RSA Labs Home

RSA Home

Search

Sitemap

List of changes to the previous draft of PKCS #1 v2.0:

1. The following security comment was added to the end of the second paragraph in section 7.1:

We briefly note that to receive the full security benefit of RSAES-OAEP, it should not be used in a protocol involving RSAES-PKCS1-v1_5. It is possible that in a protocol in which both encryption schemes are present, an adaptive chosen ciphertext attack such as [4] would be useful.

2. A third and last paragraph was added to section 7.1 concerning the encoding parameters P:

Both the encryption and the decryption operations of RSAES-OAEP take the value of the parameter string *P* as input. In this version of PKCS #1, *P* is an octet string that is specified explicitly. See Section 11 for the relevant ASN.1 syntax.

3. The encoding parameters, *P*, were added as input to RSAES-OAEP-DECRYPT in section 7.1.2.

4. Two sentences defining the term *signature schemes with appendix* were added to the end of the first paragraph of section 8:

To verify a signature constructed with this type of scheme it is necessary to have the message itself. In this way, signature schemes with appendix are distinguished from signature schemes with message recovery, which are not supported in this document.

5. The following message was added as a possible output from the encoding operation in section 9.1.1.1: “parameter string too long”

6. In section 9.1.1.1, a new first step was added:

> If the length of *P* is greater than the input limitation for the hash function (2^{61}-1 octets for SHA-1) then output “parameter string too long” and stop.

7. In section 9.1.1.2, the sentence added in step 6 was added as the new first step.

8. In the last sentence of the first paragraph of section 10.2, “RSAES-PKCS1-v1_5” was changed to “RSAES-OAEP”.

9. A reference to the Eurocrypt `94, Bellare-Rogaway paper, *Optimal Asymmetric Encryption-How to Encrypt with RSA*, was added.

10. Several minor editorial changes were made.

PKCS Home | RSA Laboratories Home

Contact RSA Laboratories at: rsa-labs@rsa.com Website feedback: webmaster@rsa.com