PKCS#11 Contribution Letter

Title

PKCS #11 Version 2.10, Proposed Amendment 1 Draft 2

Classification

Proposed Specification

Contributor

Francois Rousseau
frousseau@chrysalis-its.com
Chrysalis-ITS
1688 Woodward Drive
Ottawa, Ontario, K2C 3R7 CANADA

Date/Version

November 30, 2000
Version 2.10, Amendment 1, Draft 2

Abstract

This second draft represents an amendment to the current version of the PKCS #11 standard. It includes the following enhancements over proposed the previous draft of Amendment 1 to PKCS#11 Version 2.10:

- clarifies the EC domain parameters
- clarifies references to ANSI X9.62 and X9.63
- clarifies the mechanism parameters
- clarifies the key derivation mechanisms
- minor editorial changes

Description

The following is a detailed list of each set of edits to the version 2.10 document included in this proposed third draft amendment:

- uses the expression “EC domain parameters” consistently
- uses the expressions “ANSI X9.62” and “ANSI X9.63” consistently when referring to these standards
- renames a key derivation function (KDF)
- clarifies that the key derivation function (KDF) CKD_SHA1_KDF is based on SHA-1
- clarifies exactly which key derivation mechanism(s) each mechanism parameters is for
- renames a mechanism parameters to be more generic
- clarifies that the same EC domain parameters are used for all key pairs for each key derivation mechanism

Intellectual Property Issues

Contributor hereby submits this Contribution to RSA Laboratories for possible consideration in RSA Laboratories' Public-Key Cryptography Standards (PKCS) and agrees to the guidelines for PKCS contributions in effect at the time this Contribution is submitted.

Contributor also hereby grants RSA Laboratories license to make derivative works of this Contribution and to include all or portions of this Contribution or of such derivative works in PKCS documents and drafts. Contributor represents that it has authority to grant such license.

Chrysalis-ITS makes no intellectual property claims to contributed items. Chrysalis-ITS makes no representations regarding intellectual property claims by other parties. Such determination is the responsibility of the user.

References

All references are included in the proposed draft document itself.