

Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: December 23, 2012

D. Harkins, Ed.
Aruba Networks
S. Turner, Ed.
IECA, Inc
June 21, 2012

The application/csrattrs Media Type
draft-harkins-application-csrattrs-media-type-00

Abstract

This document specifies a media type used by Certification Authorities (CAs) to indicate which attributes a client should include in their Certification Request-- a PKCS#10 Certificate Signing Request (CSR)-- when using Enrollment over Secure Transport (EST).

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#). This document may not be modified, and derivative works of it may not be created, except to format it for publication as an RFC or to translate it into languages other than English.

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 December 23, 2012.

Copyright Notice

Copyright (c) 2012 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.

Table of Contents

1.	Introduction	3
1.1.	Requirements Language	3
1.2.	Terminology	3
2.	Distribution of Attributes	3
3.	Format of the application/csrattrs Body	4
4.	Receipt of the application/csrattrs Body	5
5.	IANA Considerations	5
6.	Security Considerations	7
7.	References	7
7.1.	Normative References	7
7.2.	Informative References	8
	Authors' Addresses	8

1. Introduction

Enrollment over Secure Transport [[EST](#)] defines a Certificate enrollment protocol that allows client to generate certification request and transmit it to a server acting as a Certification Authority (CA) or Registration Authority (RA). The CA then issues a Certificate based on the certification request.

In some cases, the CA may want to include client-provided attributes in certificates it issues. These attributes may describe information that is not available to the CA, for instance the MAC address of a client's wireless interface might be needed in a certificate used to gain access to a wireless medium. The media type described here allows the server to inform the client of a (set of) attribute(s) to include, if possible, in its certification request.

This document defines a URI [[RFC3986](#)] that can be used with Enrollment over Secure Transport (EST) protocol [[EST](#)].

1.1. Requirements Language

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](#)].

1.2. Terminology

The reader is assumed to be familiar with the terms and concepts of [[EST](#)] and [[RFC2986](#)].

Attribute

Any kind of identifying information that can be added to a certification request.

2. Distribution of Attributes

Attribute request messages MUST be sent through the TLS-protected channel [[RFC5246](#)] established as part of the [[EST](#)] protocol.

The request MUST be made with an HTTPS GET message to the common path to the EST server-- referred to as BASEPATH-- with an OPERATIONPATH extension of '/csrattrs'. For example, if BASEPATH had the value arbitrary/base then an example URI would be:

`https://example.org/arbitrary/base/csrattrs`

The server MUST reply to the client's HTTPS message with a (set of)

attribute(s). Responses to attribute request messages MUST be encoded as content type "application/csrattrs".

3. Format of the application/csrattrs Body

The syntax for application/csrattrs body is as follows:

```
Csrattrs ::= SEQUENCE SIZE (0..MAX) OF OBJECT IDENTIFIER { }
```

A robust application SHOULD output Distinguished Encoding Rules (DER) ([X.690]) but MAY use Basic Encoding Rules (BER) ([X.680]). Data produced by DER or BER is 8-bit. When the transport for the application/csrattrs is limited to 7-bit data, a suitable transfer encoding MUST be applied in MIME-compatible transports, the base64 encoding (section 4 of [RFC4648]) SHOULD be used with application/csrattrs, although any 7-bit transfer encoding may work.

Clients MUST encode csrattrs as an empty SEQUENCE OF. That is, no object identifiers are included when the client creates an application/csrattrs media type. For example, it would produce an ASN.1 SEQUENCE:

```
30 00
```

and then base64 encode that ASN.1 SEQUENCE OF nothing to produce:

```
MA==
```

The resulting request would look like this:

```
Content-Type: application/csrattrs; name=attributes
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=attributes
```

```
MA==
```

Servers include zero or more object identifiers that they wish the client to include in their certification request. When the server encodes csrattrs as an empty SEQUENCE OF it means that the server has no attributes it wants in client certification requests.

