Doc. No. : LITD 17 (12716)
IS/ISO/IEC 18033-5:2015

BUREAU OF INDIAN STANDARDS

DRAFT FOR COMMENTS ONLY

Draft Indian Standard

INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — ENCRYPTION ALGORITHMS — PART 5: IDENTITY-BASED CIPHERS

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 5) which is identical with ISO/IEC 18033-5:2015 'Information technology – Security techniques – Encryption algorithms —Part 5: 'Identity-Based Ciphers' 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 2 Asymmetric ciphers
Part 3 Block ciphers
Part 4 Stream ciphers

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 18033-1 Information technology — Security techniques — Encryption algorithms — Part 1: General	IS/ISO/IEC 18033-1:2015 Information technology — Security techniques — Encryption algorithms — Part 1: General (Under Print)	Identical with ISO/IEC 18033-1:2015
ISO/IEC 18033-2 Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers	IS/ISO/IEC 18033-2 :2006 Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers (Under Print)	Identical with ISO/IEC 18033-2:2006
ISO/IEC 18033-3 Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers	IS/ISO/IEC 18033-3:2010 Information technology — Security techniques — Encryption algorithms — Part 3:Block ciphers (Under Print)	Identical with ISO/IEC 18033-3:2010

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 18033-5:2015 is as follows:

“This part of ISO/IEC 18033 specifies identity-based encryption mechanisms. For each mechanism the functional interface, the precise operation of the mechanism, and the cipher text format are specified. However, conforming systems may use alternative formats for storing and transmitting cipher texts.**”**

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 18033-5:2015 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