RFC 9579
Use of Password-Based Message Authentication Code 1 (PBMAC1) in PKCS #12 Syntax

Abstract

This document specifies additions and amendments to RFCs 7292 and 8018. It defines a way to use the Password-Based Message Authentication Code 1 (PBMAC1), defined in RFC 8018, inside the PKCS #12 syntax. The purpose of this specification is to permit the use of more modern Password-Based Key Derivation Functions (PBKDFs) and allow for regulatory compliance.

Status of This Memo

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

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are 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/rfc9579.

Copyright Notice

Copyright (c) 2024 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 (https://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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

**Table of Contents**

1. Introduction
2. Rationale
3. Requirements Language
4. Embedding PBMAC1 in PKCS #12
5. Recommended Parameters
6. Password Encoding
7. Deprecated Algorithms
8. IANA Considerations
9. Security Considerations
10. References
   10.1. Normative References
   10.2. Informative References
Appendix A. Test Vectors
   A.1. Valid PKCS #12 File with SHA-256 HMAC and PRF
   A.2. Valid PKCS #12 File with SHA-256 HMAC and SHA-512 PRF
   A.3. Valid PKCS #12 File with SHA-512 HMAC and PRF
   A.4. Invalid PKCS #12 File with Incorrect Iteration Count
   A.5. Invalid PKCS #12 File with Incorrect Salt
   A.6. Invalid PKCS #12 File with Missing Key Length
Appendix B. ASN.1 Module
Author's Address
1. Introduction

The PKCS #12 format [RFC7292] is widely used for the interoperable transfer of certificate, key, and other miscellaneous secrets between machines, applications, browsers, etc. Unfortunately, [RFC7292] mandates the use of a PKCS #12 specific password-based key derivation function that only allows change of the underlying message digest function.

2. Rationale

Due to security concerns with the key derivation function from [RFC7292] and the much higher extensibility of PBMAC1 [RFC8018], we propose the use of PBMAC1 for integrity protection of PKCS #12 structures. The new syntax is designed to allow legacy applications to still be able to decrypt the key material, even if they are unable to interpret the new integrity protection, provided that they can ignore failures in Message Authentication Code (MAC) verification. This change allows for the use of PBKDF2 [RFC8018] or scrypt PBKDFs [RFC7914] for derivation of MAC keys and future extensibility. Use of the extensible PBMAC1 mechanism also allows for greater flexibility and alignment with different government regulations, for example, in environments where PBKDF2 is the only allowed password-based key derivation function.

As the recommended methods for key protection require both encryption and integrity protection, we decided to amend the PKCS #12 format to support different key derivation functions rather than extending the PKCS #5 format by a new field that allows integrity protection.

We included an ASN.1 module [x680] [x681] [x682] [x683] [x690] that can be combined with the ASN.1 modules in [RFC7292] and [RFC8018] to incorporate additional MAC algorithms.

3. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

4. Embedding PBMAC1 in PKCS #12

The MacData structure in the PFX object, as described in item #3 in Section 4 of [RFC7292], is updated to include the following PBMAC1-specific guidance:

   a. The id-PBMAC1 object identifier is permitted as a valid type for the DigestAlgorithmIdentifier inside the DigestInfo object. If the algorithm field of the DigestAlgorithmIdentifier is id-PBMAC1, then the parameters field MUST be present and have a value consistent with PBMAC1-params parameters.
b. If the PBMAC1 algorithm is used, the digest value of the DigestInfo object **MUST** be the result of the PBMAC1 calculation over the authSafe field using the PBMAC1-params parameters.

c. If the PBMAC1 algorithm is used, the macSalt value **MUST** be ignored. For backwards compatibility, it **SHOULD NOT** be empty.

d. If the PBMAC1 algorithm is used, the iterations value **MUST** be ignored. For backwards compatibility, it **SHOULD** have a non-zero positive value.

### 5. Recommended Parameters

To provide interoperability between different implementations, all implementations of this specification **MUST** support the PBKDF2 key derivation function paired with SHA-256 HMAC [SHA2] [RFC2104] for both integrity check and the PBKDF2 pseudorandom function (PRF). It’s **RECOMMENDED** for implementations to support other SHA-2-based HMACs. Implementations **MAY** use other hash functions, like the SHA-3 family of hash functions [SHA3]. Implementations **MAY** use other KDF methods, like the scrypt PBKDF [RFC7914].

The length of the key generated by the used KDF **MUST** be encoded explicitly in the parameters field and **SHOULD** be the same size as the HMAC function output size. This means that PBMAC1-params specifying SHA-256 HMAC should also include KDF parameters that generate a 32-octet key. In particular, when using the PBKDF2, implementations **MUST** include the keyLength field in the encoded PBKDF2-params. Implementations **MUST NOT** accept PBKDF2 KDF with PBKDF2-params that omit the keyLength field.

### 6. Password Encoding

As documented in Appendix B.1 of [RFC7292], the handling of password encoding in the underlying standards is underspecified. However, just as with PBES1 and PBES2 when used in the context of PKCS #12 objects, all passwords used with PBMAC1 **MUST** be created from BMPStrings with a NULL terminator.

