PKCS #9 v2.0 Amendment 1 – Draft 1

RSA Laboratories

DRAFT 1 – November 12, 2002

Editor's note: This is the first draft of PKCS #9 v2.0 Amendment 1, which is available for a 30-day public review period (deadline: December 13, 2002). Please send comments and suggestions, both technical and editorial, to pkcs-tng@rsasecurity.com.

Table of Contents

000-000000-000-000-000

1. Scope

This amendment documents the changes to PKCS #9 v2.0 ([3]) needed to protect signers using tokens with presentation capabilities (such as Personal Trusted Devices [2]) from certain attacks. It does so by defining a new authenticated attribute.

2. Background

PKCS #11 v2.11 Amendment 1 [4], introduced the concept of Personal Trusted Devices (PTDs) and a signature mechanism, CKM_CMS_SIG, aimed to allow users to benefit from such devices. A PTD that receives a message to sign through this mechanism may, depending on the message's content type [1], be able to securely present the message to the signer before asking for authorization.

When the message to sign is not a media object itself, the recipient will have to rely on the caller's stated content type when determining the presentation mechanism. Since the stated content type is not included in the signature, there is a possibility for an attack where the caller may take advantage of differences in presentation mechanisms for various content types in the PTD.

By defining an (authenticated) attribute intended to carry the alleged media type, this amendment presents one method to protect against such attacks. Note that for this method to succeed, a PTD must not allow the caller to assign the value of this attribute directly; the value must be the caller's *stated* content type, which was used by the PTD to decide on a particular presentation mechanism.

3. Changes to Section 5.3, "Attribute types for use in PKCS #7 data"

[Add a new section 5.3.7 as follows:]

5.3.7 Alleged content type

The **allegedContentType** attribute type specifies the content type provided by the party requesting a signature. It is intended for use in **SignedData** values, and must be an authenticated attribute.

```
allegedContentType ATTRIBUTE ::= {
        WITH SYNTAX AllegedContentType
        EQUALITY MATCHING RULE caseIgnoreMatch
        SINGLE VALUE TRUE
        ID pkcs-9-at-allegedContentType
}

AllegedContentType ::= UTF8String
```

As indicated, the attribute must have a single attribute value.

4. Changes to Appendix A, "ASN.1 module"

[Add the following ASN.1 value assignment right after the ***pkcs-9-at-pkcs7PDU*** *value assignment:]*

```
pkcs-9-at-allegedContentType OBJECT IDENTIFIER ::= {pkcs-9-at TBD}
```

*[Add the following ASN.1 type definitions right after the **counterSignature** type definition:]*

```
allegedContentType ATTRIBUTE ::= {
        WITH SYNTAX AllegedContentType
        EQUALITY MATCHING RULE caseIgnoreMatch
        SINGLE VALUE TRUE
        ID pkcs-9-at-allegedContentType
}

AllegedContentType ::= UTF8String
```

5. Changes to Appendix B.3, "Attribute types"

[Add a new section B.3.19 as follows:]

B.3.19 allegedContentType

In the (highly unlikely) event that this attribute is to be stored in a directory, it is to be stored and requested in binary form, as `allegedContentType;binary`. Attribute values shall be stored as binary (BER- or DER-encoded) data.

```
(
      1.2.840.113549.1.9.25.TBD
      NAME 'allegedContentType'
      DESC 'PKCS #7 alleged content type'
      SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
)
```

A. Intellectual property considerations

RSA Security makes no patent claims on the general constructions described in this document, although specific underlying techniques may be covered.

License to copy this document is granted provided that it is identified as "RSA Security Inc. Public-Key Cryptography Standards (PKCS)" in all material mentioning or referencing this document.

RSA Security makes no representations regarding intellectual property claims by other parties. Such determination is the responsibility of the user.

B. References

[1] Freed, N., and N. Borenstein, "*Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies*," IETF RFC 2045, November 1996. URL: http://ietf.org/rfc/rfc2045.txt.

[2] "*MeT PTD Definition – Personal Trusted Device Definition*," Version 1.0, 21 February 2001. URL: http://www.mobiletransaction.org.

[3] RSA Laboratories. *PKCS #9: Selected Object Classes and Attribute Types*. Version 2.0, February 2000. URL: ftp://ftp.rsasecurity.com/pub/pkcs/.

[4] RSA Laboratories, PKCS #11 v2.11 Amendment 1, August 2002. URL: ftp://ftp.rsasecurity.com/pub/pkcs/.

C. About PKCS

The *Public-Key Cryptography Standards* are specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide for the purpose of accelerating the deployment of public-key cryptography. First published in 1991 as a result of meetings with a small group of early adopters of public-key technology, the PKCS documents have become widely referenced and implemented. Contributions from the PKCS series have become part of many formal and *de facto* standards, including ANSI X9 documents, PKIX, SET, S/MIME, and SSL.

Further development of PKCS occurs through mailing list discussions and occasional workshops, and suggestions for improvement are welcome. For more information, contact:

PKCS Editor
RSA Laboratories
174 Middlesex Turnpike
Bedford, MA 01730 USA
pkcs-editor@rsasecurity.com
http://www.rsasecurity.com/rsalabs/