PKCS #12 v1.0 Technical Corrigendum 1

RSA Laboratories

February 25, 2000

Table of Contents

1. Introduction

This corrigendum lists known errors in version 1.0 of PKCS #12 [1], and should be incorporated into that version.

2. Changes to Section 4, "PFX PDU Syntax"

2.1 Changes to Section 4.2.4, "The CRLBag type"

*[Replace the definition of **x509CRL** with:]*

```
x509CRL BAG-TYPE ::=
        {OCTET STRING IDENTIFIED BY {crlTypes 1}}
        -- DER-encoded X.509 CRL stored in OCTET STRING
```

2.2 Changes to Section 4.2.5, "The SecretBag Type"

*[Replace the definition of **SecretBag** with:]*

```
SecretBag ::= SEQUENCE {
        secretTypeId  BAG-TYPE.&id ({SecretTypes}),
        secretValue   [0] EXPLICIT BAG-TYPE.&Type ({SecretTypes}{@secretTypeId})
}
```


003-903079-100-000-000

3. Changes to Appendix C, "ASN.1 Module"

[Replace the definition of ***pkcs-8ShroudedKeyBag*** *with:]*

```
pkcs8ShroudedKeyBag BAG-TYPE ::=
        {PKCS8ShroudedKeyBag IDENTIFIED BY {bagtypes 2}}
```

[Replace the definition of ***CRLBag*** *with:]*

```
CRLBag ::= SEQUENCE {
        crlId           BAG-TYPE.&id ({CRLTypes}),
        crlValue  [0] EXPLICIT BAG-TYPE.&Type ({CRLTypes}{@crlId})
}
```

[Replace the definition of ***x509CRL*** *with:]*

```
x509CRL BAG-TYPE ::=
        {OCTET STRING IDENTIFIED BY {crlTypes 1}}
        -- DER-encoded X.509 CRL stored in OCTET STRING
```

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 #12: Personal Information Exchange Syntax Standard*. Version 1.0, June 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/