487/RFC5646, September 2009, <<https://www.rfc-editor.org/info/rfc5646>>.

Internet-Draft

Logotypes in X.509 Certificates

February 2022

- [RFC5755] Farrell, S., Housley, R., and S. Turner, "An Internet Attribute Certificate Profile for Authorization", [RFC 5755](#), DOI 10.17487/RFC5755, January 2010, <<https://www.rfc-editor.org/info/rfc5755>>.
- [RFC6838] Freed, N., Klensin, J., and T. Hansen, "Media Type Specifications and Registration Procedures", [BCP 13](#), [RFC 6838](#), DOI 10.17487/RFC6838, January 2013, <<https://www.rfc-editor.org/info/rfc6838>>.
- [RFC7540] Belshé, M., Peon, R., and M. Thomson, Ed., "Hypertext Transfer Protocol Version 2 (HTTP/2)", [RFC 7540](#), DOI 10.17487/RFC7540, May 2015, <<https://www.rfc-editor.org/info/rfc7540>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.
- [RFC8740] Benjamin, D., "Using TLS 1.3 with HTTP/2", [RFC 8740](#), DOI 10.17487/RFC8740, February 2020, <<https://www.rfc-editor.org/info/rfc8740>>.
- [SVGT] World Wide Web Consortium, "Scalable Vector Graphics (SVG) Tiny 1.2 Specification", W3C PR-SVGTiny12-20081117, 17 November 2008, <<http://www.w3.org/TR/2008/PR-SVGTiny12-20081117>>.

[12.2.](#) Informative References

- [ISO19005] ISO, "Document management -- Electronic document file format for long-term preservation -- Part 1: Use of PDF 1.4 (PDF/A-1)", ISO 19005-1:2005, 2005.
- [ISO32000] ISO, "Document management -- Portable document format -- Part 1: PDF 1.7", ISO 32000-1:2008, 2008.
- [OLD-ASN1] CCITT, "Specification of Abstract Syntax Notation One (ASN.1)", CCITT Recommendation X.208, November 1988, <<https://www.itu.int/rec/T-REC-X.208/en>>.
- [PNGR] World Wide Web Consortium, "Media Type Registration for

image/png",
<<https://www.iana.org/assignments/media-types/image/png>>.

- [RFC3709] Santesson, S., Housley, R., and T. Freeman, "Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates", [RFC 3709](#), DOI 10.17487/RFC3709, February 2004, <<https://www.rfc-editor.org/info/rfc3709>>.
- [RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", [RFC 5912](#), DOI 10.17487/RFC5912, June 2010, <<https://www.rfc-editor.org/info/rfc5912>>.
- [RFC6170] Santesson, S., Housley, R., Bajaj, S., and L. Rosenthol, "Internet X.509 Public Key Infrastructure -- Certificate Image", [RFC 6170](#), DOI 10.17487/RFC6170, May 2011, <<https://www.rfc-editor.org/info/rfc6170>>.
- [RFC6268] Schaad, J. and S. Turner, "Additional New ASN.1 Modules for the Cryptographic Message Syntax (CMS) and the Public Key Infrastructure Using X.509 (PKIX)", [RFC 6268](#), DOI 10.17487/RFC6268, July 2011, <<https://www.rfc-editor.org/info/rfc6268>>.
- [RFC8118] Hardy, M., Masinter, L., Markovic, D., Johnson, D., and M. Bailey, "The application/pdf Media Type", [RFC 8118](#), DOI 10.17487/RFC8118, March 2017, <<https://www.rfc-editor.org/info/rfc8118>>.
- [SVGR] World Wide Web Consortium, "Media Type Registration for image/svg+xml", <<https://www.iana.org/assignments/media-types/image/svg+xml>>.
- [SVGZR] "A separate MIME type for svgz files is needed", <<https://github.com/w3c/svgwg/issues/701>>.

[A.1.](#) ASN.1 Modules with 1988 Syntax

This appendix contains two ASN.1 modules, both using the old syntax [[OLD-ASN1](#)].

The first ASN.1 module provides the syntax for the Logotype certificate extension. Only comments have changed in the module from [RFC 3709](#), and the IMPORTS now come from [[RFC5280](#)].

