Internet Engineering Task Force (IETF)
Request for Comments: 5877
Category: Informational
ISSN: 2070-1721

R. Housley
Vigil Security

May 2010

The application/pkix-attr-cert Media Type for Attribute Certificates

Abstract

This document specifies a MIME media type used to carry a single attribute certificate as defined in RFC 5755.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5877.

1. Introduction

RFC 2585 [RFC2585] defines the MIME media types for public key certificates and certificate revocation lists (CRLs). This document specifies a MIME media type for use with attribute certificates as defined in RFC 5755 [RFC5755].

Attribute certificates are ASN.1 encoded [X.680]. RFC 5755 [RFC5755] tells which portions of the attribute certificate must use the distinguished encoding rules (DER) [X.690] and which portions are permitted to use the basic encoding rules (BER) [X.690]. Since DER is a proper subset of BER, BER decoding all parts of a properly constructed attribute certificate will be successful.

2. IANA Considerations

This document registers with IANA the "application/pkix-attr-cert" Internet Media Type for use with an attribute certificate as defined in [RFC5755]. This registration follows the procedures defined in BCP 13 [RFC4288].

Type name: application

Subtype name: pkix-attr-cert

Required parameters: None

Optional parameters: None

Encoding considerations: binary

Security considerations:
An attribute certificate provides authorization information. An attribute certificate is most often used in conjunction with a public key certificate [RFC5280], and the two certificates should use the same encoding of the distinguished name as described in the Security Considerations of this document.

Interoperability considerations:
The media type will be used with HTTP to fetch attribute certificates. Other uses may emerge in the future.

Published specification: RFC 5755

Applications that use this media type:
The media type is used with a MIME-compliant transport to transfer an attribute certificate. Attribute certificates convey authorization information, and they are most often used in conjunction with public key certificates as defined in [RFC5280].

Additional information:
Magic number(s): None
File extension(s): .ac
Macintosh File Type Code(s): none

Person & email address to contact for further information:
Russ Housley
housley@vigilsec.com

Intended usage: COMMON

Restrictions on usage: none

Author:
Russ Housley <housley@vigilsec.com>

Intended usage: COMMON

Change controller:
The IESG <iesg@ietf.org>

3. Security Considerations

Attribute certificate issuers must encode the holder entity name in exactly the same way as the public key certificate distinguished name. If they are encoded differently, implementations may fail to recognize that the attribute certificate and public key certificate belong to the same entity.

4. References

4.1. Normative References

[RFC5755] Farrell, S., Housley, R., and S. Turner, "An Internet Attribute Certificate Profile for Authorization", RFC 5755, January 2010.

4.2. Informative References

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

[RFC4288] Freed, N. and J. Klensin, "Media Type Specifications and Registration Procedures", BCP 13, RFC 4288, December 2005.

[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.

[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.

[X.690] ITU-T Recommendation X.690 (2002) | ISO/IEC 8825-1:2002, Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

Author’s Address

Russell Housley
Vigil Security, LLC
918 Spring Knoll Drive
Herndon, VA 20170
USA
EMail: housley@vigilsec.com