Doc. No. : LITD 17 (12704)
IS/ ISO/IEC 11770-4: 2017

BUREAU OF INDIAN STANDARDS

DRAFT FOR COMMENTS ONLY

Draft Indian Standard

INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — KEY MANAGEMENT –PART 4: MECHANISMS BASED ON WEAK SECRETS

(First Revision)

ICS 35.030

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 4) which is identical with ISO/IEC 11770-4:2017 'Information technology – Security techniques –Key Management – Part 4: Mechanisms based on weak secrets' 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.

This standard was originally published in 2017 and was identical with ISO/IEC 11770-4:2006. First revision of this standard has been undertaken to align with latest version of ISO/IEC 11770-4.

Other parts in this series are:

Part 1 Framework
Part 2 Mechanisms using symmetric techniques
Part 3 Mechanisms using asymmetric techniques
Part 5 Group key management
Part 6 Key derivation

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.

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 11770-4:2017 is as follows:

"This document defines key establishment mechanisms based on weak secrets, i.e. secrets that can be readily memorized by a human, and hence, secrets that will be chosen from a relatively small set of possibilities. It specifies cryptographic techniques specifically designed to establish one or more secret keys based on a weak secret derived from a memorized password, while preventing offline brute-force attacks associated with the weak secret. This document is not applicable to the following aspects of key management:

— life-cycle management of weak secrets, strong secrets, and established secret keys;

— mechanisms to store, archive, delete, destroy, etc. weak secrets, strong secrets, and established secret keys."

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 11770-4:2017 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