The second ASN.1 module provides the Certificate Image object identifier. The module is unchanged from [RFC 6170](#).

```
<CODE BEGINS>
```

```
LogotypeCertExtn
```

```
  { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-mod(0)
    id-mod-logotype(22) }
```

```
DEFINITIONS IMPLICIT TAGS ::=
BEGIN
```

```
IMPORTS
```

```
  AlgorithmIdentifier FROM PKIX1Explicit88 -- RFC 5280
  { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-mod(0)
    id-pkix1-explicit(18) };
```

```
-- Logotype Extension OID
```

```
id-pe-logotype OBJECT IDENTIFIER ::=
  { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-pe(1) 12 }
```

```
-- Logotype Extension Syntax
```

```
LogotypeExtn ::= SEQUENCE {
  communityLogos  [0] EXPLICIT SEQUENCE OF LogotypeInfo OPTIONAL,
  issuerLogo      [1] EXPLICIT LogotypeInfo OPTIONAL,
  subjectLogo     [2] EXPLICIT LogotypeInfo OPTIONAL,
```

otherLogos [3] EXPLICIT SEQUENCE OF OtherLogotypeInfo
 OPTIONAL }

-- Note: At least one of the OPTIONAL components MUST be present

LogotypeInfo ::= CHOICE {
 direct [0] LogotypeData,
 indirect [1] LogotypeReference }

LogotypeData ::= SEQUENCE {
 image SEQUENCE OF LogotypeImage OPTIONAL,
 audio [1] SEQUENCE OF LogotypeAudio OPTIONAL }

-- Note: At least one of the OPTIONAL components MUST be present

LogotypeImage ::= SEQUENCE {
 imageDetails LogotypeDetails,
 imageInfo LogotypeImageInfo OPTIONAL }

LogotypeAudio ::= SEQUENCE {

 audioDetails LogotypeDetails,
 audioInfo LogotypeAudioInfo OPTIONAL }

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 }

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 5646](#) Language Tag

LogotypeImageType ::= INTEGER { grayScale(0), color(1) }

LogotypeImageResolution ::= CHOICE {
 numBits [1] INTEGER, -- Resolution in bits

```

        tableSize      [2] INTEGER } -- Number of colors or grey tones

LogotypeAudioInfo ::= SEQUENCE {
    fileSize          INTEGER, -- In octets
    playTime          INTEGER, -- In milliseconds
    channels           INTEGER, -- 1=mono, 2=stereo, 4=quad
    sampleRate        [3] INTEGER OPTIONAL, -- Samples per second
    language          [4] IA5String OPTIONAL } -- RFC 5646 Language Tag

OtherLogotypeInfo ::= SEQUENCE {
    logotypeType      OBJECT IDENTIFIER,
    info              LogotypeInfo }

LogotypeReference ::= SEQUENCE {
    refStructHash     SEQUENCE SIZE (1..MAX) OF HashAlgAndValue,
    refStructURI      SEQUENCE SIZE (1..MAX) OF IA5String }
    -- Places to get the same LogotypeData
    -- image or audio object

-- Note: The referenced LogotypeData binary file contain DER-encoded
--       LogotypeData type

HashAlgAndValue ::= SEQUENCE {
    hashAlg           AlgorithmIdentifier,
    hashValue         OCTET STRING }

-- Other logotype type OIDs

```

```

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

id-logo-loyalty OBJECT IDENTIFIER ::= { id-logo 1 }

id-logo-background OBJECT IDENTIFIER ::= { id-logo 2 }

END

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
<CODE ENDS>

```

[A.2.](#) ASN.1 Module with 1997 Syntax

Some developers like to use the latest version of ASN.1 standards. This appendix provides an ASN.1 module to assist in that goal. It uses the ASN.1 syntax defined in [[NEW-ASN1](#)], and it follows the conventions established in [[RFC5912](#)] and [[RFC6268](#)].

