201

SYNOPSIS

Number and Title of the Indian Standard: IS?ISO/IEC 14888-3:2018
IT Security techniques — Digital signatures with appendix —Part 3:Discrete logarithm based mechanisms

a) Scope: This document specifies digital signature mechanisms with appendix whose security is based on the discrete logarithm problem.

This document provides

— a general description of a digital signature with appendix mechanism, and

— a variety of mechanisms that provide digital signatures with appendix.

For each mechanism, this document specifies

— the process of generating a pair of keys,

— the process of producing signatures, and

— the process of verifying signatures.

Annex A defines object identifiers assigned to the digital signature mechanisms specified in this document, and defines algorithm parameter structures.

Annex B defines conversion functions of FE2I, I2FE, FE2BS, BS2I, I2BS, I2OS and OS2I used in this document.

Annex D defines how to generate DSA domain parameters.

b) Salient features of content:

- This document includes 14 mechanisms: two of which (DSA and Pointcheval/Vaudenay algorithm) were in ISO/IEC 14888-3:1998, three of which (EC-DSA, EC-KCDSA, and EC-GDSA) were from ISO/IEC 15946-2:2002 and three of which (KCDSA, IBS-1 and IBS-2) were added in ISO/IEC 14888-3:2006, four of which (SRA, EC-RDSA, EC-SDSA and EC-FSDSA) were added in ISO/IEC 14888-3:2006/Amd 1:2010, and two of which (SM2 and Chinese IBS) are added in this document.

- The mechanisms specified in this document use a collision resistant hash-function to hash the message being signed (possibly in more than one part). ISO/IEC 10118 specifies hash-functions.

c) Types/grades/classes, if any covered in the standard: No

d) Disclaimer (to be automatically provided by the program/software)