### 7. Deprecated Algorithms

While attacks against SHA-1 HMACs are not considered practical [RFC6194] to limit the number of algorithms needed for interoperability, implementations of this specification **SHOULD NOT** use PBKDF2 with the SHA-1 HMAC. In addition, implementations **MUST NOT** use any other message digest functions with an output of 160 bits or less.

### 8. IANA Considerations

IANA has registered the following object identifier in the "SMI Security for S/MIME Module Identifier (1.2.840.113549.1.9.16.0)" registry. See Appendix B for the ASN.1 module.
9. Security Considerations

Except for the use of different key derivation functions, this document doesn't change how the integrity protection on PKCS #12 objects is computed; therefore, all the security considerations from [RFC7292] apply.

Use of PBMAC1 and PBKDF2 is unchanged from [RFC8018]; therefore, all the security considerations from [RFC8018] apply.

The KDFs generally don't have a lower limit for the generated key size, allowing the specification of very small key sizes (of 1 octet), which can facilitate brute-force attacks on the HMAC. Since the KDF parameters are not cryptographically protected and HMACs accept arbitrary key sizes, implementations MAY refuse to process KDF parameters that specify small key output sizes or weak parameters. It's RECOMMENDED to reject any KDF parameters that specify key lengths less than 20 octets.

10. References

10.1. Normative References


Table 1

<table>
<thead>
<tr>
<th>Decimal</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>76</td>
<td>id-pkcs12-pbmac1-2023</td>
<td>RFC 9579</td>
</tr>
</tbody>
</table>

Kario Informational Page 5
10.2. Informative References


Appendix A. Test Vectors

All test vectors use "1234" as the password for both encryption and integrity protection.

A.1. Valid PKCS #12 File with SHA-256 HMAC and PRF

The following base64-encoded PKCS #12 file MUST be readable by implementations following this RFC.
 RFC 9579  
PBMAC1 in PKCS #12  
May 2024
A.2. Valid PKCS #12 File with SHA-256 HMAC and SHA-512 PRF