This ASN.1 module incorporates the module from [RFC 3709](#) and the module from [RFC 6170](#).

```

<CODE BEGINS>
LogotypeCertExtn
    { iso(1) identified-organization(3) dod(6) internet(1)
      security(5) mechanisms(5) pkix(7) id-mod(0)
      id-mod-logotype(TBD) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS
    EXTENSION
    FROM PKIX-CommonTypes-2009    -- RFC 5912

```

```

    { iso(1) identified-organization(3) dod(6) internet(1)
      security(5) mechanisms(5) pkix(7) id-mod(0)
      id-mod-pkixCommon-02(57) }

AlgorithmIdentifier{}, DIGEST-ALGORITHM
FROM AlgorithmInformation-2009
    { iso(1) identified-organization(3) dod(6) internet(1)

```



```

    security(5) mechanisms(5) pkix(7) id-mod(0)
    id-mod-algorithmInformation-02(58) } ;

-- Logotype Extension

ext-logotype EXTENSION ::= {
    SYNTAX LogotypeExtn
    IDENTIFIED BY id-pe-logotype }

-- Logotype Extension OID

id-pe-logotype OBJECT IDENTIFIER ::=
    { iso(1) identified-organization(3) dod(6) internet(1)
      security(5) mechanisms(5) pkix(7) id-pe(1) 12 }

-- Logotype Extension Syntax

LogotypeExtn ::= SEQUENCE {
    communityLogos  [0] EXPLICIT SEQUENCE OF LogotypeInfo OPTIONAL,
    issuerLogo      [1] EXPLICIT LogotypeInfo OPTIONAL,
    subjectLogo     [2] EXPLICIT LogotypeInfo OPTIONAL,
    otherLogos      [3] EXPLICIT SEQUENCE OF OtherLogotypeInfo
                      OPTIONAL }
    -- At least one of the OPTIONAL components MUST be present
    ( WITH COMPONENTS { ..., communityLogos PRESENT } |
      WITH COMPONENTS { ..., issuerLogo PRESENT } |
      WITH COMPONENTS { ..., subjectLogo PRESENT } |
      WITH COMPONENTS { ..., otherLogos PRESENT } )

LogotypeInfo ::= CHOICE {
    direct          [0] LogotypeData,
    indirect        [1] LogotypeReference }

LogotypeData ::= SEQUENCE {
    image           SEQUENCE OF LogotypeImage OPTIONAL,
    audio           [1] SEQUENCE OF LogotypeAudio OPTIONAL }
    -- At least one of the OPTIONAL components MUST be present
    ( WITH COMPONENTS { ..., image PRESENT } |
      WITH COMPONENTS { ..., audio PRESENT } )

```

```

LogotypeImage ::= SEQUENCE {
    imageDetails    LogotypeDetails,
    imageInfo       LogotypeImageInfo OPTIONAL }

LogotypeAudio ::= SEQUENCE {
    audioDetails    LogotypeDetails,
    audioInfo       LogotypeAudioInfo OPTIONAL }

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 }

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 5646 Language Tag

LogotypeImageType ::= INTEGER { grayScale(0), color(1) }

LogotypeImageResolution ::= CHOICE {
    numBits         [1] INTEGER, -- Resolution in bits
    tableSize       [2] INTEGER } -- Number of colors or grey tones

LogotypeAudioInfo ::= SEQUENCE {
    fileSize        INTEGER, -- In octets
    playTime        INTEGER, -- In milliseconds
    channels         INTEGER, -- 1=mono, 2=stereo, 4=quad
    sampleRate      [3] INTEGER OPTIONAL, -- Samples per second
    language        [4] IA5String OPTIONAL } -- RFC 5646 Language Tag

OtherLogotypeInfo ::= SEQUENCE {
    logotypeType    OBJECT IDENTIFIER,
    info            LogotypeInfo }

LogotypeReference ::= SEQUENCE {
    refStructHash   SEQUENCE SIZE (1..MAX) OF HashAlgAndValue,
    refStructURI    SEQUENCE SIZE (1..MAX) OF IA5String }
    -- Places to get the same LogotypeData
    -- image or audio object

-- Note: The referenced LogotypeData binary file contain DER-encoded
--       LogotypeData type

