Stream: Internet Engineering Task Force (IETF)
RFC: 9579
Updates: 7292, 8018
Category: Informational
Published: May 2024
ISSN: 2070-1721
Author: H. Kario
Red Hat, Inc.

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

Table of Contents

1. Introduction 3
2. Rationale 3
3. Requirements Language 3
4. Embedding PBMAC1 in PKCS #12 3
5. Recommended Parameters 4
6. Password Encoding 4
7. Deprecated Algorithms 4
8. IANA Considerations 4
9. Security Considerations 5
10. References 5
10.1. Normative References 5
10.2. Informative References 6
Appendix A. Test Vectors 6
A.1. Valid PKCS #12 File with SHA-256 HMAC and PRF 6
A.2. Valid PKCS #12 File with SHA-256 HMAC and SHA-512 PRF 8
A.3. Valid PKCS #12 File with SHA-512 HMAC and PRF 9
A.4. Invalid PKCS #12 File with Incorrect Iteration Count 10
A.5. Invalid PKCS #12 File with Incorrect Salt 11
A.6. Invalid PKCS #12 File with Missing Key Length 12
Appendix B. ASN.1 Module 13
Author's Address 15

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 for 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.

Decimal	Description	Reference
76	id-pkcs12-pbmac1-2023	RFC 9579

Table 1

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

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997, <https://www.rfc-editor.org/info/rfc2104>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC6194] Polk, T., Chen, L., Turner, S., and P. Hoffman, "Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms", RFC 6194, DOI 10.17487/RFC6194, March 2011, <https://www.rfc-editor.org/info/rfc6194>.

[RFC7292] Moriarty, K., Ed., Nystrom, M., Parkinson, S., Rusch, A., and M. Scott, "PKCS #12: Personal Information Exchange Syntax v1.1", RFC 7292, DOI 10.17487/RFC7292, July 2014, <https://www.rfc-editor.org/info/rfc7292>.

[RFC8018] Moriarty, K., Ed., Kaliski, B., and A. Rusch, "PKCS #5: Password-Based Cryptography Specification Version 2.1", RFC 8018, DOI 10.17487/RFC8018, January 2017, <https://www.rfc-editor.org/info/rfc8018>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[SHA2] National Institute of Standards and Technology (NIST), "Secure Hash Standard (SHS)", FIPS PUB 180-4, DOI 10.6028/NIST.FIPS.180-4, August 2015, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>.

[x680] ITU-T, "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, ISO/IEC 8824-1:2021, February 2021, <https://www.itu.int/rec/T-REC-X.680>.

[x681] ITU-T, "Information technology - Abstract Syntax Notation One (ASN.1): Information object specification", ITU-T Recommendation X.681, ISO/IEC 8824-2:2021, February 2021, <https://www.itu.int/rec/T-REC-X.681>.

[x682] ITU-T, "Information technology - Abstract Syntax Notation One (ASN.1): Constraint specification", ITU-T Recommendation X.682, ISO/IEC 8824-3:2021, February 2021, <https://www.itu.int/rec/T-REC-X.682>.

[x683] ITU-T, "Information technology - Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications", ITU-T Recommendation X.683, ISO/IEC 8824-4:2021, February 2021, <https://www.itu.int/rec/T-REC-X.683>.

[x690] ITU-T, "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, ISO/IEC 8825-1:2021, February 2021, <https://www.itu.int/rec/T-REC-X.690>.

10.2. Informative References

[RFC7914] Percival, C. and S. Josefsson, "The scrypt Password-Based Key Derivation Function", RFC 7914, DOI 10.17487/RFC7914, August 2016, <https://www.rfc-editor.org/info/rfc7914>.

[SHA3] National Institute of Standards and Technology (NIST), "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions", FIPS PUB 202, DOI 10.6028/NIST.FIPS.202, August 2015, <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf>.

