Storing Validation Parameters in PKCS#8

Abstract

   This memo describes a method of storing parameters needed for
   private-key validation in the Private-Key Information Syntax
   Specification as defined in PKCS#8 format (RFC 5208). It is equally
   applicable to the alternative implementation of the Private-Key
   Information Syntax Specification as defined in RFC 5958.

   The approach described in this document encodes the parameters under
   a private enterprise extension and does not form part of a formal
   standard.

Status of This Memo

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

   This is a contribution to the RFC Series, independently of any other
   RFC stream. The RFC Editor has chosen to publish this document at
   its discretion and makes no statement about its value for
   implementation or deployment. Documents approved for publication by
   the RFC Editor are not candidates for any level of Internet Standard;
   see Section 2 of RFC 7841.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   https://www.rfc-editor.org/info/rfc8479.

Table of Contents

1. Introduction

   RSA or DSA private keys generated using the Shawe-Taylor prime
   generation algorithm described in [FIPS186-4] allow for parameter
   validation, i.e., they verify whether the primes are actually prime
   and were correctly generated. That is done by generating the
   parameters from a known seed and a selected hash algorithm.

   Storing these parameters in a private-key format such as the RSA
   Private-Key Syntax from PKCS#1 [RFC8017] or common representations
   for DSA private keys does not allow information needed for validation
   to be attached to the parameters. The purpose of this document is to
   describe such a method using the Private-Key Information Syntax
   Specification as defined in [RFC5208] and the alternative
   specification described in [RFC5958].

   The approach described in this document encodes the parameters under
   a private enterprise extension and does not form part of a formal
   standard. The encoding can be used as is or as the basis for a
   standard at a later time.

2. ValidationParams Attribute

   The information related to the validation parameters is stored as an
   attribute in the PrivateKeyInfo structure. The attribute is
   identified by the id-attr-validation-parameters object identifier and
   contains as AttributeValue a single ValidationParams structure.

```
   id-attr-validation-parameters OBJECT IDENTIFIER ::=
                                     {1 3 6 1 4 1 2312 18 8 1}

   ValidationParams ::= SEQUENCE {
       hashAlgo OBJECT IDENTIFIER,
       seed OCTET STRING
   }
```

   The algorithm identifier in ValidationParams should be a hash
   algorithm identifier for the methods described in [FIPS186-4]. The
   ValidationParams sequence must be DER encoded [ITU-T-X690].

3. Example Structure

   The following structure contains an RSA key generated using the
   algorithm from Section B.3.3 of [FIPS186-4], with SHA2-384 hash. The
   seed used is
   8af4328c87bebcec31e303b8f5537effcb6a91d947084d99a369823b36f01462 (hex
   encoded).

   -----BEGIN PRIVATE KEY-----
   MIIE/gIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCpPwXwfhDsWA3q
   jN2BWg1xfDjvZDVNfgTV/b95g304Aty3z13xPXAhHZ3ROW3pgPxTj9fiq7ZMy4Ua
   gMpPK81v3pHX1uokC2KcGXbgbAq2Q8ClxSXgEJllRwDENufjEdV10gArt8NlIP0N
   lota1kQUuI1DMsqc5DTIa35Nq4j1GW+KmLtP0kCrGq9fMGwjDbPEpSp9DTquEMHJ
   o7kyJIjB+93ikLvBUTgbxr+jcnTLXuhA8rC8r+KXre4NPPNPRyefRcALLt/URvfA
   rTvFOQfi3vIjNhBZL5FdC+FVAr5QnF3r2+cuDPbnczr4/rr81kzFGWrwyAgF5FWu
   pFtB5IYDAgMBAAECggEAHZ88vGNsNdmRkfhWupGW4cKCuo+Y7re8Q/H2Jd/4Nin2
   FKvUPuloaztiSGDbVm+vejama/Nu5FEIumNJRYMeoVJcx2DDuUxO1ZB1aIEwfMct
   /DWd0/JDzuCXB0Cu5GTWLhlz0zMGHXihIdQ0DtGKt++3Ncg5gy1D+cIqqJB515/z
   jYdZmb0Wqmz7H3DisuxvnhiCAOuNrjcDau80hpMA9TQlb+XKNGHIBgKpJe6lnB0P
   MsS/AjDiDoEpP9GG9mv9+96rAga4Nos6avYlwWwbC6d+hHIWvWEWsmrDfcJlm2gN
   tjvG8omj00t5dAt7qGhfOoNDGr5tvJVo/g96O/0I8QKBgQDdzytVRulo9aKVdAYW
   /Nj04thtnRaqsTyFH+7ibEVwNIUuld/Bp6NnuGrY+K1siX8+zA9f8mKxuXXV9KK4
   O89Ypw9js2BxM7VYO9Gmp6e1RY3Rrd8w7pG7/KqoPWXkuixTay9eybrJMWu3TT36
   q7NheNmBHqcFmSQQuUwEmvp3MQKBgQDDVaisMJkc/sIyQh3XrlfzmMLK+GlPDucD
   w5e50fHl8Q5PmTcP20zVLhTevffCqeItSyeAno94Xdzc9vZ/rt69410kJEHyBO9L
   CmhtYz94wvSdRhbqf4VzAl2WU184sIYiIZDGsnGScgIYvo6v6mITjRhc8AMdYoPR
   rL6xp6frcwKBgFi1+avCj6mFzD+fxqu89nyCmXLFiAI+nmjTy7PM/7yPlNB76qDG
   Dil2bW1Xj+y/1R91d6S1CVnxRbqLe+TZLuVS82m5nRHJT3b5fbD8jquGJOE+e+xT
   DgA0XoCpBa6D8yRt0uVDIyxCUsVd5DL0JusN7VehzcUEaZMyuL+CyDeRAoGBAImB
   qH6mq3Kc6Komnwlw4ttJ436sxr1vuTKOIyYdZBNB0Zg5PGi+MWU0zl5LDroLi3vl
   FwbVGBxcvxkSBU63FHhKMQw7Ne0gii+iQQcYQdtKKpb4ezNS1+exd55WTIcExTgL
   tvYZMhgsh8tRgfLWpXor7kWmdBrgeflFiOxZIL1/AoGAeBP7sdE+gzsh8jqFnVRj
   7nOg+YllJAlWsf7cTH4pLIy2Eo9D+cNjhL9LK6RaAd7PSZ1adm8HfaROA2cfCm84
   RI4c7Ue0G+N6LZiFvC0Bfi5SaPVAExXOty8UqjOCoZavSaXBPuNcTXZuzswcgbxI
   G5/kaJNHoEcdlVsPsYWKRNKgPzA9BgorBgEEAZIIEggBMS8wLQYJYIZIAWUDBAIC
   BCCK9DKMh7687DHjA7jlU37/y2qR2UcITZmjaYI7NvAUYg==
   -----END PRIVATE KEY-----