```

Internet-Draft

Logotypes in X.509 Certificates

February 2022

```
HashAlgAndValue ::= SEQUENCE {
    hashAlg      AlgorithmIdentifier{DIGEST-ALGORITHM, {...}},
    hashValue    OCTET STRING }

-- Other logotype type OIDs

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

id-logo-loyalty    OBJECT IDENTIFIER ::= { id-logo 1 }

id-logo-background OBJECT IDENTIFIER ::= { id-logo 2 }

id-logo-certImage  OBJECT IDENTIFIER ::= { id-logo 3 }

END
<CODE ENDS>
```

[Appendix B](#). Examples

[B.1](#). Example from [RFC 3709](#)

The following example displays a logotype extension containing one Issuer logotype using direct addressing. The issuer logotype image is of the type image/gif. The logotype image is referenced through one URI and the image is hashed with SHA-1. This example is unchanged from [RFC 3709](#), except that shallow indenting is used to keep the example within traditional margins. The use of SHA-1 was reasonable at the time that [RFC 3709](#) was published, but many better choices are available today.

The values on the left are the ASN.1 tag (in hexadecimal) and the length (in decimal).

```
30 106: SEQUENCE {
06   8:  OBJECT IDENTIFIER logotype (1 3 6 1 5 5 7 1 12)
04  94:  OCTET STRING, encapsulates {
30  92:   SEQUENCE {
A1  90:    [1] {
A0  88:    [0] {
30  86:      SEQUENCE {
30  84:        SEQUENCE {
30  82:          SEQUENCE {
16   9:          IA5String 'image/gif'
30  33:          SEQUENCE {
30  31:            SEQUENCE {
30   7:            SEQUENCE {
06   5:              OBJECT IDENTIFIER sha1 (1 3 14 3 2 26)
:              }
04  20:            OCTET STRING
:              8F E5 D3 1A 86 AC 8D 8E 6B C3 CF 80 6A D4 48 18
:              2C 7B 19 2E
:              }
:            }
30  34:          SEQUENCE {
16  32:            IA5String 'http://logo.example.com/logo.gif'
:            }
:          }
:        }
:      }
:    }
:  }
: }
```

[B.2.](#) Issuer Logotype Example

The following example displays a logotype extension containing one Issuer logotype using direct addressing. The issuer logotype image

is of the type image/jpeg. The logotype image is referenced through one URI and the image is hashed with SHA-256.

The values on the left are the ASN.1 tag (in hexadecimal) and the length (in decimal).

```
30 124: SEQUENCE {
06  8:  OBJECT IDENTIFIER logotype (1 3 6 1 5 5 7 1 12)
04 112: OCTET STRING, encapsulates {
30 110:  SEQUENCE {
A1 108:    [1] {
A0 106:    [0] {
30 104:      SEQUENCE {
30 102:        SEQUENCE {
30 100:          SEQUENCE {
16 10:            IA5String 'image/jpeg'
30 49:            SEQUENCE {
30 47:              SEQUENCE {
30 11:                SEQUENCE {
06  9:                  OBJECT IDENTIFIER
:                      sha-256 (2 16 840 1 101 3 4 2 1)
:                      }
04 32:                OCTET STRING
:                    1E 8F 96 FD D3 50 53 EF C6 1C 9F FC F0 00 2E 53
:                    B4 9C 24 9A 32 C5 E9 0C 2C 39 39 D3 AD 6D A9 09
:                    }
:                  }
30 35:                SEQUENCE {
16 33:                  IA5String 'http://logo.example.com/logo.jpeg'
:                  }
:                }
:              }
:            }
:          }
:        }
:      }
```

```

:   }
:   }
:   }

```

B.3. Embedded Image Example

The following example displays a logotype extension containing one Subject logotype using direct addressing. The subject logotype image uses image/svg+xml-compressed. The logotype image is embedded in the certificate extension with a "data:" URI and the image is hashed by SHA-256. This technique produces a large certificate extension, but offers reduced latency and improved privacy.

