

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 15, 2016

M. Pritikin
Cisco Systems, Inc.
C. Wallace
Red Hound Software, Inc.
April 13, 2016

**Alternative Challenge Password Attributes for Enrollment over Secure
Transport
draft-wallace-est-alt-challenge-08**

Abstract

This document defines a set of new Certificate Signing Request attributes for use with the Enrollment over Secure Transport (EST) protocol. These attributes provide disambiguation of the existing overloaded uses for the challengePassword attribute defined in PKCS (Public-Key Cryptography Standards) #9 ([RFC2985](https://tools.ietf.org/html/rfc2985)). Uses include the original certificate revocation password, common authentication password uses, and EST-defined linking of transport security identity.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](https://tools.ietf.org/html/bcp-78) and [BCP 79](https://tools.ietf.org/html/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 October 15, 2016.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](https://tools.ietf.org/html/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	2
2.	Terminology	3
3.	Alternative Challenge Password Attributes	3
3.1.	OTP Challenge Attribute	4
3.2.	Revocation Challenge Attribute	4
3.3.	EST Identity Linking Attribute	5
4.	Indicating Support for the Alternative Challenge Attributes .	5
5.	Security Considerations	6
6.	IANA Considerations	6
7.	References	6
7.1.	Normative References	6
7.2.	Informative References	7
Appendix A.	ASN.1 Module	8
Appendix B.	Acknowledgements	9
	Authors' Addresses	9

[1.](#) Introduction

PKCS (Public-Key Cryptography Standards) #9 [[RFC2985](#)] defined a challengePassword attribute that has been overloaded by modern protocol usage with the appropriate interpretation being provided by context rather than OID definition. PKCS #9 defines the challengePassword attribute as "a password by which an entity may request certificate revocation". The parsing and embedding of this attribute within Certificate Signing Requests is well supported by common PKI tool sets, but many work-flows leverage this supported field as a one-time password for authentication. For example this is codified in many Simple Certificate Enrollment Protocol (SCEP) implementations as indicated by [[I-D.gutmann-scep](#)]. Continuing this trend, Enrollment over Secure Transport (EST) [[RFC7030](#)] defines an additional semantic for the challengePassword attribute in [Section 3.5](#), in order to provide a linking of the Certificate Signing Request (CSR) to the secure transport.

Where the context of the protocol operation fully defined the proper semantic, and when only one use was required at a time, the overloading of this field did not cause difficulties. Implementation experience with EST has shown this to be a limitation though. There are plausible use cases where it is valuable to use either of the existing methods separately or in concert. For example an EST server

might require the client to authenticate itself using the existing client X.509 certificate, the user's username and password and to include a one-time password within the CSR all while maintaining identity linking to bind the CSR to the secure transport. The overloading of a single attribute type should not be the limiting factor for administrators attempting to meet their security requirements.

This document defines the otpChallenge attribute for use when a one-time password (OTP) value within the CSR is a requirement. The revocationChallenge attribute is defined to allow disambiguated usage of the original challenge password attribute semantics for certificate revocation. The estIdentityLinking attribute is defined to reference existing EST challenge password semantics with no potential for confusion with legacy challenge password practices.

The attributes defined in this specification supplement existing EST mechanisms and are not intended to displace current usage of any existing EST authentication mechanisms. Conveying the authentication value itself as an attribute may be preferable to using an HTTP or Transport Layer Security (TLS) password or other TLS authentication mechanism in environments where the certificate request processing component is removed from the HTTP/TLS termination point, for example, when a web application firewall is used.

2. Terminology

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 [[RFC2119](#)].

3. Alternative Challenge Password Attributes

The following sections describe three alternative challenge password attributes for use with EST [[RFC7030](#)]. [Appendix A](#) provides an ASN.1 module containing the new definitions.

Each attribute described below is defined as a DirectoryString with maximum length 255, which features several possible encoding options. Attribute values generated in accordance this document SHOULD use the PrintableString encoding whenever possible. If internationalization issues make this impossible, the UTF8String alternative SHOULD be used. Attribute processing systems MUST be able to recognize and process the PrintableString and UTF8String string types in DirectoryString values. Support for other string types is OPTIONAL.