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.

```
MIIKigIBAzCCCgUGCSqGSIb3DQEHAaCCCfYEggnyMIIJ7jCCBGIGCSqGSIb3DQEH
BqCCBFMwggRPAgEAMIIESAYJKoZIhvcNAQcBMFcGCSqGSIb3DQEFDTBKMCkGCSqG
SIb3DQEFDDAcBAg9pxXxY2yscwICCAAwDAYIKoZIhvcNAgkFADAdBglghkgBZQME
ASoEEK7yYaFQDi1pYwWzm9F/fs+AggPgFIT2XapyaFgDppdvLkdvaF3HXw+zjzKb
7xFC76DtVPhVTWVHD+kIss+jsj+XyvMwY0aCuAhAG/Dig+vzWomnsqB5ssw5/kTb
+TMQ5PXLkNeoBmB6ArKeGc/QmCBQvQG/a6b+nXSWmxNpP+71772dmWmB8gcSJ0kF
Fj75NrIbmNiDMCb71Q8gOzBMFf6BpXf/3xWAJtxyic+tSNETfOJa8zTZb0+lV0w9
5eUmDrPUpuxEVbb0KJtIc63gRkcfrPtDd6Ii4Zzbzj2Evr4/S4hnrQBsiryVzJWy
IEjaD0y6+DmG0JwMgRuGi1wBoGowi37GMrDCOyOZWC4n5wHLtYyhR6JaElxbrhxP
H46z2USLKmZoF+YgEQgYcSBXMgP0t36+XQocFWYi2N5niy02TnctwF430FYsQlhJ
Suma4I33E808dJuMv8T/soF66HsD4Zj46hOf4nWmas7IaoSAbGKXgIa7KhGRJvij
xM3WOX0aqNi/8bhnxSA7fCmIy/7opyx5UYJFWGBSmHP1pBHBVmx7Ad8SAsB9MSsh
nbGjGiUk4h0QcOi29/M9WwFlo4urePyI8PK2qtVAmpD3rTLlsmgzguZ69L0Q/CFU
fbtqsMF0bgEuh8cfivd1DYFABEt1gypuwCUtCqQ7AXK2nQqOjsQCxVz9i9K8NDeD
aau98VAl0To2sk3/VR/QUq0PRwU1jPN5BzUevhE7SOy/ImuJKwpGqqFljYdrQmj5
jDe+LmYH9QGVRlfN8zuU+48FY8CAoeBeHn5AAPml0PYPVUnt3/jQN1+v+CahNVI+
La8q1Nen+j1R44aa2I3y/pUgtzXRwK+tPrxTQbG030EU51LYJn8amPWmn3w75ZIA
MJrXWeKj44de7u4zdUsEBVC2uM44rIHM8MFjyYAwYsey0rcp0emsaxzar+7ZA67r
lDoXvvS3NqsnTXHcn3T9tkPRoee6L7Dh3x4Od96lcRwgdYT5BwyH7e34ld4VTUmJ
bDEq7Ijvn4JKrwQJh1RCC+Z/ObfkC42xAm7G010u3g08xB0QujpdG4a7VcuWrywF
c7hLNquuaF4qoDaVwYXHH3iuX6YlJ/3siTKbYCVXPEZOAMBP9lF/OU76UMJBQNfU
0xjDx+3AhUVgnGuCsmYlK6ETDp8qOZKGyV0KrNSGtqLx3uMhd7PETeW+ML3tDQ/0
X9fMkcZHi4C2fXnoHV/qa2dGhBj4jjQ0Xh1poU6mxGn2Mebe2hDsBZkkBpnn7pK4
wP/VqXdQTwqEuvzGHLVFsCuADe40ZFBmtBrf70wG7ZkO8SUZ8Zz1IX3+S024g7yj
QRev/6x6TtkwggWEBgkqhkiG9w0BBwGgggV1BIIFcTCCBW0wggVpBgsqhkiG9w0B
DAoBAqCCBTEwggUtMFcGCSqGSIb3DQEFDTBKMCkGCSqGSIb3DQEFDDAcBAhTxzw+
VptrYAICCAAwDAYIKoZIhvcNAgkFADAdBglghkgBZQMEASoEEK9nSqc1I2t4tMVG
bWHpdtQEggTQzCwI7j34gCTvfj6nuOSndAjShGv7mN2j7WMV0pslTpq2b9Bn3vn1
Y0JMvL4E7sLrUzNU02pdOcfCnEpMFccNv2sQrLp1mOCKxu8OjSqHZLoKVL0ROVsZ
8dMECLLigDlPKRiSyLErl14tErX4/zbkUaWMROO28kFbTbubQ8YoHlRUwsKW1xLg
vfi0gRkG/zHXRfQHjX/8NStv7hXlehn7/Gy2EKPsRFhadm/iUHAfmCMkMgHTU248
JER9+nsXltd59H+IeDpj/kbxZ+YvHow9XUZKu828d3MQnUpLZ1BfJGhMBPVwbVUD
A40CiQBVdCoGtPJyalL28xoS3H0ILFCnwQOr6u0HwleNJPGHq78HUyH6Hwxnh0b0
5o163r6wTFZn5cMOxpbs/Ttd+3TrxmrYpd2XnuRme3cnaYJ0ILvpc/8eLLR7SKjD
T4JhZ0h/CfcV2WWvhpQugkY0pWrZ+EIMneB1dZB96mJVLxOi148OeSgi0PsxZMNi
YM33rTpwQT5WqOsEyDwUQpne5b8Kkt/s7EN0LJNnPyJJRL1LcqOdr6j+6YqRtPa7
a9oWJqMcuTP+bqzGRJh+3HDlFBw2Yzp9iadv4KmB2MzhStLUoi2MSjvnnkkd5Led
sshAd6WbKfF7kLAHQHT4Ai6dMEO4EKkEVF9JBtxCR4JEn6C98Lpg+Lk+rfY7gHOf
ZxtgGURwgXRY3aLUrdT55ZKgk3ExVKPzi5EhdpAau7JKhpOwyKozAp/OKWMNrz6h
obu2Mbn1B+IA60psYHHxynBgsJHv7WQmbYh8HyGfHgVvaA8pZCYqxxjpLjSJrR8B
Bu9H9xkTh7KlhxgreXYv19uAYbUd95kcox9izad6VPnovgFSb+Omdy6PJACPj6hF
W6PJbucP0YPpO0VtWtQdZZ3df1P0hZ7qvKwOPFA+gKZSckgqASfygiP9V3Zc8jIi
wjNzoDM2QT+UUJKiiGYXJUEOO9hxzFHlGj759DcNRhpgl5AgR57ofISD9yBuCAJY
PQ/aZHPFuRTrcVG3RaIbCAS73nEznKyFaLOXfzyfyaSmyhsH253tnyL1MejC+2bR
Eko/yldgFUxvU5JI+Q3KJ6Awj+PnduHXx71E4UwSuu2xXYMpxnQwI6rroQpZBX82
HhqgcLV83P8lpzQwPdHjH5zkoxmWdC0+jU/tcQfNXYpJdyoaX7tDmVclLhwl9ps/
O841pIsNLJWXwvxG6B+3LN/kw4QjwN194PopiOD7+oDm5mhttO78CrBrRxHMD/0Q
qniZjKzSZepxlZq+J792u8vtMnuzzChxu0Bf3PhIXcJNcVhwUtr0yKe/N+NvC0tm
p8wyik/BlndxN9eKbdTOi2wIi64h2QG8nOk66wQ/PSIJYwZl6eDNEQSzH/1mGCfU
QnUT17UC/p+Qgenf6Auap2GWlvsJrB7u/pytz65rtjt/ouo6Ih6EwWqwVVpGXZD0
7gVWH0Ke/Vr6aPGNvkLcmftPuDZsn9jiig3guhdeyRVf10Ox369kKWcG75q77hxE
IzSzDyUlBNbnom9SIjut3r+qVYmWONatC6q/4D0I42Lnjd3dEyZx7jmH3g/S2ASM
FzWr9pvXc61dsYOkdZ4PYa9XPUZxXFagZsoS3F1sU799+IJVU0tC0MExJTAjBgkq
hkiG9w0BCRUxFgQUwWO5DorvVWYF3BWUmAw0rUEajScwfDBtMEkGCSqGSIb3DQEF
DjA8MCwGCSqGSIb3DQEFDDAfBAhvRzw4sC4xcwICCAACASAwDAYIKoZIhvcNAgkF
ADAMBggqhkiG9w0CCQUABCB6pW2FOdcCNj87zS64NUXG36K5aXDnFHctIk5Bf4kG
3QQITk9UIFVTRUQCAQE=
```