The values on the left are the ASN.1 tag (in hexadecimal) and the length (in decimal).

```

30 2160: SEQUENCE {
06   8:  OBJECT IDENTIFIER logotype (1 3 6 1 5 5 7 1 12)
04 2146:  OCTET STRING, encapsulates {
30 2142:   SEQUENCE {
A2 2138:    [2] {
A0 2134:     [0] {
30 2130:      SEQUENCE {
30 2126:       SEQUENCE {
30 2122:        SEQUENCE {
16  24:         IA5String 'image/svg+xml-compressed'
30  49:         SEQUENCE {
30  47:          SEQUENCE {
30  11:           SEQUENCE {
06   9:            OBJECT IDENTIFIER
:             sha-256 (2 16 840 1 101 3 4 2 1)
:             }
04  32:            OCTET STRING
:             C5 AC 94 1A 0A 25 1F B3 16 6F 97 C5 52 40 9B 49
:             9E 7B 92 61 5A B0 A2 6C 19 BF B9 D8 09 C5 D9 E7
:             }
:            }
30 2041:          SEQUENCE {

```

```

16 2037:      IA5String
:      ''
:      'AA2xvZ28tY29weS5zdmcApVbbbhs3EH3nV0y3Lw2Q9fK2JLe'
:      'wHdROUBRo2iBxW+RRlTa2UFkypIWV5ut7zLB2UqF9cuLLUkt'
:      'yLmfOzPD8xafbtdyPu/1qu5k17sw2sp/mm+V8vd2Ms2azbV5'
:      'cmPNvXv16efXh7WvZ31/L299e/vzTpTRt1/0RLrvu1dUref/'
:      '7j+KtdXawsete/9IYaW6m6e77rjscDmeHcLbdXXdX7zpu6t6'
:      '9vmxxon08AREdRDt7tpyWDRRSz7+tgP2b/ew/hEKI5WGoPKy'
:      'W082s8SmeWf13NzVyM66ub6ZZk+xxH+9X4+Hl9t0ssWLLy35'
:      '53ARpd7txP+7uxx/2d+NiejefVttZ8+nNavkBj9y040RLb8d'
:      'pvpXP8wtzuRvn07iUP/+Wu+20my9GcWfOPpfDbjVN44YLb8d'
:      'p3Mn7cb3aXGNCAICCc+a8+yLo/FpwfLP/uN3dzhqdriH5uwf'
:      'bnj9a+Uz2i/maK66utA+zZ435uFqvZ823R38Q1t32Lw3pZqT'
:      'hd/PpRpaz5o2LNkocvCzaIm0vrQvSpog359lLy3my0ga+e3H'
:      'p+B4InjVFPD9awdhnrGEFW30Sl/Pnpvta2QBVxUEVxFbJ2VU'
:      'FfYC01pUs+04GK84V/k6CHUFyhvhiDVQF8Y5aPDbmnsrXbS7'
:      '4DANjguwgENZLPwjUYVTRJQgEpiLR0ctiWj+Ig8rCvZAARxK'
:      'ExEEWMJLqMA1F+ggnsQDXgpQeomJPCVhtCRycNrAWxgAI+g1'
:      'Qsr6IUxlomBswjydYBEg0eVCDORReBjiFjX2SdSA60BP5DgQ'
:      'M63xoPlWHbNq+egAEeAzxyNAdCQz+sDEM0haGisKJdSlS6gt'
:      'Wwm4M1rQwP0egEBIhhFLoXuCJhR4mT5RJBaILKqqFR0UEzYr'
:      '1idG0gahwCzEnk+AMJLdp0FevQQ6VZ+SK0wGl0IJ0h1MVjo0'
:      'eB6DRA10SRpSY6il/eFFKAm+MKSIWNFqSo40FnORfWH5wJHC'
:      'MNM0qlDRlcIwUEkDlgiSBhiEpBgMK0x5FdAYqI3KYewKKkAI'
:      'tTABTkp5khI86kgb0gRywEBR0VGcwAjf8t9wqvduMG6GLabI'
:      '0QQ8CbzCTtCSn/DEhCbm++duQaiRG1mQkdWHnminHA+r5wpL'

