Implementation Report for the Public Key Infrastructure Certificate
and Certificate Revocation List (CRL) Profile RFC 5280
<draft-cooper-pkix-rfc5280-impl-report-01.txt>

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the
provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering
Task Force (IETF), its areas, and its working groups. Note that
other groups may also distribute working documents as
Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months
and may be updated, replaced, or obsoleted by other documents at any
time. It is inappropriate to use Internet-Drafts as reference
material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html

Copyright and License Notice

Copyright (c) 2010 IETF Trust and the persons identified as the
document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal
Provisions Relating to IETF Documents
(http://trustee.ietf.org/license-info) in effect on the date of
publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.
Abstract

This is an implementation report of RFC 5280 for the purpose of advancing the document to Draft Standard.

Table of Contents

1. Introduction ................................................. 2
2. Summary ................................................... 2
3. Methodology ............................................... 3
4. Exceptions ................................................. 3
5. Details ..................................................... 4
   5.1. Certificate and CRL Issuers ......................... 4
   5.2. Certificate and CRL Processing ...................... 5
6. Security Considerations ................................. 6
7. IANA Considerations ....................................... 6
8. References ................................................. 6
   8.1. Normative References ............................... 6
   8.2. Informative References .............................. 6
Author’s Address ........................................... 7

1. Introduction

This is an implementation report of the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile [RFC5280]. It follows the outline suggested by [RFC5657].

2. Summary

RFC 5280 specifies a profile of the X.509 certificate and CRL formats [X.509]. The X.509 certificate and CRL formats are in widespread use and there are many different certification authority (CA) products that can issue X.509 certificates and CRLs and many different path validation implementations that can process X.509 certificates and CRLs. Most CAs use the RFC 5280 profile as the basis for defining the profiles under which they issue certificates and CRLs.

X.509, and thus RFC 5280, certificate and CRL validation is implemented in Web browsers, to support server authenticated TLS [RFC5246], email clients, to support S/MIME [RFC5750], IPsec clients [RFC4306], and in many other types of applications. In addition to the many different vendors who issue TLS-server certificates, millions of certificates have been issued by corporations and government agencies to their employees to support authentication.

Interoperability of RFC 5280 clients and servers has been
demonstrated in practice through the successful, widespread use of X.509 certificates to support server authentication in HTTP over TLS. TLS server certificates that are in widespread use have been issued by many different vendors, using different CA products, and these certificates are validated by several different Web browsers that use different certification path validation libraries.

3. Methodology

In order to verify that the requirements for advancing RFC 5280 to Draft Standard have been satisfied, efforts were made to find certificates and CRLs, issued by different CAs, that included each of the features described in RFC 5280 and path validation libraries were tested to verify that they could process each of the features described in RFC 5280.

For CAs, the goal was to ensure that the certificates and CRLs were issued in conformance with the RFC 5280 profile. Whenever possible, certificates that were in actual deployment were used. These certificates were found by visiting TLS protected web sites and downloading the certificates and CRLs needed to authenticate the web server and by extracting certificates from signed emails. When no such certificates or CRLs could be found that included a certain feature, certificates or CRLs including the feature were created using two different CA products.

The Public Key Interoperability Test Suite [PKITS] was used to verify that certification path validation libraries correctly implemented the features of RFC 5280. For features of RFC 5280 that were not covered by PKITS, new certification paths were created and were tested against at least two independent implementations.

4. Exceptions

While interoperable implementations of almost every feature in RFC 5280 were identified, there were a few features for which no implementations could be found.

The main feature for which implementations could not be found was the processing rules for internationalized names in Section 7 of RFC 5280. These processing rules are new in RFC 5280. The predecessors to RFC 5280, RFC 2459 and RFC 3280, did not require implementations to be able to process internationalized names, and interoperable implementations have been found for the more limited name processing rules specified in RFC 3280. In practice, the inability of clients to normalize internationalized names before comparison has not created any interoperability problems since CAs follow the RFC 5280 requirement to encode names in exactly the same way wherever they
appear, allowing clients to obtain the correct results even if they use a simple binary comparison rule rather than normalizing the names before comparison.

None of the production CAs whose certificates were obtained were issuing indirect CRLs, and an inquiry to the PKIX mail list only identified one CA implementation that is capable of issuing indirect CRLs. However, two independently implemented path validation libraries were found that can correctly process indirect CRLs. Since indirect CRLs are a feature of X.509, and RFC 5280 merely describes how indirect CRLs should be issued and processed, without encouraging their use, it is believed that the description of indirect CRLs should remain in the certificate and CRL profile even though multiple independent CA implementations of indirect CRLs were not identified.

