INTERNET-DRAFT
Intended Status: Proposed Standard
Updates: 5280 (if approved)
Expires: February 17, 2013

P. Yee
AKAYLA

August 16, 2012

Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile <draft-ietf-pkix-rfc5280-clarifications-08.txt>

Status of this Memo

Copyright and License Notice

Abstract

This document updates RFC 5280, the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. 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. This document also provides some clarifications on the use of self-signed certificates, trust anchors, and some updated security considerations.

Table of Contents

1. Introduction

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

This document makes a recommendation that self-signed certificates used to convey trust anchor data be marked as CA certificates, which is not always current practice.

The acceptable and unacceptable encodings for the explicitText field of the user notice policy qualifier are updated to bring them in line with existing practice.

The use of self-signed certificates as trust anchors in Section 6.2 is clarified. While it is optional to use additional information in these certificates in the path validation process, [RFC5937] is noted

as providing guidance in that regard.

The Section 7.3 rules for ASCII encoding of Internationalized Domain Names (IDN) as Distinguished Names are aligned with the rules in Section 7.2 which govern IDN encoding as GeneralNames.

In light of some observed attacks, the Security Considerations now give added depth to the consequences of CA key compromise. This section additionally notes that collision resistance is not a required property of one-way hash functions when used to generate key identifiers.

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 3.2: Certification Paths and Trust

Add the following paragraph to the end of RFC 5280, Section 3.2:

| Consistent with Section 3.4.61 of X.509 (11/2008) [X.509] we note
| that use of self-issued certificates and self-signed certificates
| issued by other than CAs are outside the scope of this specification.
| Thus, for example, a web server or client might generate a self-
| signed certificate to identify itself. These certificates, and how a
| relying party uses them to authenticate asserted identities, are
| both outside the scope of RFC 5280.

3. 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 or
| BMPString. Conforming CAs MUST NOT encode explicitText as
| IA5String. 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 or BMPString encoding is used, all character
| sequences SHOULD be normalized according to Unicode normalization
| form C (NFC) [NFC].

4. Update to RFC 5280, Section 6.2: Using the Path Validation Algorithm

RFC 5280, Section 6.2, the third paragraph says:

| Where a CA distributes self-signed certificates to specify trust
| anchor information, certificate extensions can be used to specify
| recommended inputs to path validation. For example, a policy
| constraints extension could be included in the self-signed
| certificate to indicate that paths beginning with this trust anchor
| should be trusted only for the specified policies. Similarly, a name
| constraints extension could be included to indicate that paths
| beginning with this trust anchor should be trusted only for the
| specified name spaces. The path validation algorithm presented in
| Section 6.1 does not assume that trust anchor information is provided
| in self-signed certificates and does not specify processing rules for
| additional information included in such certificates.
| Implementations that use self-signed certificates to specify trust
| anchor information are free to process or ignore such information.

This paragraph is replaced with:

| Where a CA distributes self-signed certificates to specify trust
| anchor information, certificate extensions can be used to specify
| recommended inputs to path validation. For example, a policy
| constraints extension could be included in the self-signed
| certificate to indicate that paths beginning with this trust anchor
| should be trusted only for the specified policies. Similarly, a name
| constraints extension could be included to indicate that paths
| beginning with this trust anchor should be trusted only for the
| specified name spaces. The path validation algorithm presented
| in Section 6.1 does not assume that trust anchor information is
| provided in self-signed certificates and does not specify processing
| rules for additional information included in such certificates.
| However, [RFC5914] defines several formats for representing trust
| anchor information, including self-signed certificates, and [RFC5937]
| provides an example of how such information may be used to initialize
| the path validation inputs. Implementations are free to make use of
| any additional information that is included in a trust anchor
| representation, or to ignore such information.

5. 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.

6. Security Considerations

This document modifies the Security Considerations section of RFC 5280 as follows. The fifth paragraph of the Security Considerations section of RFC 5280 says:

> The protection afforded private keys is a critical security factor. On a small scale, failure of users to protect their private keys will permit an attacker to masquerade as them or decrypt their personal information. On a larger scale, compromise of a CA's private signing key may have a catastrophic effect. If an attacker obtains the private key unnoticed, the attacker may issue bogus certificates and CRLs. Existence of bogus certificates and CRLs will undermine confidence in the system. If such a compromise is detected, all certificates issued to the compromised CA MUST be revoked, preventing services between its users and users of other CAs. Rebuilding after such a compromise will be problematic, so CAs are advised to implement a combination of strong technical measures (e.g., tamper-

| resistant cryptographic modules) and appropriate management
| procedures (e.g., separation of duties) to avoid such an incident.

This paragraph is replaced with:

| The protection afforded private keys is a critical security factor.
| On a small scale, failure of users to protect their private keys will
| permit an attacker to masquerade as them or decrypt their personal
| information. On a larger scale, compromise of a CA's private signing
| key may have a catastrophic effect.
|
| If an attacker obtains the private key of a CA unnoticed, the
| attacker may issue bogus certificates and CRLs. Even if an attacker
| is unable to obtain a copy of a CA's private key, the attacker may be
| able to issue bogus certificates and CRLs by making unauthorized use
| of the CA's workstation or of an RA's workstation. Such an attack
| may be the result of an attacker obtaining unauthorized access to the
| workstation, either locally or remotely, or may be the result of
| inappropriate activity by an insider. Existence of bogus
| certificates and CRLs will undermine confidence in the system. Among
| many other possible attacks, the attacker may issue bogus
| certificates that have the same subject names as legitimate
| certificates in order impersonate legitimate certificate subjects.
| This could include bogus CA certificates in which the subject names
| in the bogus certificates match the names under which legitimate CAs
| issue certificates and CRLs. This would allow the attacker to issue
| bogus certificates and CRLs that have the same issuer names, and
| possibly the same serial numbers, as certificates and CRLs issued by
| legitimate CAs.

The following text is added to the end of the Security Considerations section of 5280:

One-way hash functions are commonly used to generate key identifier values (AKI and SKI), e.g., as described in Sections 4.1.1 and 4.1.2. However, none of the security properties of such functions are required for this context.

7. IANA Considerations

This document has no actions for IANA.

8. References

8.1. Normative References

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

[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, May 2008.

[RFC5914] Housley, R., Ashmore, S., and C. Wallace, "Trust Anchor Format", RFC 5914, June 2010.

[X.509] ITU-T Recommendation X.509 (2008) | ISO/IEC 9594-8:2008, Information Technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks

8.2. Informative References

[RFC5937] Ashmore, S. and C. Wallace, "Using Trust Anchor Constraints during Certification Path Processing", RFC 5937, August 2010.

[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/>.

9. Acknowledgements

David Cooper is acknowledged for his fine work in editing versions 00 through 04 of this document.

Author's Address

Peter E. Yee
AKAYLA
7150 Moorland Drive
Clarksville, MD 21029
USA

EMail: peter@akayla.com