PKIX Working Group
INTERNET-DRAFT
Expires June 2004

S. Santesson (Microsoft)
R. Housley (Vigil Security)
T. Freeman (Microsoft)
December 2003

Internet X.509 Public Key Infrastructure: Logotypes in X.509 certificates

<draft-ietf-pkix-logotypes-13.txt>

Status of this Memo

Abstract

This document specifies a certificate extension for including logotypes in public key certificates and attribute certificates.

Please send comments on this document to the ietf-pkix@imc.org mailing list.

Table of Contents

1. Introduction

This specification supplements RFC 3280 [PKIX-1], which profiles X.509 certificates and certificate revocation lists (CRLs) for use in the Internet. The X.509 certificate and CRL definitions use ASN.1 [X.208-88], the Basic Encoding Rules (BER) [X.209-88], and the Distinguished Encoding Rules (DER) [X.509-88].

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 PKI has developed certificates far beyond this functionality in order to meet the needs of modern global networks and heterogeneous IT 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 easy 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 accept when 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 member of 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 it 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, it 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 is 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 RFC 3280 [PKIX-1].

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 Security Considerations section.

1.4. 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 RFC 2119 [STDWORDS].

2. Different Types of Logotypes in Certificates

This specification defines the inclusion of three standard logotype types.

1) Community logotype
2) Issuer organization logotype
3) 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 4.2 of this standard.

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. Rather, a

URI identifying the location to the logotype data and a one-way hash of the referenced data is included in the certificate.

Several image files, representing the same image in different formats, sizes, and color palates, may represent each logotype image. At least one of the image files 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 audio files may further represent the same audio sequence in different formats and resolutions. At least one of the audio files representing a logotype SHOULD have a play time between 1 and 30 seconds.

If a logotype of a certain type (as defined in section 2) is represented by more than one image file, then the image files MUST contain variants of roughly the same image. Likewise, if a logotype of a certain type is represented by more than one audio file, then the audio files MUST contain variants of the same audio information. A spoken message in different languages is considered variants of the same audio information. Compliant applications MUST NOT display more than one of the images and MUST NOT play more than one of the audio sequences for any logotype type at the same time.

A client MAY simultaneously display multiple logotypes of different logotype types. For example, it may display one subject organization logotype at the same time as 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 file.

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 extension.

4.1 Extension format

The logotype extension MAY be included in public key certificates [PKIX-1] or attribute certificates [PKIX-AC]. 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. Clients 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 files. Direct addressing supports cases where just one or a few alternative images and audio files 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 file. Indirect addressing supports cases where each logotype is represented by many alternative audio or image files.

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 URI MUST use either the HTTP scheme (http://...) or the FTP scheme (ftp://...) [URI]. At least one URI in each sequence MUST use the HTTP scheme. Clients MUST support retrieval of referenced LogoTypeData with HTTP/1.1 [HTTP/1.1]. Clients MAY support retrieval using FTP [FTP].

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 3066 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 3066 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 "LTD" file

  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. The referenced file name SHOULD include a file extension of "LTD".

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

The LogotypeReference and LogotypeDetails structures explicitly identify one or more one-way hash functions employed to authenticate referenced data files. Clients MUST support the SHA-1 [SHS] one-way hash function, and clients MAY support other one-way hash functions. CAs MUST include a SHA-1 hash value for each referenced file, calculated on the whole file, and CAs MAY include other one-way 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 one-way hash function value does not match the one-way hash function value in the certificate extension.

A MIME type is used to specify the format of the file containing the logotype data. Implementations MUST support both the JPEG and GIF image formats (with MIME types of "image/jpeg" and "image/gif" [MEDIA], respectively). Animated images SHOULD NOT be used. Implementations that support audio MUST support the MP3 audio format (with a MIME type of "audio/mpeg" [AUDIO/MPEG]). MIME types MAY include parameters.

When language is specified, the language tag MUST use the RFC 3066 [LANGCODES] syntax.

Logotype types defined in this specification are:

Community Logotype. If communityLogos is present, the logotypes

MUST represent one or more communities to 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 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 standard.

4.2 Other Logotypes

Logotypes identified by otherLogos (as defined in 4.1) can be used to enhance 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.

The following other logotype types are defined in this standard:

- Loyalty logotype
- Certificate Background logotype

OID Definitions:

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

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



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

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 standard. The logotype extension MAY contain more than one Loyalty logotype.

The certificate background logotype, if present, MUST contain a graphical image intended as 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.

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 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 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 the security considerations section).

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 replaying 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 appropriate context of logotype information is provided. This is especially difficult with audio logotypes. It is important that the human user is able to distinguish 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. 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 2, and it refers to the type of entity or affiliation represented by the logotype, not the type of binary format.

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 a whole 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, this increases the possibility of errors related to assigning wrong logotypes to organizations.

This is not a new issue for electronic identification instruments. It is already dealt with in numerous of similar situations in the physical world, including physical employee identification cards. Secondly, 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 graphic.

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 contains 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 cashed, 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.

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 RFC 3280 [PKIX-1] 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 polices. 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 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.

8. IANA Considerations

Certificate extensions and attribute certificate extensions are identified by object identifiers (OIDs). The OID for the extension defined in this document was assigned from an arc delegated by the IANA to the PKIX Working Group. No further action by the IANA is necessary for this document or any anticipated updates

9. IPR Considerations

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the

IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

10. References

10.1. Normative References

[LANGCODES] H. T. Alvestrand, "Tags for Identification of Languages", RFC 3066, January 2001.

[PKIX-1] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[SHS] Federal Information Processing Standards Publication (FIPS PUB) 180-1, Secure Hash Standard, 17 April 1995. [Supersedes FIPS PUB 180 dated 11 May 1993.]

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

[HTTP/1.1] UC Irvine, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616

[FTP] J. Postel, and J. K. Reynolds, "File Transfer Protocol (FTP)", RFC 959, October 1985.

[URI] T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

[MEDIA] N. Freed and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, November 1996

[AUDIO/MPEG] M. Nilsson, "The audio/mpeg Media Type", RFC 3003,

November 2000

[X.208-88] CCITT Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1), 1988.

[X.209-88] CCITT Recommendation X.209: Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), 1988.

10.2. Informative References

[CMS] R. Housley, Cryptographic Message Syntax (CMS), RFC 3369, August 2002.

[X.509-88] CCITT Recommendation X.509: The Directory - Authentication Framework. 1988.

APPENDIX A. ASN.1 Module

```
   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 3280
        { 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 }

   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 3066 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 3066 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 "LTD" file

   -- Note: The content of referenced "LTD" files is defined by the
   --       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
```

APPENDIX B. Example extension

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 file is referenced through 1 URI and the image is hashed by one sha1 hash value.

The values on the left are the ASN.1 tag and length, in hexadecimal.

```
 30  106: SEQUENCE {
 06    8:   OBJECT IDENTIFIER '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'
       :                   }
       :                 }
       :               }
       :             }
       :           }
       :         }
       :       }
       :     }
       :   }
```


APPENDIX C. Acknowledgments

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.

APPENDIX D. Author Addresses

Stefan Santesson
Microsoft Denmark
Tuborg Boulevard 12
DK-2900 Hellerup
Denmark
stefans@microsoft.com

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

Trevor Freeman
Microsoft Corporation
One Microsoft Way
Redmond WA 98052
USA
trevorf@microsoft.com

Full Copyright Statement