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.

```
MIIKigIBAzCCCgUGCSqGSIb3DQEHAaCCCfYEggnyMIIJ7jCCBGIGCSqGSIb3DQEH
BqCCBFMwggRPAgEAMIIESAYJKoZIhvcNAQcBMFcGCSqGSIb3DQEFDTBKMCkGCSqG
SIb3DQEFDDAcBAi4j6UBBY2iOgICCAAwDAYIKoZIhvcNAgkFADAdBglghkgBZQME
ASoEEFpHSS5zrk/9pkDo1JRbtE6AggPgtbMLGoFd5KLpVXMdcxLrT129L7/vCr0B
0I2tnhPPA7aFtRjjuGbwooCMQwxw9qzuCX1eH4xK2LUw6Gbd2H47WimSOWJMaiUb
wy4alIWELYufe74kXPmKPCyH92lN1hqu8s0EGhIl7nBhWbFzow1+qpIc9/lpujJo
wodSY+pNBD8oBeoU1m6DgOjgc62apL7m0nwavDUqEt7HAqtTBxKxu/3lpb1q8nbl
XLTqROax5feXErf+GQAqs24hUJIPg3O1eCMDVzH0h5pgZyRN9ZSIP0HC1i+d1lnb
JwHyrAhZv8GMdAVKaXHETbq8zTpxT3UE/LmH1gyZGOG2B21D2dvNDKa712sHOS/t
3XkFngHDLx+a9pVftt6p7Nh6jqI581tb7fyc7HBV9VUc/+xGgPgHZouaZw+I3PUz
fjHboyLQer22ndBz+l1/S2GhhZ4xLXg4l0ozkgn7DX92S/UlbmcZam1apjGwkGY/
7ktA8BarNW211mJF+Z+hci+BeDiM7eyEguLCYRdH+/UBiUuYjG1hi5Ki3+42pRZD
FZkTHGOrcG6qE2KJDsENj+RkGiylG98v7flm4iWFVAB78AlAogT38Bod40evR7Ok
c48sOIW05eCH/GLSO0MHKcttYUQNMqIDiG1TLzP1czFghhG97AxiTzYkKLx2cYfs
pgg5PE9drq1fNzBZMUmC2bSwRhGRb5PDu6meD8uqvjxoIIZQAEV53xmD63umlUH1
jhVXfcWSmhU/+vV/IWStZgQbwhF7DmH2q6S8itCkz7J7Byp5xcDiUOZ5Gpf9RJnk
DTZoOYM5iA8kte6KCwA+jnmCgstI5EbRbnsNcjNvAT3q/X776VdmnehW0VeL+6k4
z+GvQkr+D2sxPpldIb5hrb+1rcp9nOQgtpBnbXaT16Lc1HdTNe5kx4ScujXOWwfd
Iy6bR6H0QFq2SLKAAC0qw4E8h1j3WPxll9e0FXNtoRKdsRuX3jzyqDBrQ6oGskkL
wnyMtVjSX+3c9xbFc4vyJPFMPwb3Ng3syjUDrOpU5RxaMEAWt4josadWKEeyIC2F
wrS1dzFn/5wv1g7E7xWq+nLq4zdppsyYOljzNUbhOEtJ2lhme3NJ45fxnxXmrPku
gBda1lLf29inVuzuTjwtLjQwGk+usHJm9R/K0hTaSNRgepXnjY0cIgS+0gEY1/BW
k3+Y4GE2JXds2cQToe5rCSYH3QG0QTyUAGvwX6hAlhrRRgUG3vxtYSixQ3UUuwzs
eQW2SUFLl1611lJ7cQwFSPyr0sL0p81vdxWiigwjkfPtgljZ2QpmzR5rX2xiqItH
Dy4E+iVigIYwggWEBgkqhkiG9w0BBwGgggV1BIIFcTCCBW0wggVpBgsqhkiG9w0B
DAoBAqCCBTEwggUtMFcGCSqGSIb3DQEFDTBKMCkGCSqGSIb3DQEFDDAcBAhDiwsh
4wt3aAICCAAwDAYIKoZIhvcNAgkFADAdBglghkgBZQMEASoEELNFnEpJT65wsXwd
fZ1g56cEggTQRo04bP/fWfPPZrTEczq1qO1HHV86j76Sgxau2WQ9OQAG998HFtNq
NxO8R66en6QFhqpWCI73tSJD+oA29qOsT+Xt2bR2z5+K7D4QoiXuLa3gXv62VkjB
0DLCHAS7Mu+hkp5OKCpXCS7fo0OnAiQjM4EluAsiwwLrHu7z1E16UwpmlgKQnaC1
S44fV9znS9TxofRTnuCq1lupdn2qQjSydOU6inQeKLBflKRiLrJHOobaFmjWwp1U
OQAMuZrALhHyIbOFXMPYk3mmU/1UPuRGcbcV5v2Ut2UME+WYExXSCOYR3/R4UfVk
IfEzeRPFs2slJMIDS2fmMyFkEEElBckhKO9IzhQV3koeKUBdM066ufyax/uIyXPm
MiB9fAqbQQ4jkQTT80bKkBAP1Bvyg2L8BssstR5iCoZgWnfA9Uz4RI5GbRqbCz7H
iSkuOIowEqOox3IWbXty5VdWBXNjZBHpbE0CyMLSH/4QdGVw8R0DiCAC0mmaMaZq
32yrBR32E472N+2KaicvX31MwB/LkZN46c34TGanL5LJZx0DR6ITjdNgP8TlSSrp
7y2mqi7VbKp/C/28Cj5r+m++Gk6EOUpLHsZ2d2hthrr7xqoPzUAEkkyYWedHJaoQ
TkoIisZb0MGlXb9thjQ8Ee429ekfjv7CQfSDS6KTE/+mhuJ33mPz1ZcIacHjdHhE
6rbrKhjSrLbgmrGa8i7ezd89T4EONu0wkG9KW0wM2cn5Gb12PF6rxjTfzypG7a50
yc1IJ2Wrm0B7gGuYpVoCeIohr7IlxPYdeQGRO/SlzTd0xYaJVm9FzJaMNK0ZqnZo
QMEPaeq8PC3kMjpa8eAiHXk9K3DWdOWYviGVCPVYIZK6Cpwe+EwfXs+2hZgZlYzc
vpUWg60md1PD4UsyLQagaj37ubR6K4C4mzlhFx5NovV/C/KD+LgekMbjCtwEQeWy
agev2l9KUEz73/BT4TgQFM5K2qZpVamwmsOmldPpekGPiUCu5YxYg/y4jUKvAqj1
S9t4wUAScCJx8OvXUfgpmS2+mhFPBiFps0M4O3nWG91Q6mKMqbNHPUcFDn9P7cUh
s1xu3NRLyJ+QIfVfba3YBTV8A6WBYEmL9lxf1uL1WS2Bx6+Crh0keyNUPo9cRjpx
1oj/xkInoc2HQODEkvuK9DD7VrLr7sDhfmJvr1mUfJMQ5/THk7Z+E+NAuMdMtkM2
yKXxghZAbBrQkU3mIW150i7PsjlUw0o0/LJvQwJIsh6yeJDHY8mby9mIdeP3LQAF
clYKzNwmgwbdtmVAXmQxLuhmEpXfstIzkBrNJzChzb2onNSfa+r5L6XEHNHl7wCw
TuuV/JWldNuYXLfVfuv3msfSjSWkv6aRtRWIvmOv0Qba2o05LlwFMd1PzKM5uN4D
DYtsS9A6yQOXEsvUkWcLOJnCs8SkJRdXhJTxdmzeBqM1JttKwLbgGMbpjbxlg3ns
```

```
N+Z+sEFox+2ZWOglgnBHj0mCZOiAC8wqUu+sxsLT4WndaPWKVqoRQChvDaZaNOaN
qHciF9HPUcfZow+fH8TnSHneiQcDe6XcMhSaQ2MtpY8/jrgNKguZt22yH9gw/VpT
3/QOB7FBgKFIEbvUaf3nVjFIlryIheg+LeiBd2isoMNNXaBwcg2YXukxJTAjBgkq
hkiG9w0BCRUxFgQUwWO5DorvVWYF3BWUmAw0rUEajScwfDBtMEkGCSqGSIb3DQEF
DjA8MCwGCSqGSIb3DQEFDDAfBAgUr2yP+/DBrgICCAACASAwDAYIKoZIhvcNAgsF
ADAMBggqhkiG9w0CCQUABCA5zFL93jw8ItGlcbHKhqkNwbgpp6layuOuxSju4/Vd
6QQITk9UIFVTRUQCAQE=
```

