Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 12, 2015

S. Leonard
Penango, Inc.

September 8, 2014

URI Fragment Identifiers for the application/pkix-cert Media Type draft-seantek-certfrag-00

Abstract

This memo describes Uniform Resource Identifier (URI) fragment identifiers for PKIX certificates, which are identified with the Internet media type application/pkix-cert.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on March 12, 2015.

Copyright Notice

1. Fragment

A digital certificate [RFC5280] is comprised of parts that are of interest to particular users and applications. For example, a user agent may wish to draw attention to the "notAfter" time for an expired certificate. Uniform Resource Indicators (URIs) can include fragment identifiers to identify such sub-parts of a resource; see Section 3.5 of [RFC3986]. However, the semantics of fragment identifiers depend upon the Internet media type [RFC2046], not the URI scheme. Therefore, the fragment identifiers in this memo apply to the application/pkix-cert Internet media type [RFC2585]. The following fragments are hereby defined:

Identifier	Certificate Part (ASN.1 identifier)
v	tbsCertificate.version
sn	tbsCertificate.serialNumber
sig	tbsCertificate.signature; also signatureAlgorithm
issuer	tbsCertificate.issuer
nb	tbsCertificate.validity.notBefore
na	tbsCertificate.validity.notAfter
subject	tbsCertificate.subject
spki	tbsCertificate.subjectPublicKeyInfo
ext	tbsCertificate.extensions
ext:<OID>	tbsCertificate.extensions {Extension matching extoid == extnID}*
sigval	signatureValue

* The particular extension in the Extensions "SEQUENCE" is identified by OID only; there are no textual identifiers. The syntax of the <OID> matches the "numericoid" production of [RFC4512].

Table 1: Certificate Parts and Fragments

The fragments defined in the table above are case-insensitive. However, a generator that complies with this memo MUST produce the fragment identifiers with the exact casing as provided above. The table is not exhaustive: should additional identifiers be required, a future document may specify additional identifiers.

The key word "MUST" in this document is to be interpreted as described in RFC 2119 [RFC2119].

2. IANA Considerations

IANA needs to add a reference to this specification in the application/pkix-cert media type registration.

Additionally, the registration template needs to be updated to add the following section:

Fragment identifier considerations: Fragment identification is supported by using fragment identifiers as specified by this memo.

3. Security Considerations

Digital certificates are important building blocks for authentication, integrity, authorization, and (occasionally) confidentiality services. Accordingly, identifying digital certificates incorrectly can have significant security ramifications.

A URI that identifies a certificate will likely be used by an application or user for some security-related service, such as to retrieve the certificate as part of a validation procedure. When a fragment identifies a part of a certificate, the application will define the behavioral semantics. A certificate displaying application might zoom in on that aspect of the certificate, while a public key-processing application might use a fragment identifier like "#spki" to extract the "SubjectPublicKeyInfo" structure for further processing. Interpreting these identifiers incorrectly may cause denial-of-service attacks.

4. Normative References

[RFC2046] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, November 1996.

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

[RFC2585] Housley, R. and P. Hoffman, "Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP", RFC 2585, May 1999.

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[RFC4512] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP): Directory Information Models", RFC 4512, June 2006.

[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.

Author's Address

Sean Leonard
Penango, Inc.
5900 Wilshire Boulevard
21st Floor
Los Angeles, CA 90036
USA

Email: dev+ietf@seantek.com
URI: http://www.penango.com/