The following base64-encoded PKCS #12 file SHOULD be readable by implementations following this RFC.

```
MIIkigIBAzCCCGUCGcSqiB3DQEHaAAdCCCFyEgynnMlI7jCCCBGICGcSqiB3DQFETBKMcKCsGQG
SiB3DQFETdAcBai4j6XYY2iyzoIiCAAAwDAYiOhzKvHzCnqfAgfADAbg1hkgZBQME
A5s0EEAHPHSSk3J9kF1e6A0ggPgtbMLGoF5kJkLpVXMcxLrT129L7/vCRb8
@IZtlnfHPA7afTrrjuGbwqowCMQxkw9zQuxC1eHx42LW666b1H7WmSSOWMANlU4b
wy4a1LIEWYAfQ7kPxBH921U1qhum88E8gh117BnhBfWaz0wlq1p9c19/lpujO
wodSY*pNBD8oeBau1m6D9jg5c2aLp7M/0woudVqEt7HAgMyTBxKxu/1lp1b9nb1
XLTQ0a6x9fXERf+QQAqS24HULJpGp301cCMHDZVH685qrgY5R9N3ISP0HC11d11nb
JwlyurAhXv8BMD4KAvkXETb8q7xtP3U7E/Mh1gyZG092B2DdvNDAk712HSOS
3AxrFncGDXnwlx9fN BT7f7cyC789V9UC/1+xGGPhGZouaZw+13lPuz
fjhhbyolQer22ndBz+1/s2GHhZ4XxLg4100zgkn7DX92S/UlbmcZam1apjGwKY/
7KtA8BranNZ211mJF+zHci+BeDiM7eyEuGUCYRhdR/+hBU1uyJgi5lK5i43+2PRZ
FZKLTHG0C6q6q2EJEDsEj+RKGiyj498v7fml4iwVFABV78A1AgO3T868d4oerV70k
c4g8sIOWI6sCE/GLSC0HkkTtyUNQMNqD1G1LTPzCzGfhG9hG7iXyTKL2c2yFs
pgggPeDrdq1fnBZumC2sBwhRgRbSpD6me6OuqvjoxIIZQAEV53xmd63un1UH1
jhVYfCwSamnhu+/v+iWSTZq0wghF7DmHq268itck7Z7Byp5xcD1U0Z5p5fgr9Jrk
DZTOOYM51A8kte6KCWa+jnngCstsIEBbNsCjNvAT3q/X77VdmmehWVel+6k4
z+GvKr+D3xPdp1tjbrb+/v9rLg1bn0gtQgPntBnXa1l6C1HdN6e5x4sCjUOXWf
Iy6bR6H0QjQ2LLKAAACq6n4E8h1j3WPxl19e8FXNroRkdsRux3jiyqDr606skkl
wnytMVjV5x+39cx6v4gyFPMFWbD3Ng3syJuDu0pUsraEwMATs4jasadWKEeyIC2F
srw1dzFm/wv1g17E7WqnmLr44dpssylOjlzNjU7hE2j1Ihme3N45fXnxMrRku
gBdai11fL29inVuzr7wtjLjQwKd+vusHm9r/K0HTaSNRqepxnjX8Y1c9g+96eyr1/BW
k3*y4GIE2JdxsdQOE5oR5qS5HQO5QTyAU6w6kXalhrRrUGU3vxtYSQ3Uuuzw
e0q2UFL16vdw7qWf5pysr8lpt8vdwxwiiwigjKftpJlIZQmMrz5X25qizITH
Dy4+e+iyiVigWqEBggqkhi1g9gW6gBggvY1IIIFcTCCB80wqV6pBsqghkki9gWb6
DaOaBacQCBSTEEwgtUfMCqC8EwD3FDBTMBCKMCQCSqS3iB3DQFETDdB4CAdHdWsh
4wt3aAIChQfIzKhEAgfADAbg1hkgZBQMEAS0EELGFXCnqfGqFnnPrb4M3Ng3syJuDu0pUsraEwMATs4jasadWKEeyIC2F
fsz1g56cEgqTQro94bp/fwFwPzr7TeCzqg1o1H7V8j6s76saxu2Q9OQA999fHTnq
N0X8R6en66khqPWC737sDd6aO2wq9G05t+xt2n2r225+K7D4Oxiu3A93g7exVkbJ
