PKIX Working Group
INTERNET-DRAFT
Expires August 2002

S. Santesson (AddTrust)
R. Housley (RSA Laboratories)
T. Freeman (Microsoft)
April 2002

Internet X.509 Public Key Infrastructure

Logotypes in X.509 certificates

<draft-ietf-pkix-logotypes-02.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

Appendices

1. Introduction

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 systematic certificate verification and human recognition.

Systematic 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 <TBD> [PKIX-1].

The systematic 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 predefined 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.

3. Image formats

This specification defines two image format types:

- High Resolution (included by reference)
- Low Resolution (icon-sized image embedded in the extension)

Format restrictions:

	High Resolution	Low Resolution
Image format	JPEG or GIF	JPEG or GIF
Size	Max 150 x 50 pixels	20 x 20 pixels
Color palette	Unlimited	256 colors (8-bit)

A high resolution image SHOULD include a black border. Exceptions are such things as arrows or X's. These images SHOULD be fairly flat in appearance with little dimensioning or shading.

There is no need to significantly increase the size of the certificate by including image data of logotypes in high quality format. Rather, a URI identifying the location to the logotype image and a one-way hash of the referenced data is included in the

certificate.

To enhance functionality for off-line and low bandwidth situations where reasonable access to high quality logotypes are not available, the icon-sized version of the logotype may optionally be stored directly in the certificate extension.

Applications may also enhance processing and off-line functionality by cashing the higher quality logotype data.

4. Logotype extension

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-logotypeInfo OBJECT IDENTIFIER  ::= {id-pe XX}
```

The logotype extension MUST have the following syntax:

```
LogotypeInfo ::= SEQUENCE {
   communityLogo     [0] LogotypeData OPTIONAL,
   issuerLogo        [1] LogotypeData OPTIONAL,
   subjectLogo       [2] LogotypeData OPTIONAL,
   otherLogos        [3] SEQUENCE OF OtherLogotypeData OPTIONAL }

OtherLogotypeData ::= SEQUENCE {
   logotypeTypeID    OBJECT IDENTIFIER,
   logotypeData      LogotypeData }

LogotypeData ::= SEQUENCE {
   highRes           LogotypeReference OPTIONAL,
   lowRes            EmbeddedLogotype OPTIONAL }

LogotypeReference ::= SEQUENCE {
   hashAlgorithm     AlgorithmIdentifier,
   logotypeHash      OCTET STRING,
   logotypeUri       IA5String }