3.1. OTP Challenge Attribute

The otpChallenge attribute is defined as a DirectoryString with an maximum length of 255. This is consistent with the challengePassword attribute as originally defined in PKCS#9 [RFC2985]. The otpChallenge attribute is identified by the id-aa-otpChallenge object identifier. This facilitates reuse of existing challengePassword code by associating the new object identifiers with the existing parsing and generation code. This attribute provides a means of conveying a one-time password value as part of a CSR request. Generation, verification, storage, etc. of the value is not addressed by this specification. [RFC4226] and [RFC6238] define one-time password mechanisms that MAY be used with this attribute.

```
ub-aa-otpChallenge INTEGER ::= 255
id-aa-otpChallenge OBJECT IDENTIFIER ::= {
    id-smime TBD1
}
otpChallenge ATTRIBUTE ::= {
    WITH SYNTAX DirectoryString {ub-aa-otpChallenge}
    EQUALITY MATCHING RULE caseExactMatch
    SINGLE VALUE TRUE
    ID id-aa-otpChallenge
}
```

3.2. Revocation Challenge Attribute

The original PKCS#9 challengePassword field has been overloaded and the common use is unclear. The revocationChallenge attribute defined here provides an unambiguous method of indicating the original PKCS#9 intent for this attribute type. The revocationChallenge attribute is identified by the id-aa-revocationChallenge object identifier. [RFC2985] discusses the original semantics for the PKCS #9 challenge password attribute.

```
ub-aa-revocationChallenge INTEGER ::= 255
id-aa-revocationChallenge OBJECT IDENTIFIER ::= {
    id-smime TBD2
}
revocationChallenge ATTRIBUTE ::= {
    WITH SYNTAX DirectoryString {ub-aa-revocationChallenge}
    EQUALITY MATCHING RULE caseExactMatch
    SINGLE VALUE TRUE
    ID id-aa-revocationChallenge
}
```


3.3. EST Identity Linking Attribute

EST defines a mechanism for associating identity information from an authenticated TLS session with proof-of-possession information in a certificate request. The mechanism was labeled using the pkcs-9-at-challengePassword identifier from [RFC2985]. To avoid any confusion with the semantics described in [RFC2985] or any other specifications that similarly defined use of the PKCS #9 challenge password attribute for their own purposes, a new object identifier is defined here and associated with the semantics described in [section 3.5 of \[RFC7030\]](#).

```
ub-aa-est-identity-linking INTEGER ::= 255
id-aa-estIdentityLinking OBJECT IDENTIFIER ::= {
    id-smime TBD3
}
estIdentityLinking ATTRIBUTE ::= {
    WITH SYNTAX DirectoryString {ub-aa-est-identity-linking}
    EQUALITY MATCHING RULE caseExactMatch
    SINGLE VALUE TRUE
    ID id-aa-estIdentityLinking
}
```

4. Indicating Support for the Alternative Challenge Attributes

The EST server MUST indicate these attributes, as the particular use case requires, in every CSR Attributes Response. An EST server MAY send both the "estIdentityLinking" and also the [\[RFC7030\]](#) "challengePassword" in a CSR Attrs response to ensure support for legacy [\[RFC7030\]](#) clients.

The client MUST include every indicated attribute for which it has values in the subsequent CSR. If a client sees "estIdentityLinking" in a CSR Attributes Response it SHOULD prefer that and not include an [\[RFC7030\]](#) "challengePassword" in the resulting CSR. EST clients that include an unsolicited "estIdentityLinking" attribute MAY also include the [\[RFC7030\]](#) "challengePassword" attribute to ensure support for legacy [\[RFC7030\]](#) servers.

EST servers MUST evaluate each challenge attribute independently. All challenge attributes included by an EST client MUST be successfully processed by an EST server for a request to be considered valid. The EST server MAY ignore challenge attributes according to local policy, for example if the EST client is an authenticated Registration Authority the EST server ignores the "estIdentityLinking" within a CSR (see [Section 3.7 of \[RFC7030\]](#)). The EST server MAY refuse enrollment requests that are not encoded according to the CA's policy.

5. Security Considerations

In addition to the security considerations expressed in the EST specification [[RFC7030](#)], additional security considerations may be associated with the mechanism used to generate and verify the otpChallenge value. Where a one-time password is used, the security considerations expressed in the "HOTP: An HMAC-Based One-Time Password Algorithm" [[RFC4226](#)] or "TOTP: Time-Based One-Time Password Algorithm" [[RFC6238](#)] specifications may be relevant. Similarly, the security considerations from [[RFC2985](#)] that apply to the challenge attribute are relevant as well.

6. IANA Considerations

[Section 3](#) defines three attributes that need object identifier assignments from the SMI Security for S/MIME Attributes (1.2.840.113549.1.9.16.2) registry [[RFC7107](#)].

[RFC Editor: please replace the TBDx references below, in [section 3.1](#), in [section 3.2](#), in [section 3.3](#) and in [Appendix A](#).]

Value	Description	Reference
-----	-----	-----
TBD1	id-aa-otpChallenge	[this document]
TBD2	id-aa-revocationChallenge	[this document]
TBD3	id-aa-estIdentityLinking	[this document]

[Appendix A](#) contains an ASN.1 module, and a module identifier needs to be assigned from the SMI Security for PKIX Module Identifier registry [[RFC7299](#)].