0DLCHAS7Mu+hkp50CkPCXs77f00A1qJmMe4EuAsiwvwLrHuz7eI16UpmlmgkQnaC1
S49f4vz9nS9xcrTnuCqllnpd2qQjSy0U6i6xQeKLBfKlriJhOboaFmJwP1u1
QOAmzRAlhYbd1OFMXP3kum3u/1uPrGccV5v2TU2ume+WYEXS3C0YR3/R4UdF
IfEzeRFPs21l5MD5FSKmFKEeBckhK09i7zvK3ovKeKUBdM66uufay/uIyXpM
M1B9fAbpQojQkJQT8T8bBkkBAPivyg2LBSsrrR51CoooWfAnu94z1R56bBpCz7H
iSkU0iOowQoX3MY5hIvXWJX7BHbBpeEc0MYL8S/4qDwGw880DRc1AC0mMmAqZ
4r3bR32E4Z7N2+Zcakycrv3Xmwb/LKZN46c34T4anL5gLZJ5WzO8wEDkkyEwJaoq
Tk0i11sLzgB9hjy9Q8ee429ek5jv7qFCss68KTE/-mhuJ33mP3ZicaiCjHdHe
6brbKjhrJLb6mg6aS7ed89T4ONg08wkkl9G99k80WJm5sCn5gb1b2F6 rz1f7ypG7a50
yclt1J2WMrB7g6yGypVnVocEieNh71L7xyeQGGR0/S1zDx0uYaJVM9FZjaJMN9K9pZgno
CMQeameaq8P3CMk3jma8e4bIiKk39DkWODWYv1gCPVPYYZK6cPw+Efwsx+2zhGzYzcc
vupW669mdI1PD4UsyQaqag3J7uB6K4Cm2h5xMx0V/C+KoDgkeMcbTweQueWy
agev2i192KU1jB7T4Q2KZpVwammsonmlDpeedkipGnCu5yXyg/y4UkAVaq1j
S9t4wUKEACXcJx80VUXfqgms2+mhPFBPf6s8O43nWWWG1Q6mKmBHPUCfD9nnP67cuh
s1xu3NRLy+J+Ql1Fvba3BYTBA6WBymiEml9x1f1ULW87x2E+6Crh0kObkY4f90Crjpx
1jo/n1ocosoQODekv9KDDVR7Ls7DhFmvr1mUjFmqj7/KThZkE4NnAmdMtkM2
yKXqXh2AbBrQkU3mLW1581Pj5lujw00g/LjJvQjJ6h6yeJH4HYb8mb9ldmeP3LQAF
CyKzZnqmgvkmMvAXQmuLEmPf11stZKbrhNjZcbuzzonNsf+a+r5L6EXHmN1L7wC
TuUv/JLVdNuXYLFvpv3umsf5J1SwkV62RtWRIm0V0Qa2o5L1Wfm1PZKms5N4D
DYtsS9A6yQXOEsXvKClQrnC685JrXJdcmseBqM1JttkL6gYlgbmbjx1g3n
```
A.3. Valid PKCS #12 File and PRF

The following base64-encoded PKCS #12 file SHOULD be readable by implementations following this RFC.

```
N+Z+sEFox+ZWQoglBJh0mC20iAC8wquU+sxslT4WnndaPWKVqROChvDaZhA0ANqHci19PHufcFZw+fhHT8nShnevQcd6XcMhSaQ2MtpY8/jrgNKguzT2yH9gp/wVpT3/QO87BFgKFIEbuvAfasVfIbIryIheg+Leib2di0MNXNAwbcg2YxuxkJA7Jbgkq
h1ki9gwBWCUXfgQwuWO5S6dorvWVY3BFWUMaw0rUEajScwFdBTEKGCqsGqSib3DQEF
DjA8MwCgcGgsGgsb3DQFEDFABAgur2yP/+/Dr9gICCAACASAWDAYKOzHvcNAg5F
ADAM0ggkhh1g9w8CCQUABCA3f5L93jw8IgCbkHhqkNwbpp6lauy0uxSju4/Vd
6QQIK9UIFVTRQCAQ=
```
A.4. Invalid PKCS #12 File with Incorrect Iteration Count

