Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: February 4, 2016

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

August 3, 2015

Alternative Challenge Password Attributes for Enrollment over Secure Transport
draft-wallace-est-alt-challenge-00

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 PKCS #9 challengePassword attribute. Uses include the original certificate revocation password, common authentication password uses, and EST defined linking of transport security identity.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

PKCS #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 SCEP implementations as indicated by [I-D.gutmann-scep]. Continuing this trend, Enrollment over Secure Transport [RFC7030] defines an additional semantic for the challengePassword attribute in Section 3.5, in order to provide a linking of the Certificate Signing Request 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 x509 certificate, the user's username and password and to

include a One Time Password within the Certificate Signing Request 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 is 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 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 RFC 2119.

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.

3.1. OTP Challenge Attribute

The otpChallenge attribute is defined as a DirectoryString with an upper bound of 255. This is consistent with the challengePassword attribute as originally defined in PKCS#9. The otpChallenge attribute is identified by the id-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 an CSR request. Generation, verification, storage, etc. of the values is not addressed by this specification.

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

3.2. PKCS #9 Challenge Password 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 revocation Challenge attribute is identified by the id-revocationChallenge object identifier. [RFC2985] discusses the original semantics for the PKCS #9 challenge password attribute.

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

3.3. EST Identity Linking Attribute

EST defines a mechanism for association 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 using of the PKCS #9 challenge password attribute for their purposes, a new object identifier is defined here and associated with the semantics described in section 3.5 of [RFC7030].

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

4. Indicating Support for the Alternative Challenge Password Attributes

The EST server MAY indicate any or all of these in the /csrattrs. The EST client SHOULD include the indicated attributes in the subsequent CSR. The EST server can of course refuse enrollment requests that are not encoded according to the CA's policy.

Note that the "estIdentityLinking" attribute is a disambiguated alternative to the overloading of the "challengePassword" in section 3.5 of [RFC7030], therefore any EST server that requests "estIdentityLinking" MUST check the [RFC7030] "challengePassword" as specified in [RFC7030] as well as the "estIdentityLinking" requested in order to support legacy EST clients. EST clients that include the "estIdentityLinking" attribute SHOULD NOT also include the "challengePassword" attribute.

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 [RFC4226] or TOTP [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 an OID (id-otpChallenge) that should be assigned in the S/MIME arc maintained by IANA as described in section 3.5 of [RFC7107].

Appendix A defines an OID (EST-Alt-Challenge-Module) that should be assigned in the PKIX arc maintained by IANA as described in section 3.3 of [RFC7299].

Value	Description	Reference
TBD1	id-otpChallenge	[RFC7107]
TBD2	id-revocationChallenge	[RFC7107]
TBD3	id-estIdentityLinking	[RFC7107]
TBD4	EST-Alt-Challenge-Module	[RFC7299]

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>.

[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>.

7.2. Informative References

[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>.

[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>.

[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>.

[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., Pritikin, M., Nourse, A., and J. Vilhuber, "Simple Certificate Enrolment Protocol", draft-gutmann-scep-00 (work in progress), March 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].

```
EST-Alt-Challenge-Module {
   id-pkix 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-otpChallenge INTEGER ::= 255
id-otpChallenge OBJECT IDENTIFIER ::= {
```

```
      iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
      smime(16) aa(2) TBD
   }
   otpChallenge ATTRIBUTE ::= {
      WITH SYNTAX DirectoryString {ub-otpChallenge}
      EQUALITY MATCHING RULE caseExactMatch
      SINGLE VALUE TRUE
      ID id-otpChallenge
   }
   ub-revocationChallenge INTEGER ::= 255
   id-revocationChallenge OBJECT IDENTIFIER ::= {
      id-smime TBD2
   }
   revocationChallenge ATTRIBUTE ::= {
      WITH SYNTAX DirectoryString {ub-revocationChallenge}
      EQUALITY MATCHING RULE caseExactMatch
      SINGLE VALUE TRUE
      ID id-revocationChallenge
   }
   ub-est-identity-linking INTEGER ::= 255
   id-estIdentityLinking OBJECT IDENTIFIER ::= {
      id-smime TBD3
   }
   estIdentityLinking ATTRIBUTE ::= {
      WITH SYNTAX DirectoryString {ub-est-identity-linking}
      EQUALITY MATCHING RULE caseExactMatch
      SINGLE VALUE TRUE
      ID id-estIdentityLinking
   }
   END
```

Appendix B. Acknowledgements

Thanks to 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