```

```

:      'vsJbCALUKsDW5NAj43J+AD5vpfamUzJqiRJACmCWwIMhQq4H'
:      'mYGKaiiJPmIvpS80UzTtAjdSraApQZogslGfCJHw0y5WoEXD'
:      'Yr/aTqfxk2qhcg3z6ETQL+S18llvH0ZQvLE0VEVpzqCozE9V'
:      '6JZhh/lCslg7mUFY4AR7IlcApmgV6gz3DCSDe56fQ0SRS7el'
:      '0NJW08mQ6mkc6ylPpaL7QUZ5IR/M/dEwoJiEp+L6iT4cdSyI'
:      'p4ljDkoaZpQlgMoz0ApahjTiTWbZYu9v+MUqVjY61j2Bxr68'
:      'bPF3uS1232qAyAQDMhr4MRyVZq5l2QcuwgY/oTozbgoIKyCh'
:      '+yQxhzQsPJQ/ne90mRKvYH1AeKA/EQRtZrmaYUuiHUhpJ0W4b'
:      'reSaxZ/TVc3ZAQJKOagAJiw6pRHVkBMIba5E+SUMWi0ZNW1R'
:      'fn/xQXyWHXyMHN5G8WF6gZ2IVjANHMIJQ1lAJQE8MJjZHjiU'
:      'tQZAWzmkiSdywTVWSqLkkQG2NNB3wwyaerqRGLNKpVwU0haQ'
:      'FiYcqviSjvp1n8WnRRzXF59IXDxiidD8HU/R0oAGn9+QgTPE'
:      'Vu6HaN6i0VPuv1SCzwyZeHwBA1EjFY0Ak2jJ30FeJ5Gp1E+3'
:      'Dlf3Aj70bbvmag5oyKHunVyGPq6+EnvTua/JUn3iadMHLqUa'
:      'psK2T8SwCBJUF1JnEmhu0ntBthJoQpZqumsBk5mA1hRc0LR5'

```



```

06      9:      OBJECT IDENTIFIER
          :      sha-256 (2 16 840 1 101 3 4 2 1)
          :      }
04     32:      OCTET STRING
          :      83 14 B3 26 9B D3 8B 0B 2A E6 6E 42 74 E2 A7 57
          :      7A 40 B7 E1 2E 53 42 44 CC 7C AE 14 68 1B 0E B6
          :      }
          :      }
30 2777:      SEQUENCE {
16 2773:      IA5String
          :      ''
          :      'AA0NlcnRjbWFnZURlbW8uc3ZnANVaW2/b0BZ+n19BqBigwdo'
          :      'S7xK9jmeapB0EWHQHzez2WZZoR1tZMiQ5jvvr95CSL7G1Em'
          :      '8C9d9iERSPOd85+05EB3+9jhL0YMuyiTPLh3iYgfpLMrjJJt'
          :      'eOv/661M/cFBZhVkcpcnmml50sd34b/TiSh6YoiS+da11UySS'
          :      'Jwkqj21k41Q6CDbNyUMSTS+e+quYDz1sul+6SuXkx9YhSysP'
          :      'Uo7QPK/r1KqvCx35Wvmu+a/uGYow9EOigh0Qvr/LHSwcjjDj'
          :      'GiGHQ914n0/sKlMf4Vwctk7i6X7/sGEYdNA5L/WeRT5IUDKm'
          :      'SbLVWNoo2cqNCh1XyoKN8Nsuz0iqwVW8Qb1f0F0Vqp+PI06m'
          :      'e6awqPeISzxn9goYzXYVxWlUWpfWLCMwCgoLpgy83n8wzGkb'
          :      'R4GtefENmMBznC7DEroKp0BpM8mIWVqPEYGtA+BvoMfS2E5u'
          :      'F1Wqu7R6FLvNFEe1WReNo1piV3l2VpGntMW9nk6RKdf0+9Br'
          :      'FrMbeVuWhtzbHvMR6UlobPyVpBWjXBk7six2vH5nCwY6nXCo'
          :      '5xb7YusvFVPqC0Gh16fSxSxglmPkScLfvmDDmC4FLDc1wov8'
          :      'IF2WZhNlVumgEPRLiimDD3PhGPYTgUUMC6lKqKAjxaptq1bo'
          :      'UJvQFsvi+LOJyxZkPE/vCwHuAmXmoj1AarnRBatzqkbv7cK5'
          :      'Ls2ORfwM/vsOG5lURZqXx0nDXPKZw5t5jVzIhFK00B6D6hAR'
          :      'SXDR6Fzqq7H7mQeJAOQiUSPvFIrUH0fuui3zrFI5dYVeAmpc'
          :      '0c0b9u63vLjae4kYX4yRifYPrTa2SlmigYd0+cEWeGADMLZL'
          :      'H96SH4R9xRYAp16q3Y02f+Nz1RAL+cZSKhB6qSIVa80fsqMn'
          :      'W0qZJpmsXwAPoyNaQ95uNIGasKPwhxGzQz0XzMIIzBKabmLI'
          :      'il470zfsjWWn+kvvpLQ9g1l3yRIc8gukz0uysEcakcDfy3KM'
          :      'k+l0SOXl0opl1tJL7EPtUlzZfP4tnM70k8xkKCyst92MwfIXP'
          :      'oTe0pnu4dYbp7hJ/kxWySN0ey0o/1qbiCsxDXJMWwo37QekB'
          :      'cAUFPSGkPCnUJF5wwBacDK5cGLEp4BC2lYoJcrNNGVc7DzIq'
          :      'xT4CKsPlrAG8mL8whRejiQe9EmImIAoz3sds9NxP4RZEzugq'
          :      'zb7c3Q89u3WQKY9aegbsA/AUJB/bJs6pfJt9BHFEuk5DWITz'
          :      'OH5uZSThLUsdjQ5GE6RMsyihMTaQLfA6BIiAQMAhnHHN1sd6'
          :      '1WtUhDVJiuhkrdBXd740+hLB9Vm1HjQe4ywLOBLWOMMIyQAX'
          :      'NB8sm9Gx2qdGgGkMG6wY8aLfqgH4dfnmrVc+pPrE/Z/QnZOs'