The following base64-encoded PKCS #12 file MUST NOT be readable by an implementation following this RFC when it is verifying integrity protection.

```text
yEMqPlvnPWswdnaid35pxios79fPl1Hr0/Q6+DoA5GyYq8SFd7EYLrGMGa5J+i
5sN7z6U4umZ2xuxKYHnuhB0zii6Y0a4+fhT71x02eTe7aPlEB391UqsysjUVJnso
bckcw Ou/j08s9YeFdd93B44xezuYyv1vdo191qcm1Ttsa2w7d1w/yu4d7KrVP2
VXXXqgomoAQQoZiuSf91/7YsyrV8U4H3U2i4nrSVJ8EJtPQs0BW5170dGqWxyXb
BHTqfJ4LG/pKePMoP0uzqGwDv2jJtybml1q1Mzgyp2ycMomn4vp7DeQLGszXFeANy+

MUST NOT

RFC 9579
PBMAC1 in PKCS #12
May 2024

Kario

Informational

Page 10

```

MIKIwiBBAzcCCcQcGSGsIb3DQEHAacYjppEggnyMIIJ7jCBGICGcQgSISb3DDOEH
BqCBQfmgqPRApEAMIEASAYjKoZihvNaQcBMfCCqGSGsISb3DDQFDTBKMGCcQgS
Slb3DDQFDTDCBa8g9ppxzXy25yscCwCAADwYiOkzihvNagFKFADAgb1gkhgBZQOME
AsoEEK7YyaFQD1pYVwz99/fs+AgPpgfIT2XapyaFgDppvdLkdvaf3hXwzejzkb
7Xpc67dtvPvTHVWHD+kIs+jj+jx+mYmvW0AucAhAG/Dig/vzWomsqasB5sws5tKtb
+TMQPSXKLNeomB6aAReKeG/eqCMcBGcQ/af+6+nXSMwNp+777+77dnW8bBgcSJKOF
Fj75Nr1bmnDmCmh71qOgqBmF6bPxF/3xwAXJtyn+ct+SNETF0jA8sTFtXpYNv2X
vheZrErxYhj7/9o4G3UrcIe36gRmkFpRdtD6i1z4zbb2je4r/S4hnrQbsryrz3j5
IEjaD06+DmGjWmgRui1WboGow1J37MRMDCOyOZWC4n5WhLytRh6aJa1brxhP
H46z2USLKmzoF+ygeQycSBXMQGp0T36+xQocFYi2N5niy82TncTwf430FySfQhJ5
Suma4I33E88dUuMv87/soF66HsDz4j6h0f4nWmas71aosaBxGxq1l7K9GRvij
xM9X0WBaqNh1/bBnhXzFcmI7/7opyx5UJYFWGBsHPlBHgY7ad8As89M9sh
nbGj6Fuk4h0Qci09/M2fpmIo64reP18PKq2tVAMPdd3rTLLsngzqU6il90/QFCU
fbtqsMF0bgEuhE8cfvi0dYDFABFgIgypwUCtq7A3XKn2nQosjcXvzV919K9BNEd
aa9V8A10Z0sk3/VR/QUgQ8PRwU1jPN5BzUeVh7S0y/ImuJKqwpfQfjlyQmJ5
jDe/VMH9GQVRIF18bzu+U48Fy8CaeBehnS5AAPm18YPYPVUntj/3QJFv++cAhNVI+L
La8q1Nen+jr4I3a23z3p/ugtzKwkk+tPrxtQb8E39EU1LVJn8amPwMnw3W75ZIA
MljRXWEkw4jdeDy4m4EHBcM2u4R4HM8MFyjyaWyweYsprcnsaxz+7AZ67r
L0dxvS3NqsnTXhc3t9tKpRoe6L7hd3x4d0d61cRwgdYT5Bw7e7341dlVTUMJ
boDeQ7jn4JRwqJh1RCCZ/0BfkC42Xam7G901u3g8bX80rQjpdg4a7bCcWwryWf
chLNqua4f4qOaVwXyXIlY6j1/s3tKbYCYXVPE20AMB9F1/0U76UMBJQFNQ
0qdxj+3AhUVgnGusCymY1kE6Tdp8OZGkYwMrNSGtqlsu3Mhwd7PEwW43L3tDQ/0
9xfMczkHi2C4hXnoHv/qq2dGbhj4jQ0Xh1poU6mxGn2emeh2bsD2BkbPn7kP4
wp/VQxQDtwgEuvGHLhFscuAde40ZFbmrBfr7w0gw7kN23USu231ZzX3+S024afyq
vR+6x6ttkwQwEbgkhq118CBG8BbWwggV1BIFc7CBBGWg0Vbgsqkhg19GBw
DaobBAqCBTBEggUtMfCCGSGsISb3DDQFDTBKMGCcQgSISb3DDQFDTDCAhBTAxwz+
PvTPyAAMCIAADwYiOkzihvNaQcBMfCCqGSGsISb3DDQFDTBKMGCcQgSISb3DDQFDT
```

```
BqCBQfmgqPRApEAMIEASAYjKoZihvNaQcBMfCCqGSGsISb3DDOEH
MIKIwiBBAzcCCcQcGSGsIb3DQEHAacYjppEggnyMIIJ7jCBGICGcQgSISb3DDOEH
BqCBQfmgqPRApEAMIEASAYjKoZihvNaQcBMfCCqGSGsISb3DDOEH
May 2024
```
A.5. Invalid PKCS #12 File with Incorrect Salt

The following base64-encoded PKCS #12 file MUST NOT be readable by an implementation following this RFC when it is verifying integrity protection.