Value	Description	Reference
-----	-----	-----
TBD4	id-mod-EST-Alt-Challenge	[this document]

7. References

7.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<http://www.rfc-editor.org/info/rfc2119>>.
- [RFC2985] Nystrom, M. and B. Kaliski, "PKCS #9: Selected Object Classes and Attribute Types Version 2.0", [RFC 2985](#), DOI 10.17487/RFC2985, November 2000, <<http://www.rfc-editor.org/info/rfc2985>>.

- [RFC5272] Schaad, J. and M. Myers, "Certificate Management over CMS (CMC)", [RFC 5272](#), DOI 10.17487/RFC5272, June 2008, <<http://www.rfc-editor.org/info/rfc5272>>.
- [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](#), DOI 10.17487/RFC5280, May 2008, <<http://www.rfc-editor.org/info/rfc5280>>.
- [RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", [RFC 5912](#), DOI 10.17487/RFC5912, June 2010, <<http://www.rfc-editor.org/info/rfc5912>>.
- [RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", [RFC 7030](#), DOI 10.17487/RFC7030, October 2013, <<http://www.rfc-editor.org/info/rfc7030>>.

7.2. Informative References

- [RFC4226] M'Raihi, D., Bellare, M., Hoornaert, F., Naccache, D., and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm", [RFC 4226](#), DOI 10.17487/RFC4226, December 2005, <<http://www.rfc-editor.org/info/rfc4226>>.
- [RFC6238] M'Raihi, D., Machani, S., Pei, M., and J. Rydell, "TOTP: Time-Based One-Time Password Algorithm", [RFC 6238](#), DOI 10.17487/RFC6238, May 2011, <<http://www.rfc-editor.org/info/rfc6238>>.
- [RFC7107] Housley, R., "Object Identifier Registry for the S/MIME Mail Security Working Group", [RFC 7107](#), DOI 10.17487/RFC7107, January 2014, <<http://www.rfc-editor.org/info/rfc7107>>.
- [RFC7299] Housley, R., "Object Identifier Registry for the PKIX Working Group", [RFC 7299](#), DOI 10.17487/RFC7299, July 2014, <<http://www.rfc-editor.org/info/rfc7299>>.
- [I-D.gutmann-scep] Gutmann, P. and J. Marcon, "Simple Certificate Enrolment Protocol", [draft-gutmann-scep-01](#) (work in progress), September 2015.

[Appendix A](#). ASN.1 Module

The following ASN.1 module includes the definitions to support usage of the attributes defined in this specification. Modules from [\[RFC5912\]](#) are imported (original standards-track source for the imported structures is [\[RFC5280\]](#) and [\[RFC5272\]](#)).

```
Mod-EST-Alt-Challenge {
    iso(1) identified-organization(3) dod(6) internet(1) security(5)
        mechanisms(5) pkix(7) id-mod(0) TBD4
}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN
IMPORTS

DirectoryString{}
FROM PKIX1Explicit-2009 {
    iso(1) identified-organization(3) dod(6) internet(1) security(5)
        mechanisms(5) pkix(7) id-mod(0) id-mod-pkix1-explicit-02(51)
}

ATTRIBUTE
FROM PKIX-CommonTypes-2009 {
    iso(1) identified-organization(3) dod(6) internet(1) security(5)
        mechanisms(5) pkix(7) id-mod(0) id-mod-pkixCommon-02(57)
};

ub-aa-otpChallenge INTEGER ::= 255
id-aa-otpChallenge OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
        smime(16) aa(2) TBD1
}
otpChallenge ATTRIBUTE ::= {
    TYPE DirectoryString {ub-aa-otpChallenge}
    COUNTS MIN 1 MAX 1
    IDENTIFIED BY id-aa-otpChallenge
}

ub-aa-revocationChallenge INTEGER ::= 255
id-aa-revocationChallenge OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
        smime(16) aa(2) TBD2
}
revocationChallenge ATTRIBUTE ::= {
    TYPE DirectoryString {ub-aa-revocationChallenge}
    COUNTS MIN 1 MAX 1
    IDENTIFIED BY id-aa-revocationChallenge
}
```



```
ub-aa-est-identity-linking INTEGER ::= 255
id-aa-estIdentityLinking OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
    smime(16) aa(2) TBD3
}
estIdentityLinking ATTRIBUTE ::= {
    TYPE DirectoryString {ub-aa-est-identity-linking}
    COUNTS MIN 1 MAX 1
    IDENTIFIED BY id-aa-estIdentityLinking
}
END
```

[Appendix B](#). Acknowledgements

Thanks to Jim Schaad, Dan Harkins, Phil Scheffler, Geoff Beier, Mike Jenkins and Deb Cooley for their feedback.

Authors' Addresses

Max Pritikin
Cisco Systems, Inc.
510 McCarthy Drive
Milpitas, CA 95035
USA

Email: pritikin@cisco.com

Carl Wallace
Red Hound Software, Inc.

Email: carl@redhoundsoftware.com

