Doc. No. : LITD 17 (12703)
IS/ISO/IEC 11770-3:2015

BUREAU OF INDIAN STANDARDS
DRAFT FOR COMMENTS ONLY

Draft Indian Standard

INFORMATION TECHNOLOGY — SECURITYTECHNIQUES — KEY MANAGEMENT
PART 3 MECHANISMS USING ASYMMETRIC TECHNIQUES

(*First Revision*)

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 3) which is identical with ISO/IEC 11770-3:2015 'Information Technology — Security techniques — Key Management Part 3 Mechanisms Using Asymmetric Techniques' 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 2016 and was identical with ISO/IEC 11770 - 3:2008. First revision of this standard has been undertaken to align with latest version of ISO/IEC 11770-3.

Other parts in this series are:

Part 1 Framework
Part 2 Mechanisms using symmetric techniques
Part 4: Mechanisms based on weak secrets
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.

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 11770-1 Information technology — Security techniques — Key management — Part 1: Framework	ISO/IEC 11770-1:2010 Information technology — Security techniques — Key management — Part 1: Framework	Identical with ISO/IEC 11770-1:2010
ISO/IEC 15946-1 Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General	IS/ISO/IEC 15946-1:2016 Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General	Identical with ISO/IEC 15946-1:2016

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 — Key management — Part 1: Framework
ISO/IEC 18031	Information technology — Security techniques — Random bit generation

Amendment no. 1 published in 2017 to the above International Standard has been given at the end of this publication.

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 11770-3:2015 is as follows:

"This part of ISO/IEC 11770 defines key management mechanisms based on asymmetric cryptographic techniques. It specifically addresses the use of asymmetric techniques to achieve the following goals.
a) Establish a shared secret key for use in a symmetric cryptographic technique between two entities *A* and *B* by key agreement. In a secret key agreement mechanism, the secret key is computed as the result of a data exchange between the two entities *A* and *B*. Neither of them should be able to predetermine the value of the shared secret key.

b) Establish a shared secret key for use in a symmetric cryptographic technique between two entities *A* and *B* via key transport. In a secret key transport mechanism, the secret key is chosen by one entity *A* and is transferred to another entity *B*, suitably protected by asymmetric techniques.

c) Make an entity's public key available to other entities via key transport. In a public key transport mechanism, the public key of entity *A* shall be transferred to other entities in an authenticated way, but not requiring secrecy. Some of the mechanisms of this part of ISO/IEC 11770 are based on the corresponding authentication mechanisms in ISO/IEC 9798-3.[6] This part of ISO/IEC 11770 does not cover certain aspects of key management, such as

— key lifecycle management,
— mechanisms to generate or validate asymmetric key pairs, and
— mechanisms to store, archive, delete, destroy, etc. keys.

While this part of ISO/IEC 11770 does not explicitly cover the distribution of an entity's private key(of an asymmetric key pair) from a trusted third party to a requesting entity, the key transport mechanisms described can be used to achieve this. A private key can in all cases be distributed with these mechanisms where an existing, non-compromised key already exists. However, in practice the distribution of private keys is usually a manual process that relies on technological means such as smart cards, etc.

This part of ISO/IEC 11770 does not specify the transformations used in the key management mechanisms.

NOTE To provide origin authentication for key management messages, it is possible to make provisions for authenticity within the key establishment protocol or to use a public key signature system to sign the key exchange messages."

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 11770-3:2015 and Amendment published in 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