The user notice certificate policy qualifier allows for user notice text to be encoded using one of four string types: IA5String, VisibleString, BMPString, and UTF8String. While RFC 2459 and RFC 3280 provided no guidance on the selection of an encoding, RFC 5280 requires that user notice text be encoded in either UTF8String or IA5String. During the search for interoperable implementations, several Web server and email client certificates were located that included user notices, but they all encoded the user notices using the VisibleString type. A few people also noted that at least one CA product encoded user notice text in BMPString. Therefore, an update to RFC 5280 (RFC5280u) is being developed that permits user notices to be encoded as VisibleString or BMPString.

5. Details

5.1. Certificate and CRL Issuers

The ability of CAs to issue certificates and CRLs in conformance with RFC 5280 was determined primarily by examining certificates that were issued for use in production environments. By connecting to Web sites using HTTPS [RFC2818], intermediate certificates, end entity certificates, and CRLs were obtained from America Online, beTRUSTed, Entrust, Microsoft, Starfield Technologies, and VeriSign. From signed S/MIME [RFC5750] messages sent to the PKIX and S/MIME mail lists, certificates and CRLs were obtained from America Online, Ascertia, Dartmouth College, EdelWeb, Entrust, Izecon, Microsoft, MITRE, TC TrustCenter, Thawte, the U.S. Department of Defense, and VeriSign. Finally, CA certificates and CRLs were also obtained from the online directory of the U.S. Federal Public Key Infrastructure. While the CA product used to issue these certificates could not always be determined, it is known that at least five different CA products were used to issue these certificates: Entrust, Microsoft, Red Hat, RSA, and VeriSign.
Through this method, independent implementations of most of the certificate and CRL extensions profiled in RFC 5280 were located. Other than the exceptions mentioned in Section 4, the primary feature for which implementations were not located using this method was delta-CRLs. However, a survey of the PKIX working group led to the identification of two CAs, EJCBA and OpenSSL, that are capable of issuing delta-CRLs. The CA that is part of Microsoft Windows Server can also issue delta-CRLs.

As would be expected, no production certificates or CRLs were found with dates encoded in GeneralizedTime, since RFC 5280 requires all dates between 1950 and 2049 to be encoded in UTCTime. However, certificates and CRLs were generated using both Network Security Services (NSS) and OpenSSL with dates after 2049 that were encoded in GeneralizedTime.

5.2. Certificate and CRL Processing

The Public Key Interoperability Test Suite [PKITS] was designed to provide test coverage for most of the features described in RFC 3280, the predecessor to RFC 5280. Thus, PKITS covers most of the features of RFC 5280, with the exception of Section 7, Processing Rules for Internationalized Names. PKITS contains over 200 test, prospective certification paths designed to verify that certification path validation libraries can correctly process the different fields that may appear in a certificate or CRL. PKITS includes several tests designed to verify that path validation libraries can correctly process the basic fields in certificates and CRLs, such as the issuer and subject fields and the validity dates, but most of the tests deal with the certificate and CRL extensions that are profiled in RFC 5280 that must be processed as part of certification path validation.

In 2005 and 2006, the Path Discovery and Validation Working Group (http://www.idmanagement.gov/fpkia/drilldown.cfm?action=pdval_wg) tested nine certification path validation products from five different vendors using PKITS in accordance with the testing procedures specified in the Draft NIST Recommendation for X.509 Path Validation [NISTREQ]. The products tested were (1) TrustEnabler from Gemini Security Solutions, (2) Webcullis from Orion Security Solutions, (3) PathBuilder 1.0 from CoreStreet, (4) Desktop Validator 5.0 and Validation Authority 5.0 from Tumbleweed Communications, and (5) TruePass 8.0 SP1, Java Toolkit 7.1 SP1, GetAccess 7.1 SP2, and Verification Server 7.1 from Entrust. Detailed results from the testing of all of these products can be found on the Path Discovery and Validation Working Group’s Qualified Validation List [QVL].

For features that were not covered by PKITS or that were not tested as part of the process of qualifying for inclusion on the [QVL], new
certification paths were created and two independent implementations of each of the features were located. For most of these tests, Network Security Services (NSS), via either Mozilla Thunderbird or Mozilla Firefox, and OpenSSL were used. However, for a few tests either Safari or the Certificate Management Library was used as the second implementation of the feature. Features that were not covered by PKITS for which new certification paths were created included version 1 and 2 certificates, certificates with names encoded in BMPString and UniversalString, certificates with extended key usage extensions, certificates with critical certificatePolicies extensions, certificates that imposed name constraints on IP addresses, certificates with nameConstraints extensions for which the minimum and maximum fields were present, certification paths in which name constraints were imposed on uniform resource identifiers and end entity certificates included URIs that either did not have an authority component or had an authority component with an IP address, certificates with critical policyConstraints extensions in which only the inhibitPolicyMapping field was present, and CRLs with thisUpdate and nextUpdate encoded as GeneralizedTime.

6. Security Considerations

This document introduces no new security considerations.

7. IANA Considerations

This document has no actions for IANA.

8. References

8.1. Normative References


8.2. Informative References


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