INTERNET-DRAFT D. Cooper
Intended Status: Proposed Standard NIST
Updates: 5280 (if approved) November 20, 2009
Expires: May 24, 2010

Clarifications to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile <draft-cooper-pkix-rfc5280-clarifications-00.txt>

Status of this Memo

Copyright and License Notice

Abstract

This document updates the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, which is published in RFC 5280. This document changes the set of acceptable encoding methods for the explicitText field of the user notice policy qualifier and clarifies the rules for converting internationalized domain name labels to ASCII.

Table of Contents

1. Introduction 2
   1.1. Terminology 3
2. Update to RFC 5280, Section 4.2.1.4: Certificate Policies . . . 3
3. Update to RFC 5280, Section 7.3: Internationalized Domain Names in Distinguished Names 4
4. Security Considerations 5
5. IANA Considerations 5
6. References 5
   6.1. Normative References 5
   6.2. Informative References 5
Author's Address 5

1. Introduction

This document updates the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [RFC5280].

The ASN.1 [X.680] syntax for the user notice certificate policy qualifier allows for the explicitText field to be encoded using one of four possible encoding methods: IA5String, VisibleString, BMPString, and UTF8String. RFC 5280 permits certification authorities (CA) to encode strings in the explicitText field as either UTF8String or IA5String while forbiding the use of VisibleString and BMPString. However, after RFC 5280 was published, an examination of existing certificates found that the VisibleString encoding was commonly used. This document brings the requirements into closer alignment with existing practice by stating that the explicitText field may be encoded in either UTF8String or VisibleString while forbidding the use of IA5String and BMPString.

Section 7.3 of RFC 5280 specifies rules for converting internationalized domain name labels that are to appear in a domainComponent attribute to ASCII. The conversion process specified in RFC 5280 did not specify that the "UseSTD3ASCIIRules" flag needed to be set. This document modifies the conversion process specified

in Section 7.3 of RFC 5280 to clarify that "UseSTD3ASCIIRules" flag should be set. The result of this is to indicate that the check for conformance to [RFC1123] should be performed.

1.1. 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 [RFC2119].

2. Update to RFC 5280, Section 4.2.1.4: Certificate Policies

RFC 5280, Section 4.2.1.4, the tenth paragraph says:

```
|     An explicitText field includes the textual statement directly in
|     the certificate.  The explicitText field is a string with a
|     maximum size of 200 characters.  Conforming CAs SHOULD use the
|     UTF8String encoding for explicitText, but MAY use IA5String.
|     Conforming CAs MUST NOT encode explicitText as VisibleString or
|     BMPString.  The explicitText string SHOULD NOT include any control
|     characters (e.g., U+0000 to U+001F and U+007F to U+009F).  When
|     the UTF8String encoding is used, all character sequences SHOULD be
|     normalized according to Unicode normalization form C (NFC) [NFC].
```

This paragraph is replaced with:

```
|     An explicitText field includes the textual statement directly in
|     the certificate.  The explicitText field is a string with a
|     maximum size of 200 characters.  Conforming CAs SHOULD use the
|     UTF8String encoding for explicitText, but MAY use VisibleString.
|     Conforming CAs MUST NOT encode explicitText as IA5String or
|     BMPString.  The explicitText string SHOULD NOT include any control
|     characters (e.g., U+0000 to U+001F and U+007F to U+009F).  When
|     the UTF8String encoding is used, all character sequences SHOULD be
|     normalized according to Unicode normalization form C (NFC) [NFC].
```

3. Update to RFC 5280, Section 7.3: Internationalized Domain Names in Distinguished Names

RFC 5280, Section 7.3, the first paragraph says:

> Domain Names may also be represented as distinguished names using domain components in the subject field, the issuer field, the subjectAltName extension, or the issuerAltName extension. As with the dNSName in the GeneralName type, the value of this attribute is defined as an IA5String. Each domainComponent attribute represents a single label. To represent a label from an IDN in the distinguished name, the implementation MUST perform the "ToASCII" label conversion specified in Section 4.1 of RFC 3490. The label SHALL be considered a "stored string". That is, the AllowUnassigned flag SHALL NOT be set.

This paragraph is replaced with:

> Domain Names may also be represented as distinguished names using domain components in the subject field, the issuer field, the subjectAltName extension, or the issuerAltName extension. As with the dNSName in the GeneralName type, the value of this attribute is defined as an IA5String. Each domainComponent attribute represents a single label. To represent a label from an IDN in the distinguished name, the implementation MUST perform the "ToASCII" label conversion specified in Section 4.1 of RFC 3490 with the UseSTD3ASCIIRules flag set. The label SHALL be considered a "stored string". That is, the AllowUnassigned flag SHALL NOT be set. The conversion process is the same as is performed in step 4 in Section 7.2.

4. Security Considerations

This document introduces no new security considerations.

5. IANA Considerations

This document has no actions for IANA.

6. References

6.1. Normative References

[RFC1123] Braden, R., Ed., "Requirements for Internet Hosts -- Application and Support", STD 3, RFC 1123, October 1989.

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

[RFC5280] Cooper, D., S. Santesson, S. Farrell, S. Boeyen, R. Housley and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

6.2. Informative References

[X.680] ITU-T Recommendation X.680 (2002) | ISO/IEC 8824-1:2002, Information Technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation.

[NFC] Davis, M. and M. Duerst, "Unicode Standard Annex #15: Unicode Normalization Forms", October 2006, <http://www.unicode.org/reports/tr15/>.

Author's Address

David Cooper
National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8930
Gaithersburg, MD 20899-8930
USA

EMail: david.cooper@nist.gov