Network Working Group
Internet-Draft
Updates: 5208 (if approved)
Intended status: Informational
Expires: February 9, 2018

N. Mavrogiannopoulos
Red Hat

August 8, 2017

# Storing private key validation parameters in PKCS#8
# draft-mavrogiannopoulos-pkcs8-validated-parameters-00

## Abstract

This memo describes a method of storing parameters needed for private key validation in the Private-Key Information Syntax Specification Version 1.2 [RFC5208] (PKCS#8) format.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and 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 February 9, 2018.

## 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., 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 attaching information on the parameters needed for validation. The purpose of the document is to describe such a method using the Private-Key Information Syntax Specification Version 1.2 [RFC5208] format.

## 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. ValidationParams attribute

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

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

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

The algorithm identifier in the ValidationParams should be a hash algorithm identifier for the [FIPS186-4] methods.

## 4. Example Structure

The following structure contains an RSA key generated using the [FIPS186-4] section B.3.3 algorithm 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/1R9ld6S1CVnxRbqLe+TZLuVS82m5nRHJT3b5fbD8jquGJOE+e+xT
DgA0XoCpBa6D8yRt0uVDIyxCUsVd5DL0JusN7VehzcUEaZMyuL+CyDeRAoGBAImB
qH6mq3Kc6Komnwlw4ttJ436sxr1vuTKOIyYdZBNB0Zg5PGi+MWU0zl5LDroLi3vl
FwbVGBxcvxkSBU63FHhKMQw7Ne0gii+iQQcYQdtKKpb4ezNS1+exd55WTIcExTgL
tvYZMhgsh8tRgfLWpXor7kWmdBrgeflFiOxZIL1/AoGAeBP7sdE+gzsh8jqFnVRj
7nOg+YllJAlWsf7cTH4pLIy2Eo9D+cNjhL9LK6RaAd7PSZ1adm8HfaROA2cfCm84
RI4c7Ue0G+N6LZiFvC0Bfi5SaPVAExXOty8UqjOCoZavSaXBPuNcTXZuzswcgbxI
G5/kaJNHoEcdlVsPsYWKRNKgPzA9BgorBgEEAZIIEggBMS8wLQYJYIZIAWUDBAIC
BCCK9DKMh7687DHjA7j1U37/y2qR2UcITZmjaYI7NvAUYg==
-----END PRIVATE KEY-----
```

## 5. Compatibility notes

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

This document intentionally ignores [RFC5958] as it enhances PKCS#8 [RFC5208] in a way that makes new keys incompatible with old parsers.

## 6. Security Considerations

All the considerations in [RFC5208] apply.

## 7. IANA Considerations

None.

## 8. References

### 8.1. 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>.

[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, <http://www.rfc-editor.org/info/rfc5208>.

[FIPS186-4] Kerry, C. and P. Gallagher, "FIPS PUB 186-4: Digital Signature Standard (DSS)", FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION , July 2013.

### 8.2. Informative References

[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, <http://www.rfc-editor.org/info/rfc8017>.

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

## Appendix A. Acknowledgements

None.

## Author's Address

Nikos Mavrogiannopoulos
Red Hat, Inc.
Brno
Czech Republic

Email: nmav@redhat.com