EmbeddedLogotype ::= SEQUENCE {
```



```
   imageFileExtn     IA5String, -- MUST be "JPEG" or "JPG" or "GIF"
```

```
      image              OCTET STRING }
```

This extension MUST NOT be marked critical.

At least one of the optional elements in the LogotypeInfo structure MUST be present. Whenever possible, the use of otherLogos should be avoided.

The LogotypeReference structure explicitly identifies the one-way hash function employed. Implementations MUST support the SHA-1 [FIPS 180-1] algorithm, and implementations MAY support other one-way hash functions.

The predefined logotype types are:

Community Logotype. If communityLogo is present, the logotype MUST represent the community to which the certificate issuer is a member. The communityLogo MAY be present in an end entity certificate or an attribute certificate. The communityLogo MUST NOT be present in a CA certificate.

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 claimed by the issuer. The policy under which the issuer checks these logotypes is outside the scope of this standard.

Any URI pointing to a file containing the logotype data MUST include a file extension defining the image file format. The file extension is the last three or four letters of the file name, immediately following a period. Implementations MUST support both the JPEG and

GIF image formats. The JPEG image format MUST be identifier using a file extension of "JPG" or "JPEG". The GIF image format MUST be identified using the "GIF" file extension.

The same three file extension strings ("JPG," "JPEG," and "GIF") are used to identify the format of embedded images.

To ensure that certificates are not greatly enlarged by including embedded logotypes, restrictions are imposed on image size and color definition. Embedded images MUST NOT exceed 20 pixels by 20 pixels. Embedded images MUST use a 256-color (8-bit) palette. The size of an image conforming to these restrictions is about 750 octets.

5. Type of certificates

Logotypes MAY be present in three types of certificates:

- CA certificates
- End-entity certificates
- Attribute certificates

CA certificates include self-signed certificates (often used to represent trust anchors) or Intermediate CA certificates.

Some types of logotypes are not permitted in CA certificates. This ensures that logotypes are excludes from all aspects of certification path processing. As discussed above, logotypes are not intended to be part of certification path validation or any type of systematic processing. The sole purpose of logotypes is to enhance display of a particular certificate, regardless of its position in a certification path.

Logotypes MUST NOT be an active component in certification path processing, and they are included in public key certificates and attribute certificates at the discretion of the certificate issuer.

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 must trust 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. 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.

However, if the relying party software is unable to successfully validate a particular certificate, then it MUST NOT display any associated logotype graphics.

7. Security considerations

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.

The premise used for the logotype work is that logotype graphics in a certificate are trusted only if the certificate is successfully validated within a valid path. It is however impossible to prevent fraudulent creation of certificates by non-validated issuers, containing names and logotypes that the issuer has no claim to. Such

certificates could be created in an attempt to socially engineer a user into accepting a certificate. 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.

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 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 and severance pay 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. References

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

[OLD-PKIX-1] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet X.509 Public Key Infrastructure: Certificate and CRL Profile", January 1999.

[PKIX-1] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet X.509 Public Key Infrastructure: Certificate and CRL Profile", January 1999.
{Replace with Son-of-2459 as soon as it is published.}

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

9. Intellectual Property Rights

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 implementers 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.

APPENDICES

A. ASN.1 definitions

TBD

B. Logotype Placement

This Appendix documents reasons and rationales behind the technical solution selected in this standard.

Three alternatives for the placement of the logotypes in a certificate have been considered. They are:

1. Inclusion in a policy qualifier;
2. Inclusion in Issuer and Subject Alternative names extensions; and
3. Inclusion in a separate certificate extension.

B.1 Qualifier

This alternative would include logotype data as a newly defined policy qualifier.

Pros:

- This solution provides a mechanism to directly control the use and display of logotypes under a particular policy.

Cons:

- RFC <TBD> [PKIX-1] recommends against use of qualifiers.

- This is generally considered to be a major hack and stretch of semantics, since this type of data doesn't qualify a policy in any way.

B.2 Issuer and Subject Alt Names

This solution would use the other name form to include the issuer and community logotypes in the issuer alt name extension, and subject organization logo in the subject alt name extension.

Pros:

- This mechanism could possibly enable cross-certifying CAs to deny any subordinate CA the right to include logotypes in descending end entity certificates by listing the logotypes name form in excludedSubtrees.

Cons:

- Logotypes are not a name form and should not be treated as a displayable name.

- It is generally understood that it should be possible to apply general name constraint mechanisms (as described in RFC 2459 as well as RFC <TBD> [PKIX-1]) to names in the subject and issuer alt name extension. This is not possible to do with logotypes since it is not a name form.

- This split storage of logotype data into 2 different locations, which may make life worse for applications with no interest in logotypes.

- It is generally agreed that inclusion of logotype data by no means should be regarded as critical data. This may interfere with the criticality policy of the alt name extensions, especially if the certificate has no attributes in the subject field, forcing the subject alt name to be set to critical.

- This usage would possibly interfere with the resolution between IETF and ITU-T regarding use of permitted subtrees.

- Since this solution may break current implementations it would possibly block adoption of logotypes.

B.3 New extension

This solution places logotype data in a new extension.

Pros:

- This is the cleanest solution.

- This does not impact on legacy implementations.

Cons:

- This solution activates the issue whether this extension may be abused by a CA who include logotypes (in EE certificates) that violates the intention of a name constraints set by a chaining CA. This issue is addressed in the security consideration section below.

B.4 Conclusion

We must not destroy current structures. We must not create problems

or confusion.

Only the private extension solution satisfies both of these criteria. Therefore, the private extension was selected to carry logotype

information.

While the syntax and semantics of the X.509 public key certificate were used in this analysis, the logotype private extension can also be included in an X.509 attribute certificate.

C. Author Addresses

Stefan Santesson
AddTrust AB
P.O. Box 465
S-201 24 Malmoe
Sweden
stefan@addtrust.com

Russell Housley
RSA Laboratories
918 Spring Knoll Drive
Herndon, VA 20170
USA
rhousley@rsasecurity.com

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

D. Full Copyright Statement