A.3. Valid PKCS #12 File with SHA-512 HMAC and PRF

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

```
MIIKrAIBAzCCCgUGCSqGSIb3DQEHAaCCCfYEggnyMIIJ7jCCBGIGCSqGSIb3DQEH
BqCCBFMwggRPAgEAMIIESAYJKoZIhvcNAQcBMFcGCSqGSIb3DQEFDTBKMCkGCSqG
SIb3DQEFDDAcBAisrqL8obSBaQICCAAwDAYIKoZIhvcNAgkFADAdBglghkgBZQME
ASoEECjXYYca0pwsgn1Imb9WqFGAggPgT7RcF5YzEJANZU9G3tSdpCHnyWatTlhm
iCEcBGgwI5gz0+GoX+JCojgYY4g+KxeqznyCu+6GeD00T4Em7SWme9nzAfBFzng0
3lYCSnahSEKfgHerbzAtq9kgXkclPVk0Liy92/buf0Mqotjjs/5o78AqP86Pwbj8
xYNuXOU1ivO0JiW2c2HefKYvUvMYlOh99LCoZPLHPkaaZ4scAwDjFeTICU8oowVk
LKvslrg1pHbfmXHMFJ4yqub37hRtj2CoJNy4+UA2hBYlBi9WnuAJIsjv0qS3kpLe
4+J2DGe31GNG8pD01XD0l69OlailK1ykh4ap2u0KeD2z357+trCFbpWMMXQcSUCO
OcVjxYqgv/l1++9huOHoPSt224x4wZfJ7cO2zbAAx/K2CPhdvi4CBaDHADsRq/c8
SAi+LX5SCocGT51zL5KQD6pnr2ExaVum+U8a3nMPPMv9R2MfFUksYNGgFvS+lcZf
R3qk/G9iXtSgray0mwRA8pWzoXl43vc9HJuuCU+ryOc/h36NChhQ9ltivUNaiUc2
b9AAQSrZD8Z7KtxjbH3noS+gjDtimDB0Uh199zaCwQ95y463zdYsNCESm1OT979o
Y+81BWFMFM/Hog5s7Ynhoi2E9+ZlyLK2UeKwvWjGzvcdPvxHR+5l/h6PyWROlpaZ
zmzZBm+NKmbXtMD2AEa5+Q32ZqJQhijXZyIji3NS65y81j/a1ZrvU0lOVKA+MSPN
KU27/eKZuF1LEL6qaazTUmpznLLdaVQy5aZ1qz5dyCziKcuHIclhh+RCblHU6XdE
6pUTZSRQQiGUIkPUTnU9SFlZc7VwvxgeynLyXPCSzOKNWYGajy1LxDvv28uhMgNd
WF51bNkl1QYl0fNunGO7YFt4wk+g7CQ/Yu2w4P7S3ZLMw0g4eYclcvyIMt4vxXfp
VTKIPyzMqLr+0dp1eCPm8fIdaBZUhMUC/OVqLwgnPNY9cXCrn2R1cGKo5LtvtjbH
2skz/D5DIOErfZSBJ8LE3De4j8MAjOeC8ia8LaM4PNfW/noQP1LBsZtTDTqEy01N
Z5uliIocyQzlyWChErJv/Wxh+zBpbk1iXc2Owmh2GKjx0VSe7XbiqdoKkONUNUIE
siseASiU/oXdJYUnBYVEUDJ1HPz7qnKiFhSgxNJZnoPfzbbx1hEzV+wxQqNnWIqQ
U0s7Jt22wDBzPBHGao2tnGRLuBZWVePJGbsxThGKwrf3vYsNJTxme5KJiaxcPMwE
r+ln2AqVOzzXHXgIxv/dvK0Qa7pH3AvGzcFjQChTRipgqiRrLor0//8580h+Ly2l
IFo7bCuztmcwggWEBgkqhkiG9w0BBwGgggV1BIIFcTCCBW0wggVpBgsqhkiG9w0B
DAoBAqCCBTEwggUtMFcGCSqGSIb3DQEFDTBKMCkGCSqGSIb3DQEFDDAcBAi1c7S5
IEG77wICCAAwDAYIKoZIhvcNAgkFADAdBglghkgBZQMEASoEEN6rzRtIdYxqOnY+
aDS3AFYEggTQNdwUoZDXCryOFBUI/z71vfoyAxlnwJLRHNXQUlI7w0KkH22aNnSm
xiaXHoCP1HgcmsYORS7p/ITi/9atCHqnGR4zHmePNhoMpNHFehdjlUUWgt004vUJ
5ZwTdXweM+K4We6CfWA/tyvsyGNAsuunel+8243Zsv0mGLKpjA+ZyALt51s0knmX
OD2DW49FckImUVnNC5LmvEIAmVC/ZNycryZQI+2EBkJKe+BC3834GexJnSwtUBg3
Xg33ZV7X66kw8tK1Ws5zND5GQAJyIu47mnjZkIWQBY+XbWowrBZ8uXIQuxMZC0p8
u62oIAtZaVQoVTR1LyR/7PISFW6ApwtbTn6uQxsb16qF8lEM0S1+x0AfJY6Zm11t
yCqbb2tYZF+X34MoUkR/IYC/KCq/KJdpnd8Yqgfrwjg8dR2WGIxbp2GBHq6BK/DI
ehOLMcLcsOuP0DEXppfcelMOGNIs+4h4KsjWiHVDMPsqLdozBdm6FLGcno3lY5FO
+avVrlElAOB+9evgaBbD2lSrEMoOjAoD090tgXXwYBEnWnIpdk+56cf5IpshrLBA
/+H13LBLes+X1o5dd0Mu+3abp5RtAv7zLPRRtXkDYJPzgNcTvJ2Wxw2C+zrAclzZ
7IRdcLESUa4CsN01aEvQgOtkCNVjSCtkJGP0FstsWM4hP7lfSB7P2tDL+ugy6GvB
X1sz9fMC7QMAFL98nDm/yqcnejG1BcQXZho8n0svSfbcVByGlPZGMuI9t25+0B2M
TAx0f6zoD8+fFmhcVgS6MQPybGKFawckYl0zulsePqs+G4voIW17owGKsRiv06Jm
ZSwd3KoGmjM49ADzuG9yrQ5PSa0nhVk1tybNape4HNYHrAmmN0ILlN+E0Bs/Edz4
ntYZuoc/Z35tCgm79dV4/Vl6HUZ1JrLsLrEWCByVytwVFyf3/MwTWdf+Ac+XzBuC
```

```
yEMqPlvnPWswdnaid35pxios79fPl1Hr0/Q6+DoA5GyYq8SFdP7EYLrGMGa5GJ+x
5nS7z6U4UmZ2sXuKYHnuhB0zi6Y04a+fhT71x02eTeC7aPlEB319UqysujJVJnso
bkcwOu/Jj0Is9YeFd693dB44xeZuYyvlwoD19lqcim0TSa2Tw7D1W/yu47dKrVP2
VKxRqomuAQOpoZiuSfq1/7ysrV8U4hIlIU2vnrSVJ8EtPQKsoBW5l70dQGwXyxBk
BUTHqfJ4LG/kPGRMOtUzgqFw2DjJtbym1q1MZgp2ycMon4vp7DeQLGs2XfEANB+Y
nRwtjpevqAnIuK6K3Y02LY4FXTNQpC37Xb04bmdIQAcE0MaoP4/hY87aS82PQ68g
3bI79uKo4we2g+WaEJlEzQ7147ZzV2wbDq89W69x1MWTfaDwlEtd4UaacYchAv7B
TVaaVFiRAUywWaHGePpZG2WV1feH/zd+temxWR9qMFgBZySg1jipBPVciwl0LqlW
s/raIBYmLmAaMMgM3759UkNVznDoFHrY4z2EADXp0RHHVzJS1x+yYvp/9I+AcW55
oN0UP/3uQ6eyz/ix22sovQwhMJ8rmgR6CfyRPKmXu1RPK3puNv7mbFTfTXpYN2vX
vhEZReXY8hJF/9o4G3UrJ1F0MgUHMCG86cw1z0bhPSaXVoufOnx/fRoxJTAjBgkq
hkiG9w0BCRUxFgQUwWO5DorvVWYF3BWUmAw0rUEajScwgZ0wgY0wSQYJKoZIhvcN
AQUOMDwwLAYJKoZIhvcNAQUMMB8ECFDaXOUaOcUPAgIIAAIBQDAMBggqhkiG9w0C
CwUAMAwGCCqGSIb3DQILBQAEQHIAM8C9OAsHUCj9CmOJioqf7YwD4O/b3UiZ3Wqo
F6OmQIRDc68SdkZJ6024l4nWlnhTE7a4lb2Tru4k3NOTa1oECE5PVCBVU0VEAgEB
```

