PKCS #15 v1.1 Technical Corrigendum 1

RSA Laboratories

August 24, 2000

Editor's note: This is the first draft of a technical corrigendum to PKCS #15 v1.1, 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

This corrigendum lists known errors in version 1.1 of PKCS #15 [1], and should be incorporated into that version.

2. Changes to Section 5, "IC card file format"

2.1 Changes to Section 5.4.1, "EF(DIR)"

[*Remove the last sentence starting*: "An example of EF(DIR) contents…"]

3. Changes to Section 6, "Information syntax in ASN.1"

3.1 Changes to Section 6.1.5, "ReferencedValue and Path"

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

```
URL ::= CHOICE {
          url          CHOICE {printable PrintableString, ia5 IA5String}, -- ia5 option should be used
          urlWithDigest [3] SEQUENCE {
              url              IA5String,
              digest           DigestInfoWithDefault
              }
}
```

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

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

```
URL ::= CHOICE {
          url          CHOICE {printable PrintableString, ia5 IA5String}, -- ia5 option should be used
          urlWithDigest [3] SEQUENCE {
              url              IA5String,
              digest           DigestInfoWithDefault
              }
}
```

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 Syntax Standard*. Version 1.1, June 2000.

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/