



Errata for PDF Reference, fifth edition

Copyright (c) 2005 Adobe Systems Incorporated. All rights reserved.

Last modified: August 31, 2005

Chapter 3, “Syntax”

Page 74, **ID** entry in Table 3.13: Insert the following after the first sentence:

The two strings should be direct objects and should be unencrypted.

Page 95, append the following to the bulleted paragraph regarding AES encryption:

Strings and streams encrypted with AES use a padding scheme that is described in RFC 2898, PKCS #5: Password-Based Cryptography Specification Version 2.0. For an original message length of M , the pad consists of $16 - (M \bmod 16)$ bytes whose value is also $16 - (M \bmod 16)$. For example, a 9-byte message has a pad of 7 bytes, each with the value 0x07. The pad can be unambiguously removed to determine the original message length when decrypting. Note that the pad is present when M is evenly divisible by 16; it contains 16 bytes of 0x10.

Page 95, Algorithm 3.1: After step 2, append the following:

If using the AES algorithm, extend the encryption key an additional 4 bytes by adding the value "sAlT", which corresponds to the hexadecimal values 0x73, 0x41, 0x6C, 0x54. (This addition is done for backward compatibility and is not intended to provide additional security.)

Page 132, steps 2 and 3 refer to 2-character language and country codes. "Character" in this context means byte (as in ASCII character), not Unicode character.

Chapter 8, “Interactive Features”

Page 699, paragraph before section 8.7.3: Replace the last sentence, which currently reads “PKCS#1 signatures are therefore recommended in all cases where the added capabilities of PKCS#7 are not required” with the following:

The implication is that PKCS#1 signatures may be preferred for their increased portability. In practice, however, the PKCS#7 format is widely supported and it is a reasonable action to standardize on PKCS#7.

Bibliography

Page 1062, insert the following in the list of IETF RFCs:

RFC 2898, PKCS #5: Password-Based Cryptography Specification Version 2.0