```plaintext
T4JhZ0h/CfcV2WvhpOgqXy0PWrzZEIEm5e18DZ96mjVlXL011480eSi0PsZ2MNk
Y3M3rTpwQ5T5w0qseEyDwUpnpe5b8Kt/s7En08JnnJyjPRL17c0qOr6j+6YqRtpA7
a9oWqJMcUtp+bqzGRJh+3HDlFBw2Yz9p9iavd4KmBm2zStU0o2MjsVnnxkk5sLd
sshAd6WkbFWf7KbLQHOt4AId6ME04EKKfVF9J7txCT4JEn6C98LpG+K+rfy7GHoF
ZxtgUOwrgXY3ur7Ur6KZ3ExKVpZi5EdhpAau7JKhp0wKozAp/OKWNNwrz6h
oub2Mbn1B+IA60psYHxkNdgBzH7WQmbYH8YGFhVvAg8PZCYqCnjzLr9JrR8B
BuH9jXkTh7KLhzrxyXv19AYub9D95cxozizad6VPNvogF5s+Omyd6jPACJp76hF
W6JpJbcupP0Po00VWtDz3df1P0hZqvKwOPFA+gKZScggASfgyiP9V3Xc8jI1
wjNz4D2Ql7JUUKJiGIYJLU09huxzFHLgj759DcNRhp1s15aG570fISD9yBuCAjY
PqaZHPuRTrvcG3Rab3CA73nEznKyFaLOXFzyfyaSmYhsHT3nLy1Mej+2bR
Eko/y1dFjU5Ji+L3Kj6wa+PnduHx7Ie4UEuww2XyYMPnxQ1w6rOpQPZ8X82
HhqGrLV38P1pzqWpHj5tkoxmWdC9+yJt/cQfNXYjDyoo7t7mVc1lhi19ps/
0841kJSLNKLWxv6G+3LNkWk4jQn194PpopID7+oDMsGmttO78CBrHxMD/0Q
qnijKzJxszL1+qJ75uQv87MuLzzCzKuGB3pH1XcJncWhkLtrByKe/N+VcQtOm
p8wyik/B1ndxXn9Kbtd0I2zIi64h2Q8h0k66w/PSIjYwJl6eDNEOSZl/1mgCFU
QnUT17Uc/p+qOnfen6uap2o7Wlsrj7Bu/pytZ65rjt+ou0i6EHeWqWqGVZX0
7gVW4HoKe/v6aPGNvkLCmtPuDZsn9jji3g9UdeyVRfv10R0639XkW57q77Xe
I5zSyDUL8Nmno9Siju3t+rqVYW0NatC6q/40DII4Lm3de3EyZx7j3mgH3/SASM
FzwR9pXvc6dsYX0kZ4PyaXfagZso3F1sU799+iJUvOt0CEMerJTAjBkgq
kig9WGBCRuFxugU0w0dorvVW3BUwAmAw0rUEajSwctFtBTbMEKGCsgShb3DQEF
DjA8mCwCSCgCgSSb3DQEFDDfA6Ahvrw4s4cxcwICCAECASAWDAYIOKzhvNAGKF
ADAMBggkhkiG9w0BCRUxFgQUwWO5DorvVWYF3BWUmAw0rUEajScwTMBQGCSqG
SIb3DQEFDDfA6Ahvrw4s4cxcwICCAECASAWDAYIOKzhvNAGKF
```

MIIkigB1AzC6CCcUGcGSGsSib3DQEFAaAqCCCFgEgnywMIJjCBcBiGCsGqSib3DQEHE
BcCBFBwTrpaEGIEMtSAYJKbZIhecNACQgMARFgcsGSGsSib3DQEFDBTKMcKcGCssG
Sib3DQEFDDcBAg9pxY2yscwiICCAAWAYIOKzIhecNAGKFADAgB1gkgbZQME
ASeEKeT7yAaFD1ipWrwZm9Wf/+AsPggFgbIT2XapygFiredvLkvaf3lHw+zzjkKb
Fx7C76DtvPHVWHD+kKssj+XyarMvWy8aUaHAg/Dig+pvWommsqB5s5sw1/5Tb
+TMQSPXlKNleOmB6AReKeGc/QmcBQVQg/a6+nXwSmWnNPp71772dmW8bGcJ0kF
Fj75T1nBmI6rNdcB7lQ0gZBMF6bPxF/3XWAJxyc+tSNETF0aJ8Z7Zb+1V0w9
5eUmrdP uproxkVzbbk017jkL63yKcfrrPtdD61i4zZbj2Ev4r/s4hinRsbrVzJWY
IEja0Dy6+0m86JtwRGruG1iWbGowt137GWmDcovgOZWC4sNswrLyyR6JaE1brxhXp
H4z2ZULSmKmzO+YeQycQsM20pS0t3+cXoxFCFY215n5yB2Tntwcf3480F8sQh1
Suma4I3E8088dUjMv8t/s06d6HSsD4z4h0f4nWmas7IaSAbGkXgIa1k7hGRjij
xM3WOXQaNi/BBnhsA7CFmiy7/opyx5UJFJWGBSmHiplBhBYmx7A68sA89MShh
nbGjiU8Hq80c1s9iW9w04fureP8IK2qtVAm9dP3rTlsmGzq2U68Q0CU
fbtqsmF0bqEug8cfid1YDFABEt1gypwUCtucQ7QAK2nQn0qoCQxV9i1KBnD
au98VTA0e2s3k/VPQIDPmPWiruJPN5bzUeVbHS0y/IImjKwwqGqFjIydrQm5j
je+DmLy19QGVRf1N8zuU+48hF8YCAOeeBeHsn5AAPmLoPPyVunt3/jQN1+v+cAHr
NIA+Laqn1en+nJR4aa43ZIy/bUtPArKxk+tPrxTbG030EUs1LYj8hampWm3w75ZIA
MJrXWekjBel4j4udzeqEBVEc2v4M4rRHMbfYyAWysey8rccp8eMsaxzar+7A67r
1DoXv5S3QsnXThc37t9kpoee6L1h6d3x40d61cRwdgT5BYwHe74id4VtUmJ
bDEqY7jnJrKwL7rcrZt/0fBkFC42xAm7G010UGg88B0Qipddg4a7VcYuwywF
C7hLqnuqA4qOdaVXwXH3luY6Y1JL/3is1KbYCVXPEZOBMP9F1/U076UMJ6QNuF
0pxjx+SahUVgNucSmYf1k6ETDp8qZGkV8kURGStqLx3UmMd7PEWdML3tqD/0
9f1FmKzcZ17C2FxfOvh/qad2ghh8j4Jq0X8ihp0UmMxNg2Me2ehD8sb2kbp6n7pK4
wp/vQxGdhQrUevYHLVsGCAu4E4BFmBfrF78w67Zk08SUSZ8z1X3S+024g7g
Qrev/6x6rtwkgwGWEbk4h7h1g9w8B8w6gGvV11IIFTCCBEBwggvP0bqsgk1G9w8B
DАОBbAqCBTEwggUTmFccGScSib3DQEFDBTKMcKcGCsgSib3DQEEfDA6AhvRzxw5r
```