For example, if a CA wishes to have a certification request contain the MAC address [RFC2397] of a device and the pseudonym [X.520] and friendly name [RFC2925] of the holder of the private analog to the public key in the certification request, it takes the following object identifiers:

- o macAddress: 1.3.6.1.1.1.1.22
- o pseudonym: 2.5.4.65
- o friendlyName: 1.2.840.113549.1.9.20

and encodes them into an ASN.1 SEQUENCE to produce:

```
30 19 06 07 2b 06 01 01 01 01 16 06 03 55 04 41 06 09 2a 86 48 86
f7 0d 01 09 14
```

and then base64 encodes the resulting ASN.1 SEQUENCE to produce:

```
MBkGBysGAQEBARYGA1UEQYYJKoZIhvcNAQkU
```

The resulting response would look like this:

```
Content-Type: application/csrattrs; name=attributes
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=attributes
```

```
MBkGBysGAQEBARYGA1UEQYYJKoZIhvcNAQkU
```

4. Receipt of the application/csrattrs Body

A server that obtains a non-empty SEQUENCE OF SHALL ignore the OBJECT IDENTIFIERS in the application/csrattrs media type.

A client that obtains data using the application/csrattrs media type SHALL decode the body of the data, as necessary, and parse the result as an ASN.1 SEQUENCE of OBJECT IDENTIFIERS. An unknown OBJECT IDENTIFIER MUST be ignored by the client and SHALL NOT be a reason to not produce a certification request. A client SHOULD include every known OBJECT IDENTIFIER it receives in an application/csrattrs media type in its certification request with the appropriate value.

5. IANA Considerations

IANA SHALL update the Application Media Types registry with the following filled-in template from [[RFC4288](#)].

The media subtype for Attributes in a CertificationRequest is application/csrattrs.

Type name: application

Subtype name: csrattrs

Required parameters: None

Optional parameters: None

Encoding considerations: binary;

Security Considerations:

Clients request a list of attributes that servers wish to be in certification requests. The request/response SHOULD be done in a TLS-protected tunnel.

Interoperability considerations: None

Published specification: This memo.

Applications which use this media type:

Enrollment over Secure Transport (EST)

Additional information:

Magic number(s): None

File extension: None

Macintosh File Type Code(s):

Person & email address to contact for further information:

Dan Harkins <dharkins@arubanetworks.com>

Restrictions on usage: None

Author: Dan Harkins <dharkins@arubanetworks.com>

Intended usage: COMMON

Change controller: The IESG

6. Security Considerations

There are no real inherent security issues with the content being conveyed but an adversary who is able to interpose herself into the conversation could exclude attributes that a server may want, include attributes that a server may not want, and render meaningless other attributes that a server may want.

For this reason, this mime-type is used over a TLS-protected channel established as part of the [EST] protocol. certification request protocol whose Security Considerations would apply to the use of this mime-type.

The Security Considerations of [RFC2986] and [EST] apply.

7. References

7.1. Normative References

- [EST] Pritikin, M. and P. Yee, "Enrollment over Secure Transport", [draft-ietf-ipsec-pkix-est-01.txt](#) (a work in progress), March 2012.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, [RFC 3986](#), January 2005.
- [RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", [RFC 4648](#), October 2006.
- [RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", [RFC 5246](#), August 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).

7.2. Informative References

- [RFC2397] Masinter, L., "The "data" URL scheme", [RFC 2397](#), August 1998.
- [RFC2925] White, K., "Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations", [RFC 2925](#), September 2000.
- [RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", [RFC 2986](#), November 2000.
- [RFC4288] Freed, N. and J. Klensin, "Media Type Specifications and Registration Procedures", [BCP 13](#), [RFC 4288](#), December 2005.
- [X.520] "ITU-T Recommendation X.520 (2005) | ISO/IEC 9594-6:2005", Information technology - Open Systems Interconnection The Directory: Selected attribute types..

Authors' Addresses

Dan Harkins (editor)
Aruba Networks
1322 Crossman Avenue
Sunnyvale, CA 94089-1113
United States of America

Email: dharkins@arubanetworks.com

Sean Turner (editor)
IECA, Inc
3057 Nutley Street, Suite 106
Fairfax, VA 22031
United States of America

Email: turners@ieca.com

