RFC3447 - PKCS #1: RSA Cryptography Specifications

return to the IETF Standards

Table 1: Data sheet for PKCS #1: RSA Cryptography Specifications

Title	PKCS #1: RSA Cryptography Specifications
Acronym	PKCS-RSA
Version	version 2.1
Document Number	RFC3447
Release Date	February 2003
Reference	https://www.ietf.org/rfc/rfc3447.txt

Note: The following is an excerpt from the official IETF RFC. It is provided here as a convenience and is not authoritative. Refer to the original document as the authoritative reference.

Introduction

This document provides recommendations for the implementation of public-key cryptography based on the RSA algorithm [1)], covering the following aspects:

- *Cryptographic primitives*
- *Encryption schemes*
- *Signature schemes with appendix*
- *ASN.1 syntax for representing keys and for identifying the schemes*

The recommendations are intended for general application within computer and communications systems, and as such include a fair amount of flexibility. It is expected that application standards based on these specifications may include additional constraints. The recommendations are intended to be compatible with the standard IEEE-1363-2000 [26] and draft standards currently being developed by the ANSI X9F1 [1] and IEEE P1363 [27] working groups.

1)
R. Rivest, A. Shamir and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21 (2), pp. 120-126, February 1978.