May 2024

Kario

Informational

Page 11
A.6. Invalid PKCS #12 File with Missing Key Length

The following base64-encoded PKCS #12 file MUST NOT be readable by an implementation following this RFC when it is verifying integrity protection.

```
VptrYAICCAAwDAYIKoZiIhvcNAgkFADAgBgkgBZQMEASoEEK9nSqc1I2t4tMVG
bWhtpot0EGtQ2zwI7j34gCtv7J6nuOSndAjShGv7m2J7WVM0s1tpq2f9B9m3n1v
Y0JMV4LE7sLRuUzN82pdOcFmCnEpMfCcNv2srLp1m0Ckxu80jSqHZLOkVL0Rv0sZ
8dMECLMdigPr0KsryLerL114TtExR4/zbkuAWMRO028kF7bubQy0HLwusKw1LxLg
vi0g9RKg/zXhRfQfHjX/8NStv7x1hle7n/7y2E2KpsRfHdam/iUHafmCMKgMHTU248
JER9+nXl5T1hH+1eDj/pkx+z+yVHow9XUZKu28z3D6mUplLz1BgfJMBPWPvWVUVD
A40C1QVbDcGtpjaL1z8x0SH3IIFcNwQ0r6U8Hw1eNPJghQ78HUYH6Hxnhn8b0
50i636wFz5S0mX0p/s+D3t+3TrxmrYpd2XnxRme3cnaY01UqVc8/e8L4R7SjdK
T4Jh2t8h/CfCvZ2WnvPqyWkpYWzr+EImE81dBD96mJLX01i1480eG1BpXZM1
YM33rTpwQT5WqOsEyDwQune58kkt/s7E80N7JnPyJRL1JcLcq0drr+6+yYrPaT7
a90WJqNcuSp/bqzGRj3+H1D1F2yZp9i1adv4Km2z4nIEJn1Wo5sTmkkn5dL5ed
sshAD6WbfK7KLAHQT4Ai6dME04EKrE9V9JbtxC4R4En6C99LpgeLkr+yF7HG0
Zxtg0URwGRXy3aLurD5S7zkG3ExVKpzi5EhpaDuA7JkhoPyKozap/OKWMMRz6h
oub2Mbn1B+iA60p5yUWhxyNbgJh7VQmnbY8HygF6gVvaaBpCyQxjpljSjR8RB
Bu9H9XkxTh7klhxgrXYVx19uAYud95kcx9izad6VPnovgFsM+Omdyp6JAPc1h6F
W6PJBucpYP0p0WvttQd2Z3zf1P0hZqVkwOFA+p+zKazkgqAs5ypl9P93C8zjI1
wznJodM2QT+UUJkiiGyJX,UE009huzxFHIlgj759dcNRhpq15AgR57ofISD9uBACAJY
Pq/aZHPfuRTvRGC3raIbACs73znErzyFaLOxfyzfaShysh253ntyL1MejC+2BR
Eko/y1dgFuxvU5j1Q+jK3K6awj+Pndxu2sYxmyxPnW6rroQpZBXB8
HhqcgLV838p1zQwPDhjH5koxmWdc+c/jt+tcCQNYJpJdyoaX77dMvClh1w9ps/
8041pinrNsLJxwv6G6+b3LN/kwaQ4jwN194popidO7+do5m5mht078c8RrXRHM7B/9Q
qniJzKsZepj4qMNmnxZa0F3hPXiCjcNvcWurtByvE+N+cTcV9m/p8wyik1Blnx9k4Kdtdi21w164h2QBGon66w6wq/P8Jiwy2l6DNEOZtH/1McGFU
QuNT1q/p+jQgen6sAup2GWLvsJrB7u/pytz65rjt/touo6ih6ewWqwrVpXGZD0
7vgWvH0ke/V6paGPvNvkPcuDzsn9jij3gShudyFVRf10x569kWcg5757h7xvE
iSzDyUl1Bnbnom9SIjtsrurqYrVnYWanTc6q/4DB142Lm33edEyY7xjhm3G/12ASM
Fwz9Pw9vcxid6sYokd1Ya9QXPUZx+Fag2sosF3s1sU79F+IJVUc80MEXJTaBjgbk
h1k2gbw9BCRUFGo0UwW5OdorVWYF3B8WumAw6rReajScwFdbWmEgCGsGqlIG13QFE
DJa89QwXGSGsgsISb3DQEFDBFADF8A0T1QgqYwFhAAFCAACcASAwAYDKoZihvcNAgF
ADAMghqqcky9g686CCQUACB6npw2F02dcJn78z654NUXG36k5aX0DHFhClIk5Bf4K
3QQlBz80LAMuxMCAQE=
```

The following base64-encoded PKCS #12 file MUST NOT be readable by an implementation following this RFC when it is verifying integrity protection.

```
MIKlAIBaZCCqG/GsSgl3dQEHAAaCofyEggEyMIIj1CBBIG5GScSgl3DOeqH
BqGCBFWppQPAgEAMlEYAYkaZihvcNAeBMCfMCQgSgl3DOeqFDfBKMdkcCg0g
Sb3DQEFdFADBqS0Y2ycsciCAACAAwDAYKoZiIhvcNAgkFADAgBgkgBZQMEASoE
AsoEKEK7yVaFQd1pYWwzn9F/s+fSgPgfIIItXayaFgDppdvKldvaF3Hw+zzjkZb
7fxCFv67tDvTVwKHDH+Kiss+j+s+jvy+xMvy0aCuaAHAG/Dig+vzWonnasaB5sws5/kTb
+TQMPXkLNoeBm6ArAn2QcBqVqGQ/a6b+nXSwmxNp+P+71772dmWmBgcSJiK8F
Fj75NrInbMnDCMb71Qg0z0BmF6b8pxX3WAjytjcx+tSNEtFHaj8z7B4Z15vW9
5eUmDpRpuXevb0k4Itc639gKrcrPtdD6i4lzsz2jErV4/S4hnrQsbriyluzJWY
IEJaD0y6+mDmGjWJmgRuG1kwBoGwii37GMrDCOyOWc4n5wHltyYrhr6JaE1bshrH
P46z2U5LSkM0/7cm+yEgdYcSXYcMpt36+xOcFyFw12N5nyp82Tntcwf4848FsyQ1sH
Suma13i38E6sd0ZuMr8f0sF66hdS4zj446h04nWmas7IaoSAbGkXga17KhG9rjv
x93MwOhbaNq1/8bhnxsA7fCmIy/7impyx5uyJWFWSBMp1hPBvWmx7A8sAs9BMShh
nbG61gik4h0Q8k9/mw9o2lyrUR4pE8Pc2vTnvPdr3tLSmgszgUzE9L8Q/CFU
fbtsFmbf0bgEuhn8c6vdfyIDYAFABH1gpywqUUtCq7Akk2nqojq5sCxezv915ReBeD
aad984A16e2oks5+VR/Q08pRwWj1PMS5bUeAhE7SoyIjImUjkwqGqFyFyDrdMrqjm
jDe+LmYbH9Q9xriF1N8zuc+48fY8C8oeBeHiN5Apm1P8YPVPnUnt3+jQNC7+v+can7vNI+
La8q1Tn+1j15f44a231Y/pulgtxRwXt+PrxTQ6839Eai5LyN8amPwonw375ZIA
MJrXwEkl44de74zd8sEBvZ2m44riH8MFyjYAWysey80crp0emssxarz+72a67r
```
Appendix B. ASN.1 Module