```

```

:      '8C10kb2/ggwLdxlDC1D6DFPZDD98txv8xQf5TEc7Ax6ZyaDf'

```


- * Drop SHA-1 as the mandatory-to-implement hash algorithm, and encourage use of the one-way hash function that is employed by the certificate signature algorithm.
- * Update the reference for language tags to be [RFC 5646](#) instead of the now obsolete [RFC 3066](#).
- * Update the reference for the URI Generic Syntax to be [RFC 3986](#) instead of the now obsolete [RFC 2396](#).
- * Update the reference for the application/pdf media type to be [RFC 8118](#) instead of the now obsolete [RFC 3778](#).
- * No longer require support for the FTP scheme (ftp://...) URI.
- * Require support for the HTTP scheme (http://...) URI and the HTTPS scheme (https://...) URI.
- * Require support for the compressed SVG image format with the image/svg+xml+gzip media type.
- * Media types MUST follow the ABNF [[RFC5234](#)] that is provided in [Section 4.2 of \[RFC6838\]](#). This change resolves Errata ID 2679.
- * Remove the requirement that the LogotypeData file name have a file extension of ".LTD". This change resolves Errata ID 2325.
- * Provide ASN.1 modules for the older syntax [[OLD-ASN1](#)] and most recent syntax [[NEW-ASN1](#)].
- * Provide additional references.
- * Provide additional examples.

Authors' Addresses

Stefan Santesson
IDsec Solutions AB
Forskningsbyn Ideon
SE-223 70 Lund
Sweden
Email: sts@aaa-sec.com

Internet-Draft

Logotypes in X.509 Certificates

February 2022

Russ Housley
Vigil Security, LLC
516 Dranesville Road
Herndon, VA, 20170
United States of America
Email: housley@vigilsec.com

Trevor Freeman
Amazon Web Services
1918 8th Ave
Seattle, WA, 98101
United States of America
Email: frtrevor@amazon.com

Leonard Rosenthol
Adobe
345 Park Avenue
San Jose, CA, 95110
United States of America
Email: lrosenthol@adobe.com