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.

```
MIIKiwIBAzCCCgUGCSqGSIb3DQEHAaCCCfYEggnyMIIJ7jCCBGIGCSqGSIb3DQEH
BqCCBFMwggRPAgEAMIIESAYJKoZIhvcNAQcBMFcGCSqGSIb3DQEFDTBKMCkGCSqG
SIb3DQEFDDAcBAg9pxXxY2yscwICCAAwDAYIKoZIhvcNAgkFADAdBglghkgBZQME
ASoEEK7yYaFQDi1pYwWzm9F/fs+AggPgFIT2XapyaFgDppdvLkdvaF3HXw+zjzKb
7xFC76DtVPhVTWVHD+kIss+jsj+XyvMwY0aCuAhAG/Dig+vzWomnsqB5ssw5/kTb
+TMQ5PXLkNeoBmB6ArKeGc/QmCBQvQG/a6b+nXSWmxNpP+71772dmWmB8gcSJ0kF
Fj75NrIbmNiDMCb71Q8gOzBMFf6BpXf/3xWAJtxyic+tSNETfOJa8zTZb0+lV0w9
5eUmDrPUpuxEVbb0KJtIc63gRkcfrPtDd6Ii4Zzbzj2Evr4/S4hnrQBsiryVzJWy
IEjaD0y6+DmG0JwMgRuGi1wBoGowi37GMrDCOyOZWC4n5wHLtYyhR6JaElxbrhxP
H46z2USLKmZoF+YgEQgYcSBXMgP0t36+XQocFWYi2N5niy02TnctwF430FYsQlhJ
Suma4I33E808dJuMv8T/soF66HsD4Zj46hOf4nWmas7IaoSAbGKXgIa7KhGRJvij
xM3WOX0aqNi/8bhnxSA7fCmIy/7opyx5UYJFWGBSmHP1pBHBVmx7Ad8SAsB9MSsh
nbGjGiUk4h0QcOi29/M9WwFlo4urePyI8PK2qtVAmpD3rTLlsmgzguZ69L0Q/CFU
fbtqsMF0bgEuh8cfivd1DYFABEt1gypuwCUtCqQ7AXK2nQqOjsQCxVz9i9K8NDeD
aau98VAl0To2sk3/VR/QUq0PRwU1jPN5BzUevhE7SOy/ImuJKwpGqqFljYdrQmj5
jDe+LmYH9QGVRlfN8zuU+48FY8CAoeBeHn5AAPml0PYPVUnt3/jQN1+v+CahNVI+
La8q1Nen+j1R44aa2I3y/pUgtzXRwK+tPrxTQbG030EU51LYJn8amPWmn3w75ZIA
MJrXWeKj44de7u4zdUsEBVC2uM44rIHM8MFjyYAwYsey0rcp0emsaxzar+7ZA67r
lDoXvvS3NqsnTXHcn3T9tkPRoee6L7Dh3x4Od96lcRwgdYT5BwyH7e34ld4VTUmJ
bDEq7Ijvn4JKrwQJh1RCC+Z/ObfkC42xAm7G010u3g08xB0Qujpdg4a7VcuWrywF
c7hLNquuaF4qoDaVwYXHH3iuX6YlJ/3siTKbYCVXPEZOAMBP9lF/OU76UMJBQNfU
0xjDx+3AhUVgnGuCsmYlK6ETDp8qOZKGyV0KrNSGtqLx3uMhd7PETeW+ML3tDQ/0
X9fMkcZHi4C2fXnoHV/qa2dGhBj4jjQ0Xh1poU6mxGn2Mebe2hDsBZkkBpnn7pK4
wP/VqXdQTwqEuvzGHLVFsCuADe40ZFBmtBrf70wG7ZkO8SUZ8Zz1IX3+S024g7yj
QRev/6x6TtkwggWEBgkqhkiG9w0BBwGgggV1BIIFcTCCBW0wggVpBgsqhkiG9w0B
DAoBAqCCBTEwggUtMFcGCSqGSIb3DQEFDTBKMCkGCSqGSIb3DQEFDDAcBAhTxzw+
VptrYAICCAAwDAYIKoZIhvcNAgkFADAdBglghkgBZQMEASoEEK9nSqc1I2t4tMVG
bWHpdtQEggTQzCwI7j34gCTvfj6nuOSndAjShGv7mN2j7WMV0pslTpq2b9Bn3vn1
Y0JMvL4E7sLrUzNU02pdOcfCnEpMFccNv2sQrLp1mOCKxu8OjSqHZLoKVL0ROVsZ
8dMECLLigDlPKRiSyLErl14tErX4/zbkUaWMROO28kFbTbubQ8YoHlRUwsKW1xLg
vfi0gRkG/zHXRfQHjX/8NStv7hXlehn7/Gy2EKPsRFhadm/iUHAfmCMkMgHTU248
JER9+nsXltd59H+IeDpj/kbxZ+YvHow9XUZKu828d3MQnUpLZ1BfJGhMBPVwbVUD
A40CiQBVdCoGtPJyalL28xoS3H0ILFCnwQOr6u0HwleNJPGHq78HUyH6Hwxnh0b0
5o163r6wTFZn5cMOxpbs/Ttd+3TrxmrYpd2XnuRme3cnaYJ0ILvpc/8eLLR7SKjD
```

```
T4JhZ0h/CfcV2WWvhpQugkY0pWrZ+EIMneB1dZB96mJVLxOi148OeSgi0PsxZMNi
YM33rTpwQT5WqOsEyDwUQpne5b8Kkt/s7EN0LJNnPyJJRL1LcqOdr6j+6YqRtPa7
a9oWJqMcuTP+bqzGRJh+3HDlFBw2Yzp9iadv4KmB2MzhStLUoi2MSjvnnkkd5Led
sshAd6WbKfF7kLAHQHT4Ai6dMEO4EKkEVF9JBtxCR4JEn6C98Lpg+Lk+rfY7gHOf
ZxtgGURwgXRY3aLUrdT55ZKgk3ExVKPzi5EhdpAau7JKhpOwyKozAp/OKWMNrz6h
obu2Mbn1B+IA60psYHHxynBgsJHv7WQmbYh8HyGfHgVvaA8pZCYqxxjpLjSJrR8B
Bu9H9xkTh7KlhxgreXYv19uAYbUd95kcox9izad6VPnovgFSb+Omdy6PJACPj6hF
W6PJbucP0YPpO0VtWtQdZZ3df1P0hZ7qvKwOPFA+gKZSckgqASfygiP9V3Zc8jIi
wjNzoDM2QT+UUJKiiGYXJUEOO9hxzFHlGj759DcNRhpgl5AgR57ofISD9yBuCAJY
PQ/aZHPFuRTrcVG3RaIbCAS73nEznKyFaLOXfzyfyaSmyhsH253tnyL1MejC+2bR
Eko/yldgFUxvU5JI+Q3KJ6Awj+PnduHXx71E4UwSuu2xXYMpxnQwI6rroQpZBX82
HhqgcLV83P8lpzQwPdHjH5zkoxmWdC0+jU/tcQfNXYpJdyoaX7tDmVclLhwl9ps/
O841pIsNLJWXwvxG6B+3LN/kw4QjwN194PopiOD7+oDm5mhttO78CrBrRxHMD/0Q
qniZjKzSZepxlZq+J792u8vtMnuzzChxu0Bf3PhIXcJNcVhwUtr0yKe/N+NvC0tm
p8wyik/BlndxN9eKbdTOi2wIi64h2QG8nOk66wQ/PSIJYwZl6eDNEQSzH/1mGCfU
QnUT17UC/p+Qgenf6Auap2GWlvsJrB7u/pytz65rtjt/ouo6Ih6EwWqwVVpGXZD0
7gVWH0Ke/Vr6aPGNvkLcmftPuDZsn9jiig3guhdeyRVf10Ox369kKWcG75q77hxE
IzSzDyUlBNbnom9SIjut3r+qVYmWONatC6q/4D0I42Lnjd3dEyZx7jmH3g/S2ASM
FzWr9pvXc61dsYOkdZ4PYa9XPUZxXFagZsoS3F1sU799+IJVU0tC0MExJTAjBgkq
hkiG9w0BCRUxFgQUwWO5DorvVWYF3BWUmAw0rUEajScwfTBtMEkGCSqGSIb3DQEF
DjA8MCwGCSqGSIb3DQEFDDAfBAhvRzw4sC4xcwICCAECASAwDAYIKoZIhvcNAgkF
ADAMBggqhkiG9w0CCQUABCB6pW2FOdcCNj87zS64NUXG36K5aXDnFHctIk5Bf4kG
3QQITk9UIFVTRUQCAggA
```