This appendix documents ASN.1 [x680] [x681] [x682] [x683] [x690] types, values, and object sets for this specification. It does so by providing an ASN.1 module called PKCS12-PBMAC1-2023. Combine this module with the PKCS-12 ASN.1 module found in Appendix C of [RFC7292] and the pkcs5v2-1 ASN.1 module in Appendix D of [RFC8018] to add SHA-2-based HMACs by replacing the PBKDF2-PRFs class referenced from [RFC7292].
BEGIN
IMPORTS

AlgorithmIdentifier, ALGORITHM-IDENTIFIER, rsadsi
FROM PKCS5v2-1 -- From [RFC8018]
   { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-5(5)
     modules(16) pkcs5v2-1(2) }
;
-- object identifier arcs
pkcs OBJECT IDENTIFIER ::= { rsadsi 1 }
pkcs-5 OBJECT IDENTIFIER ::= { pkcs 5 }
digestAlgorithm OBJECT IDENTIFIER ::= { rsadsi 2 }
-- HMAC object identifiers
id-hmacWithSHA1 OBJECT IDENTIFIER ::= { digestAlgorithm 7 }
id-hmacWithSHA224 OBJECT IDENTIFIER ::= { digestAlgorithm 8 }
id-hmacWithSHA256 OBJECT IDENTIFIER ::= { digestAlgorithm 9 }
id-hmacWithSHA384 OBJECT IDENTIFIER ::= { digestAlgorithm 10 }
id-hmacWithSHA512 OBJECT IDENTIFIER ::= { digestAlgorithm 11 }
id-hmacWithSHA512-224 OBJECT IDENTIFIER ::= { digestAlgorithm 12 }
id-hmacWithSHA512-256 OBJECT IDENTIFIER ::= { digestAlgorithm 13 }
-- PBKDF2-PRF algorithm identifiers
PBKDF2-PRFs ALGORITHM-IDENTIFIER ::= {
   { NULL IDENTIFIED BY id-hmacWithSHA1 }       |
   { NULL IDENTIFIED BY id-hmacWithSHA224 }     |
   { NULL IDENTIFIED BY id-hmacWithSHA256 }     |
   { NULL IDENTIFIED BY id-hmacWithSHA384 }     |
   { NULL IDENTIFIED BY id-hmacWithSHA512 }     |
   { NULL IDENTIFIED BY id-hmacWithSHA512-224 } |
   { NULL IDENTIFIED BY id-hmacWithSHA512-256 },
   ...
}
-- HMAC algorithm identifiers
algid-hmacWithSHA1 AlgorithmIdentifier {{PBKDF2-PRFs}} ::= {
   algorithm id-hmacWithSHA1, parameters NULL : NULL }
algid-hmacWithSHA224 AlgorithmIdentifier {{PBKDF2-PRFs}} ::= {
   algorithm id-hmacWithSHA224, parameters NULL : NULL }
algid-hmacWithSHA256 AlgorithmIdentifier {{PBKDF2-PRFs}} ::=
{ algorithm id-hmacWithSHA256, parameters NULL : NULL }

algid-hmacWithSHA384 AlgorithmIdentifier {{PBKDF2-PRFs}} ::= 
{ algorithm id-hmacWithSHA384, parameters NULL : NULL }

algid-hmacWithSHA512 AlgorithmIdentifier {{PBKDF2-PRFs}} ::= 
{ algorithm id-hmacWithSHA512, parameters NULL : NULL }

algid-hmacWithSHA512-224 AlgorithmIdentifier {{PBKDF2-PRFs}} ::= 
{ algorithm id-hmacWithSHA512-224, parameters NULL : NULL }

algid-hmacWithSHA512-256 AlgorithmIdentifier {{PBKDF2-PRFs}} ::= 
{ algorithm id-hmacWithSHA512-256, parameters NULL : NULL }

-- PBMAC1-params

PBMAC1-params ::= SEQUENCE {
    keyDerivationFunc AlgorithmIdentifier {{PBMAC1-KDFs}},
    messageAuthScheme AlgorithmIdentifier {{PBMAC1-MACs}}
}

PBMAC1-KDFs ALGORITHM-IDENTIFIER ::= { ... }

PBMAC1-MACs ALGORITHM-IDENTIFIER ::= { ... }

id-PBKDF2 OBJECT IDENTIFIER ::= { pkcs-5 12 }

PKDF2-params ::= SEQUENCE {
    salt CHOICE {
        specified OCTET STRING,
        otherSource AlgorithmIdentifier {{PKDF2-SaltSources}}
    },
    iterationCount INTEGER (1..MAX),
    keyLength INTEGER (1..MAX) OPTIONAL,
    prf AlgorithmIdentifier {{PKDF2-PRFs}} DEFAULT algid-hmacWithSHA1
}

PKDF2-SaltSources ALGORITHM-IDENTIFIER ::= { ... }

END

Author's Address

Hubert Kario
Red Hat, Inc.
Purkynova 115
61200 Brno
Czech Republic
Email: hkario@redhat.com