Network Working Group
Request for Comments: 4630
Updates: 3280
Category: Standards Track

R. Housley
Vigil Security
S. Santesson
Microsoft

August 2006

Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Status of This Memo

Copyright Notice

Abstract

This document updates the handling of DirectoryString in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, which is published in RFC 3280. The use of UTF8String and PrintableString are the preferred encoding. The requirement for exclusive use of UTF8String after December 31, 2003 is removed.

Table of Contents

1. Introduction

At the time that RFC 3280 [PKIX1] was published, it was very unclear how international character sets ought to be supported. Implementation experience and deployment experience have made the picture much less fuzzy. This update to RFC 3280 aligns the document with this experience and the direction of the IETF PKIX Working Group.

The use of UTF8String and PrintableString are the preferred encoding. UTF8String provides support for international character sets, and PrintableString preserves support for the vast bulk of the certificates that have already been deployed.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [STDWORDS].

3. Update to RFC 3280, Section 4.1.2.4: Issuer

In Section 4.1.2.4, RFC 3280 says:

> The DirectoryString type is defined as a choice of PrintableString, TeletexString, BMPString, UTF8String, and UniversalString. The UTF8String encoding [RFC 2279] is the preferred encoding, and all certificates issued after December 31, 2003 MUST use the UTF8String encoding of DirectoryString (except as noted below). Until that date, conforming CAs MUST choose from the following options when creating a distinguished name, including their own:
>
> (a) if the character set is sufficient, the string MAY be represented as a PrintableString;
>
> (b) failing (a), if the BMPString character set is sufficient the string MAY be represented as a BMPString; and
>
> (c) failing (a) and (b), the string MUST be represented as a UTF8String. If (a) or (b) is satisfied, the CA MAY still choose to represent the string as a UTF8String.

Exceptions to the December 31, 2003 UTF8 encoding requirements are as follows:

(a) CAs MAY issue "name rollover" certificates to support an orderly migration to UTF8String encoding. Such certificates would include the CA's UTF8String encoded name as issuer and the old name encoding as subject, or vice-versa.

(b) As stated in section 4.1.2.6, the subject field MUST be populated with a non-empty distinguished name matching the contents of the issuer field in all certificates issued by the subject CA regardless of encoding.

The TeletexString and UniversalString are included for backward compatibility, and SHOULD NOT be used for certificates for new subjects. However, these types MAY be used in certificates where the name was previously established. Certificate users SHOULD be prepared to receive certificates with these types.

In addition, many legacy implementations support names encoded in the ISO 8859-1 character set (Latin1String) [ISO 8859-1] but tag them as TeletexString. TeletexString encodes a larger character set than ISO 8859-1, but it encodes some characters differently. Implementations SHOULD be prepared to handle both encodings.

This block of text is replaced with the following:

The DirectoryString type is defined as a choice of PrintableString, TeletexString, BMPString, UTF8String, and UniversalString. CAs conforming to this profile MUST use either the PrintableString or UTF8String encoding of DirectoryString, with one exception. When CAs have previously issued certificates with issuer fields with attributes encoded using the TeletexString, BMPString, or UniversalString, the CA MAY continue to use these encodings of the DirectoryString to preserve the backward compatibility.

4. Update to RFC 3280, Section 4.1.2.6: Subject

In Section 4.1.2.6, RFC 3280 says:

The subject name field is defined as the X.501 type Name. Implementation requirements for this field are those defined for the issuer field (section 4.1.2.4). When encoding attribute values of type DirectoryString, the encoding rules for the issuer field MUST be implemented.

This block of text is replaced with the following:

> The subject name field is defined as the X.501 type Name. Implementation requirements for this field are those defined for the issuer field (Section 4.1.2.4). CAs conforming to this profile MUST use either the PrintableString or UTF8String encoding of DirectoryString, with one exception. When CAs have previously issued certificates with subject fields with attributes encoded using the TeletexString, BMPString, or UniversalString, the CA MAY continue to use these encodings of the DirectoryString in new certificates for the same subject to preserve backward compatibility.
>
> Since name comparison assumes that attribute values encoded in different types (e.g., PrintableString and UTF8String) are assumed to represent different strings, any name components that appear in both the subject field and the issuer field SHOULD use the same encoding throughout the certification path.

5. Update to RFC 3280, Section 4.2.1.7: Subject Alternative Name

In Section 4.2.1.7, RFC 3280 says:

> When the subjectAltName extension contains a DN in the directoryName, the DN MUST be unique for each subject entity certified by the one CA as defined by the issuer name field. A CA MAY issue more than one certificate with the same DN to the same subject entity.

This block of text is replaced with the following:

> When the subjectAltName extension contains a DN in the directoryName, the encoding preference is defined in Section 4.1.2.4. The DN MUST be unique for each subject entity certified by the one CA as defined by the issuer name field. A CA MAY issue more than one certificate with the same DN to the same subject entity.

6. Security Considerations

The use of consistent encoding for name components will ensure that the name constraints specified in [PKIX1] work as expected.

When strings are mapped from internal representations to visual representations, sometimes two different strings will have the same or similar visual representations. This can happen for many different reasons, including the use of similar glyphs and use of composed characters (such as e + ’ equaling U+00E9, the Korean

composed characters, and vowels above consonant clusters in certain languages). As a result of this situation, people doing visual comparisons between to different names may think they are the same when in fact they are not. Also, people may mistake one string for another. Issuers of certificates and relying parties both need to be aware of this situation.

7. Normative References

[PKIX1] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

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

Authors' Addresses

Russell Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA

EMail: housley@vigilsec.com

Stefan Santesson
Microsoft
Tuborg Boulevard 12
2900 Hellerup
Denmark

EMail: stefans@microsoft.com

Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).