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.

```
MIIKigIBAzCCCgUGCSqGSIb3DQEHAaCCCfYEggnyMIIJ7jCCBGIGCSqGSIb3DQEH
BqCCBFMwggRPAgEAMIIESAYJKoZIhvcNAQcBMFcGCSqGSIb3DQEFDTBKMCkGCSqG
SIb3DQEFDDAcBAg9pxXxY2yscwICCAAwDAYIKoZIhvcNAgkFADAdBglghkgBZQME
ASoEEK7yYaFQDi1pYwWzm9F/fs+AggPgFIT2XapyaFgDppdvLkdvaF3HXw+zjzKb
7xFC76DtVPhVTWVHD+kIss+jsj+XyvMwY0aCuAhAG/Dig+vzWomnsqB5ssw5/kTb
+TMQ5PXLkNeoBmB6ArKeGc/QmCBQvQG/a6b+nXSWmxNpP+71772dmWmB8gcSJ0kF
Fj75NrIbmNiDMCb71Q8gOzBMFf6BpXf/3xWAJtxyic+tSNETfOJa8zTZb0+lV0w9
5eUmDrPUpuxEVbb0KJtIc63gRkcfrPtDd6Ii4Zzbzj2Evr4/S4hnrQBsiryVzJWy
IEjaD0y6+DmG0JwMgRuGi1wBoGowi37GMrDCOyOZWC4n5wHLtYyhR6JaElxbrhxP
H46z2USLKmZoF+YgEQgYcSBXMgP0t36+XQocFWYi2N5niy02TnctwF430FYsQlhJ
Suma4I33E808dJuMv8T/soF66HsD4Zj46hOf4nWmas7IaoSAbGKXgIa7KhGRJvij
xM3WOX0aqNi/8bhnxSA7fCmIy/7opyx5UYJFWGBSmHP1pBHBVmx7Ad8SAsB9MSsh
nbGjGiUk4h0QcOi29/M9WwFlo4urePyI8PK2qtVAmpD3rTLlsmgzguZ69L0Q/CFU
fbtqsMF0bgEuh8cfivd1DYFABEt1gypuwCUtCqQ7AXK2nQqOjsQCxVz9i9K8NDeD
aau98VAl0To2sk3/VR/QUq0PRwU1jPN5BzUevhE7SOy/ImuJKwpGqqFljYdrQmj5
jDe+LmYH9QGVRlfN8zuU+48FY8CAoeBeHn5AAPml0PYPVUnt3/jQN1+v+CahNVI+
La8q1Nen+j1R44aa2I3y/pUgtzXRwK+tPrxTQbG030EU51LYJn8amPWmn3w75ZIA
MJrXWeKj44de7u4zdUsEBVC2uM44rIHM8MFjyYAwYsey0rcp0emsaxzar+7ZA67r
lDoXvvS3NqsnTXHcn3T9tkPRoee6L7Dh3x4Od96lcRwgdYT5BwyH7e34ld4VTUmJ
bDEq7Ijvn4JKrwQJh1RCC+Z/ObfkC42xAm7G010u3g08xB0Qujpdg4a7VcuWrywF
c7hLNquuaF4qoDaVwYXHH3iuX6YlJ/3siTKbYCVXPEZOAMBP9lF/OU76UMJBQNfU
0xjDx+3AhUVgnGuCsmYlK6ETDp8qOZKGyV0KrNSGtqLx3uMhd7PETeW+ML3tDQ/0
X9fMkcZHi4C2fXnoHV/qa2dGhBj4jjQ0Xh1poU6mxGn2Mebe2hDsBZkkBpnn7pK4
wP/VqXdQTwqEuvzGHLVFsCuADe40ZFBmtBrf70wG7ZkO8SUZ8Zz1IX3+S024g7yj
QRev/6x6TtkwggWEBgkqhkiG9w0BBwGgggV1BIIFcTCCBW0wggVpBgsqhkiG9w0B
DAoBAqCCBTEwggUtMFcGCSqGSIb3DQEFDTBKMCkGCSqGSIb3DQEFDDAcBAhTxzw+
```

```
VptrYAICCAAwDAYIKoZIhvcNAgkFADAdBglghkgBZQMEASoEEK9nSqc1I2t4tMVG
bWHpdtQEggTQzCwI7j34gCTvfj6nuOSndAjShGv7mN2j7WMV0pslTpq2b9Bn3vn1
Y0JMvL4E7sLrUzNU02pdOcfCnEpMFccNv2sQrLp1mOCKxu8OjSqHZLoKVL0ROVsZ
8dMECLLigDlPKRiSyLErl14tErX4/zbkUaWMROO28kFbTbubQ8YoHlRUwsKW1xLg
vfi0gRkG/zHXRfQHjX/8NStv7hXlehn7/Gy2EKPsRFhadm/iUHAfmCMkMgHTU248
JER9+nsXltd59H+IeDpj/kbxZ+YvHow9XUZKu828d3MQnUpLZ1BfJGhMBPVwbVUD
A40CiQBVdCoGtPJyalL28xoS3H0ILFCnwQOr6u0HwleNJPGHq78HUyH6Hwxnh0b0
5o163r6wTFZn5cMOxpbs/Ttd+3TrxmrYpd2XnuRme3cnaYJ0ILvpc/8eLLR7SKjD
T4JhZ0h/CfcV2WWvhpQugkY0pWrZ+EIMneB1dZB96mJVLxOi148OeSgi0PsxZMNi
YM33rTpwQT5WqOsEyDwUQpne5b8Kkt/s7EN0LJNnPyJJRL1LcqOdr6j+6YqRtPa7
a9oWJqMcuTP+bqzGRJh+3HDlFBw2Yzp9iadv4KmB2MzhStLUoi2MSjvnnkkd5Led
sshAd6WbKfF7kLAHQHT4Ai6dMEO4EKkEVF9JBtxCR4JEn6C98Lpg+Lk+rfY7gHOf
ZxtgGURwgXRY3aLUrdT55ZKgk3ExVKPzi5EhdpAau7JKhpOwyKozAp/OKWMNrz6h
obu2Mbn1B+IA60psYHHxynBgsJHv7WQmbYh8HyGfHgVvaA8pZCYqxxjpLjSJrR8B
Bu9H9xkTh7KlhxgreXYv19uAYbUd95kcox9izad6VPnovgFSb+Omdy6PJACPj6hF
W6PJbucP0YPpO0VtWtQdZZ3df1P0hZ7qvKwOPFA+gKZSckgqASfygiP9V3Zc8jIi
wjNzoDM2QT+UUJKiiGYXJUEOO9hxzFHlGj759DcNRhpgl5AgR57ofISD9yBuCAJY
PQ/aZHPFuRTrcVG3RaIbCAS73nEznKyFaLOXfzyfyaSmyhsH253tnyL1MejC+2bR
Eko/yldgFUxvU5JI+Q3KJ6Awj+PnduHXx71E4UwSuu2xXYMpxnQwI6rroQpZBX82
HhqgcLV83P8lpzQwPdHjH5zkoxmWdC0+jU/tcQfNXYpJdyoaX7tDmVclLhwl9ps/
O841pIsNLJWXwvxG6B+3LN/kw4QjwN194PopiOD7+oDm5mhttO78CrBrRxHMD/0Q
qniZjKzSZepxlZq+J792u8vtMnuzzChxu0Bf3PhIXcJNcVhwUtr0yKe/N+NvC0tm
p8wyik/BlndxN9eKbdTOi2wIi64h2QG8nOk66wQ/PSIJYwZl6eDNEQSzH/1mGCfU
QnUT17UC/p+Qgenf6Auap2GWlvsJrB7u/pytz65rtjt/ouo6Ih6EwWqwVVpGXZD0
7gVWH0Ke/Vr6aPGNvkLcmftPuDZsn9jiig3guhdeyRVf10Ox369kKWcG75q77hxE
IzSzDyUlBNbnom9SIjut3r+qVYmWONatC6q/4D0I42Lnjd3dEyZx7jmH3g/S2ASM
FzWr9pvXc61dsYOkdZ4PYa9XPUZxXFagZsoS3F1sU799+IJVU0tC0MExJTAjBgkq
hkiG9w0BCRUxFgQUwWO5DorvVWYF3BWUmAw0rUEajScwfDBtMEkGCSqGSIb3DQEF
DjA8MCwGCSqGSIb3DQEFDDAfBAhOT1QgVVNFRAICCAACASAwDAYIKoZIhvcNAgkF
ADAMBggqhkiG9w0CCQUABCB6pW2FOdcCNj87zS64NUXG36K5aXDnFHctIk5Bf4kG
3QQIb0c8OLAuMXMCAQE=
```

