Description of rsaSignatureWithoutHash {1 3 36 3 3 1 5}

Short description: Signature algorithm with appendix similar to RSASSA-PKCS1-v1_5 of [1] but without using a digestinfo and without determining a hash algorithm within the encoding method.

Intended usage: within authentication services performed by a smart card

Application context: applications using SASCIA (signature API of the German signature alliance)

In the following description the terminology of [1] is used.

Signature generation operation:

Input: K signer's RSA private key

M message to be signed, an octet string of length m

Output: S signature, octet string of length k (k = length of RSA modulus n of K)

Error: "message too long", if "m > k – 11" holds

Steps:

1: Message encoding similar to EMSA-PKCS1-v1_5 in [1] but without using a digestinfo and without determining a hash algorithm.

EM = 0x00 || 0x01 || PS || 0x00 || M

with PS = octet string consisting of "k – m – 3" octets with value 0xFF

2: RSA signature

int = OS2IP (EM)

s = RSASP1 (K, int)

S = I2OSP (s, k)

Signature verification operation: corresponding

Remark: A corresponding RSA mechanism is available in PKCS#11 [2] for the functions C_Sign and C_Verify. There it is denoted CKM_RSA_PKCS.

References:

[1] PKCS#1 v2.1: RSA Cryptography Standard, RSA Laboratories, ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf, 14.06.2002

[2] PKCS#11 v2.20: Cryptographic Token Interface Specification, RSA Laboratories, ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf, 28.06.2004