4. Compatibility Notes

   For compatibility, it is recommended that implementations following
   this document support generation and validation using the SHA2-384
   hash algorithm.

   The extension defined in this document is applicable both to the
   Private-Key Information Syntax Specification (PKCS#8) [RFC5208] and
   to Asymmetric Key Packages [RFC5958].

5. Security Considerations

   All the considerations in [RFC5208] and [RFC5958] apply.

6. IANA Considerations

   This document has no IANA actions.

7. References

7.1. Normative References

   [FIPS186-4]
             National Institute of Standards and Technology, "Digital
             Signature Standard (DSS)", FIPS PUB 186-4,
             DOI 10.6028/NIST.FIPS.186-4, July 2013.

   [ITU-T-X680]
             International Telecommunication Union, "Abstract Syntax
             Notation One (ASN.1): Specification of basic notation",
             ITU-T Recommendation X.680, July 2002,
             <https://www.itu.int/ITU-T/studygroups/com17/languages/
             X.680-0207.pdf>.

   [ITU-T-X690]
             International Telecommunication Union, "ASN.1 encoding
             rules: Specification of Basic Encoding Rules (BER),
             Canonical Encoding Rules (CER) and Distinguished Encoding
             Rules (DER)", ITU-T Recommendation X.690, July 2002,
             <https://www.itu.int/ITU-T/studygroups/com17/languages/
             X.690-0207.pdf>.

   [RFC5208] Kaliski, B., "Public-Key Cryptography Standards (PKCS) #8:
             Private-Key Information Syntax Specification Version 1.2",
             RFC 5208, DOI 10.17487/RFC5208, May 2008,
             <https://www.rfc-editor.org/info/rfc5208>.

   [RFC5958] Turner, S., "Asymmetric Key Packages", RFC 5958,
             DOI 10.17487/RFC5958, August 2010,
             <https://www.rfc-editor.org/info/rfc5958>.

7.2. Informative References

   [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,
              <https://www.rfc-editor.org/info/rfc5912>.

   [RFC8017] Moriarty, K., Ed., Kaliski, B., Jonsson, J., and A. Rusch,
              "PKCS #1: RSA Cryptography Specifications Version 2.2",
              RFC 8017, DOI 10.17487/RFC8017, November 2016,
              <https://www.rfc-editor.org/info/rfc8017>.

Appendix A. ASN.1 Module

   This appendix provides non-normative ASN.1 definitions for the
   structures described in this specification using ASN.1 as defined in
   [ITU-T-X680] and [RFC5912].

      PrivateKeyValidationAttrV1
        { iso(1) identified-organization(3) dod(6) internet(1)
          private(4) enterprise(1) 2312 18 1 1 }

      DEFINITIONS IMPLICIT TAGS ::=

      BEGIN

      -- EXPORTS ALL

      IMPORTS

      ATTRIBUTE
       FROM PKIX-CommonTypes-2009 -- [RFC5912]
         { iso(1) identified-organization(3) dod(6) internet(1)
           security(5) mechanisms(5) pkix(7) id-mod(0)
           id-mod-pkixCommon-02(57) } ;

      -- PrivateKeyInfo is defined in [RFC5208].
      -- This definition adds the validation parameters attribute
      -- to the set of allowed attributes.

      PrivateKeyInfo ATTRIBUTE ::= {
        at-validation-parameters, ... }

      at-validation-parameters ATTRIBUTE ::= {
        TYPE ValidationParams
        IDENTIFIED BY id-attr-validation-parameters }

      id-attr-validation-parameters OBJECT IDENTIFIER ::=
        { 1 3 6 1 4 1 2312 18 8 1 }

      ValidationParams ::= SEQUENCE {
        hashAlg OBJECT IDENTIFIER,
        seed OCTET STRING }

      END

Acknowledgements

   The author would like to thank Russ Housley for his comments and the
   ASN.1 module appendix.

Author's Address

   Nikos Mavrogiannopoulos
   Red Hat, Inc.
   Brno
   Czech Republic

   Email: nmav@redhat.com