LABORATORIES

PKCS #15 v1.0 Amendment 1 Draft #1

RSA Laboratories

20 October, 1999

Editor's note: This is the first draft of this amendment, which is available for a 30-day public review period. Please send comments and suggestions, both technical and editorial, to *pkcs-editor@rsasecurity.com* or *pkcs-tng@rsasecurity.com*.

Table of Contents

1. Introduction

In certain circumstances, there is a need to make a PKCS #15-library aware of the fact that a user has to re-authenticate after accessing a private object, e.g. a private key, a certain number of times. This amendment documents the changes to PKCS #15 v1.0 needed to support this.

2. Changes to Section 7, "Information Syntax in ASN.1"

[Replace the ASN.1 definition of ***PKCS15CommonObjectAttributes*** *in Section 7.1.7 with:]*

```
PKCS15CommonObjectAttributes ::= SEQUENCE {
    label   PKCS15Label OPTIONAL,
    flags   PKCS15CommonObjectFlags OPTIONAL,
    authId  PKCS15Identifier OPTIONAL,
    ...,
    userConsent [0] INTEGER (1..pkcs15-ub-userConsent) OPTIONAL
```


Copyright © 1991-1999 RSA Laboratories, a division of RSA Security, Inc. 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.

000-000000-000-000-000

```
} (CONSTRAINED BY {-- authId should be present in the IC card
-- case if flags.private is set. It must equal an
-- authID in one AuthRecord in the AODF. userConsent may only be present if
-- flags.private is set. -- })
```

[Add the following paragraph after the currently last paragraph in Section 7.1.7:]

The `userConsent` field gives, in the case of a private object, the number of times an application may access the object without explicit consent from the user (e.g. a value of **3** indicates that a new authentication will be required before the first, the 4th, the 7th, etc. access).

3. Changes to Section 8, "ASN.1 Module"

[Add the following definition after the definition of pkcs15-ub-recordLength:]

```
pkcs15-ub-userConsent INTEGER ::= 15
```

[Replace the ASN.1 definition of ***PKCS15CommonObjectAttributes*** *with:]*

```
PKCS15CommonObjectAttributes ::= SEQUENCE {
    label   PKCS15Label OPTIONAL,
    flags   PKCS15CommonObjectFlags OPTIONAL,
    authId  PKCS15Identifier OPTIONAL,
    ...,
    userConsent INTEGER (1..pkcs15-ub-userConsent) OPTIONAL
    } (CONSTRAINED BY {-- authId should be present in the IC card
    -- case if flags.private is set. It must equal an
    -- authID in one AuthRecord in the AODF. userConsent may only be present if
    -- flags.private is set. -- })
```

Copyright © 1991-1999 RSA Laboratories.

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] RSA Laboratories. *PKCS #15: Cryptographic Token Information Format Standard*. Version 1.0, April 1999.

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
20 Crosby Drive
Bedford, MA 01730 USA
pkcs-editor@rsasecurity.com
http://www.rsasecurity.com/rsalabs/pubs/PKCS

Copyright © 1991-1999 RSA Laboratories.