INTERNET DRAFT R. Housley
Intended Status: Informational Vigil Security
Expires: 15 March 2010 11 September 2009

The application/pkix-attr-cert Content Type for Attribute Certificates
<draft-ietf-pkix-attr-cert-mime-type-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 Notice

Copyright (c) 2009 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 in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

This document specifies a MIME content type used to carry a single attribute certificate as defined in RFC 3281.

1. Introduction

RFC 2585 [RFC2585] defines the MIME content types for public key certificates and certificate revocation lists (CRLs). This document specifies a MIME content type for use with attribute certificates as defined in RFC 3281 [RFC3281].

Attribute certificates are ASN.1 encoded [X.680]. RFC 3281 [RFC3281] 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

The content type for an attribute certificate is application/pkix-attr-cert.

Type name: application

Subtype name: pkix-attr-cert

Required parameters: None

Optional parameters: None

Encoding considerations:
In most cases, the encoding will be binary. When the transport (such as SMTP) does not accommodate an unrestricted sequence of octets, the attribute certificate will be Base64 encoded [RFC4648].

Security considerations:
An attribute certificate provides authorization information. An attribute certificate is most often used in conjunction with 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 content type will be used with HTTP to fetch attribute certificates. Other uses may emerge in the future.

Published specification: RFC 3281

Applications which use this media type:
The content type is used with MIME-complaint transport to

transfer an attribute certificate. Attribute certificates convey authorization information, and they are most often used in conjunction with public key certificates [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

[RFC3281] S. Farrell, S., and R. Housley, "An Internet Attribute Certificate Profile for Authorization", RFC 3281, April 2002.

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.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006.

[RFC5280] Cooper, D., S. Santesson, S. Farrell, S. Boeyen, R. Housley, 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).

Authors' Addresses

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