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.

```
MIIKiAIBAzCCCgUGCSqGSIb3DQEHAaCCCfYEggnyMIIJ7jCCBGIGCSqGSIb3DQEH
BqCCBFMwggRPAgEAMIIESAYJKoZIhvcNAQcBMFcGCSqGSIb3DQEFDTBKMCkGCSqG
SIb3DQEFDDAcBAg9pxXxY2yscwICCAAwDAYIKoZIhvcNAgkFADAdBglghkgBZQME
ASoEEK7yYaFQDi1pYwWzm9F/fs+AggPgFIT2XapyaFgDppdvLkdvaF3HXw+zjzKb
7xFC76DtVPhVTWVHD+kIss+jsj+XyvMwY0aCuAhAG/Dig+vzWomnsqB5ssw5/kTb
+TMQ5PXLkNeoBmB6ArKeGc/QmCBQvQG/a6b+nXSWmxNpP+71772dmWmB8gcSJ0kF
Fj75NrIbmNiDMCb71Q8gOzBMFf6BpXf/3xWAJtxyic+tSNETfOJa8zTZb0+lV0w9
5eUmDrPUpuxEVbb0KJtIc63gRkcfrPtDd6Ii4Zzbzj2Evr4/S4hnrQBsiryVzJWy
IEjaD0y6+DmG0JwMgRuGi1wBoGowi37GMrDCOyOZWC4n5wHLtYyhR6JaElxbrhxP
H46z2USLKmZoF+YgEQgYcSBXMgP0t36+XQocFWYi2N5niy02TnctwF430FYsQlhJ
Suma4I33E808dJuMv8T/soF66HsD4Zj46hOf4nWmas7IaoSAbGKXgIa7KhGRJvij
xM3WOX0aqNi/8bhnxSA7fCmIy/7opyx5UYJFWGBSmHP1pBHBVmx7Ad8SAsB9MSsh
nbGjGiUk4h0QcOi29/M9WwFlo4urePyI8PK2qtVAmpD3rTLlsmgzguZ69L0Q/CFU
fbtqsMF0bgEuh8cfivd1DYFABEt1gypuwCUtCqQ7AXK2nQqOjsQCxVz9i9K8NDeD
aau98VAl0To2sk3/VR/QUq0PRwU1jPN5BzUevhE7SOy/ImuJKwpGqqFljYdrQmj5
jDe+LmYH9QGVRlfN8zuU+48FY8CAoeBeHn5AAPml0PYPVUnt3/jQN1+v+CahNVI+
La8q1Nen+j1R44aa2I3y/pUgtzXRwK+tPrxTQbG030EU51LYJn8amPWmn3w75ZIA
MJrXWeKj44de7u4zdUsEBVC2uM44rIHM8MFjyYAwYsey0rcp0emsaxzar+7ZA67r
```

```
lDoXvvS3NqsnTXHcn3T9tkPRoee6L7Dh3x4Od96lcRwgdYT5BwyH7e34ld4VTUmJ
bDEq7Ijvn4JKrwQJh1RCC+Z/ObfkC42xAm7G010u3g08xB0Qujpdg4a7VcuWrywF
c7hLNquuaF4qoDaVwYXHH3iuX6YlJ/3siTKbYCVXPEZOAMBP9lF/OU76UMJBQNfU
0xjDx+3AhUVgnGuCsmYlK6ETDp8qOZKGyV0KrNSGtqLx3uMhd7PETeW+ML3tDQ/0
X9fMkcZHi4C2fXnoHV/qa2dGhBj4jjQ0Xh1poU6mxGn2Mebe2hDsBZkkBpnn7pK4
wP/VqXdQTwqEuvzGHLVFsCuADe40ZFBmtBrf70wG7ZkO8SUZ8Zz1IX3+S024g7yj
QRev/6x6TtkwggWEBgkqhkiG9w0BBwGgggV1BIIFcTCCBW0wggVpBgsqhkiG9w0B
DAoBAqCCBTEwggUtMFcGCSqGSIb3DQEFDTBKMCkGCSqGSIb3DQEFDDAcBAhTxzw+
VptrYAICCAAwDAYIKoZIhvcNAgkFADAdBglghkgBZQMEASoEEK9nSqc1I2t4tMVG
bWHpdtQEggTQzCwI7j34gCTvfj6nuOSndAjShGv7mN2j7WMV0pslTpq2b9Bn3vn1
Y0JMvL4E7sLrUzNU02pdOcfCnEpMFccNv2sQrLp1mOCKxu8OjSqHZLoKVL0ROVsZ
8dMECLLigDlPKRiSyLErl14tErX4/zbkUaWMROO28kFbTbubQ8YoHlRUwsKW1xLg
vfi0gRkG/zHXRfQHjX/8NStv7hXlehn7/Gy2EKPsRFhadm/iUHAfmCMkMgHTU248
JER9+nsXltd59H+IeDpj/kbxZ+YvHow9XUZKu828d3MQnUpLZ1BfJGhMBPVwbVUD
A40CiQBVdCoGtPJyalL28xoS3H0ILFCnwQOr6u0HwleNJPGHq78HUyH6Hwxnh0b0
5o163r6wTFZn5cMOxpbs/Ttd+3TrxmrYpd2XnuRme3cnaYJ0ILvpc/8eLLR7SKjD
T4JhZ0h/CfcV2WWvhpQugkY0pWrZ+EIMneB1dZB96mJVLxOi148OeSgi0PsxZMNi
YM33rTpwQT5WqOsEyDwUQpne5b8Kkt/s7EN0LJNnPyJJRL1LcqOdr6j+6YqRtPa7
