Doc. No. : LITD 17 (12700)
IS/ISO/IEC 14888 -2:2008

BUREAU OF INDIAN STANDARDS

DRAFT FOR COMMENTS ONLY

Draft Indian Standard

INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — DIGITAL SIGNATURES WITH APPENDIX – PART 2 INTEGER FACTORIZATION BASED MECHANISMS

ICS 35.040

Last date for receipt of comments is: 13 August 2018

Information Systems Security and Biometrics Sectional Committee, LITD 17

NATIONAL FOREWORD

(Formal clauses to be added later)

This Draft Indian Standard (Part 2) which is identical with ISO/IEC 14888-2:2008 'Information technology – Security techniques – Digital Signatures With Appendix – part 2 Integer factorization based mechanisms' issued by International Organization for Standardization (ISO) and International Electro technical Commission (IEC) will be adopted by the Bureau of Indian Standards on the recommendations of the Information Systems Security and Biometrics Sectional Committee, and approval of the Electronics and Information Technology Division Council.

Other parts in this series are:

Part 1 General
Part 3 Discrete logarithm based mechanisms

The text of ISO/IEC Standard may be approved as suitable for publication as an Indian Standard without deviations. Certain conventions are, however, not identical to those used in Indian Standards. Attention is particularly drawn to the following:

a) Wherever the words 'International Standard' appear referring to this standard, they should be read as 'Indian Standard'.

b) Comma (,) has been used as a decimal marker while in Indian Standards, the current practice is to use a point (.) as the decimal marker.

In this adopted standard, reference appears to certain International Standards for which Indian Standard also exist. For undated references, the latest edition of the referenced document applies, including any corrigenda and amendment .The corresponding Indian Standard which is to be substituted in its respective place is listed below along with its degree of equivalence for the edition indicated:

International Standard	*Corresponding Indian Standard*	*Degree of Equivalence*
ISO/IEC 14888-1:2008 Information technology — Security techniques — Digita signatures with appendix — Part 1: General	Doc No LITD 17(12699) /ISO/IEC 14888-1:2008 Information technology — Security techniques — Digital signatures with appendix — Part 1: General	Identical

The technical committee has reviewed the provisions of following International Standards referred in this adopted standard and has decided that they are acceptable for use in conjunction with this standard. For undated references, the latest edition of the referenced document applies, including any corrigenda and amendment.

International Standards	Title
ISO/IEC 10118(all parts)	Information technology — Security techniques — Encryption algorithms — Hash-functions

For the purpose of deciding whether a particular requirement of this standard is complied with, the final value, observed or calculated, expressing the result of a test or analysis, shall be rounded off in accordance with IS 2 : 1960 ‘Rules for rounding off numerical values (revised)’. The number of significant places retained in the rounded off value should be the same as that of the specified value in this standard.

Scope of ISO/IEC 14888-2:2008 is as follows:

“This part of ISO/IEC 14888 specifies digital signatures with appendix whose security is based on the difficulty of factoring the modulus in use. For each signature scheme, it specifies:

a) The relationships and constraints between all the data elements required for signing and verifying;

b) A signature mechanism, i.e., how to produce a signature of a message with the data elements required for signing;

c) A verification mechanism, i.e., how to verify a signature of a message with the data elements required for verifying.

The production of key pairs requires random bits and prime numbers. The production of signatures often requires random bits. Techniques for producing random bits and prime number are outside the scope of this part of ISO/IEC 14888. For further information, see ISO/IEC 18031 [33] and ISO/IEC 18032 [34].

Various means are available to obtain a reliable copy of the public verification key, e.g., a public key certificate. Techniques for managing keys and certificates are outside the scope of this part of ISO/IEC14888-2. For further information, see ISO/IEC 9594-8 [27], ISO/IC 11770 [31] and ISO/IEC 15945[32].**"**

Note: The Technical content of this document has not been enclosed as these are identical with the corresponding ISO/IEC Standard. For details please refer ISO/IEC 14888-2:2008 or kindly contact.

Head
Electronics & IT Department
Bureau of Indian Standards 9,
B.S. Zafar Marg, New Delhi-110002
Email: hlitd@bis.gov.in
litd17@bis.gov.in
Telefax: 011-23608235