a9oWJqMcuTP+bqzGRJh+3HDlFBw2Yzp9iadv4KmB2MzhStLUoi2MSjvnnkkd5Led
sshAd6WbKfF7kLAHQHT4Ai6dMEO4EKkEVF9JBtxCR4JEn6C98Lpg+Lk+rfY7gHOf
ZxtgGURwgXRY3aLUrdT55ZKgk3ExVKPzi5EhdpAau7JKhpOwyKozAp/OKWMNrz6h
obu2Mbn1B+IA60psYHHxynBgsJHv7WQmbYh8HyGfHgVvaA8pZCYqxxjpLjSJrR8B
Bu9H9xkTh7KlhxgreXYv19uAYbUd95kcox9izad6VPnovgFSb+Omdy6PJACPj6hF
W6PJbucP0YPpO0VtWtQdZZ3df1P0hZ7qvKwOPFA+gKZSckgqASfygiP9V3Zc8jIi
wjNzoDM2QT+UUJKiiGYXJUEOO9hxzFHlGj759DcNRhpgl5AgR57ofISD9yBuCAJY
PQ/aZHPFuRTrcVG3RaIbCAS73nEznKyFaLOXfzyfyaSmyhsH253tnyL1MejC+2bR
Eko/yldgFUxvU5JI+Q3KJ6Awj+PnduHXx71E4UwSuu2xXYMpxnQwI6rroQpZBX82
HhqgcLV83P8lpzQwPdHjH5zkoxmWdC0+jU/tcQfNXYpJdyoaX7tDmVclLhwl9ps/
O841pIsNLJWXwvxG6B+3LN/kw4QjwN194PopiOD7+oDm5mhttO78CrBrRxHMD/0Q
qniZjKzSZepxlZq+J792u8vtMnuzzChxu0Bf3PhIXcJNcVhwUtr0yKe/N+NvC0tm
p8wyik/BlndxN9eKbdTOi2wIi64h2QG8nOk66wQ/PSIJYwZl6eDNEQSzH/1mGCfU
QnUT17UC/p+Qgenf6Auap2GWlvsJrB7u/pytz65rtjt/ouo6Ih6EwWqwVVpGXZD0
7gVWH0Ke/Vr6aPGNvkLcmftPuDZsn9jiig3guhdeyRVf10Ox369kKWcG75q77hxE
IzSzDyUlBNbnom9SIjut3r+qVYmWONatC6q/4D0I42Lnjd3dEyZx7jmH3g/S2ASM
FzWr9pvXc61dsYOkdZ4PYa9XPUZxXFagZsoS3F1sU799+IJVU0tC0MExJTAjBgkq
hkiG9w0BCRUxFgQUwWO5DorvVWYF3BWUmAw0rUEajScwejBqMEYGCSqGSIb3DQEF
DjA5MCkGCSqGSIb3DQEFDDAcBAhvRzw4sC4xcwICCAAwDAYIKoZIhvcNAgkFADAM
BggqhkiG9w0CCQUABCB6pW2FOdcCNj87zS64NUXG36K5aXDnFHctIk5Bf4kG3QQI
b0c8OLAuMXMCAggA
```

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 D of [RFC7292] and the pkcs5v2-1 ASN.1 module in Appendix C of [RFC8018] to add SHA-2-based HMACs by replacing the PBKDF2-PRFs class referenced from [RFC7292].

```
PKCS12-PBMAC1-2023
  { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
    smime(16) id-mod(0) id-pkcs12-pbmac1-2023(76) }

DEFINITIONS EXPLICIT TAGS ::=
```

```
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 ::= {
  { PBKDF2-params IDENTIFIED BY id-PBKDF2},
  ...
}

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

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

PBKDF2-params ::= SEQUENCE {
  salt CHOICE {
    specified OCTET STRING,
    otherSource AlgorithmIdentifier {{PBKDF2-SaltSources}}
  },
  iterationCount INTEGER (1..MAX),
  keyLength INTEGER (1..MAX) OPTIONAL,
  prf AlgorithmIdentifier {{PBKDF2-PRFs}} DEFAULT algid-hmacWithSHA1
}

PBKDF2-SaltSources ALGORITHM-IDENTIFIER ::= { ... }

END
```

Author's Address

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