

DRAFT AMENDMENT TO INDIAN STANDARD IN WIDE CIRCULATION

Reference : LITD/17/28867

Date : 01 October 2025

TECHNICAL COMMITTEE : Information Systems Security And Privacy, LITD 17

To,

All concerned

Dear Madam/Sir,

The following document has been prepared by the Information Systems Security And Privacy Sectional Committee, LITD 17. Please [click here](#) to view the document.

Document Number : LITD 17 (28867) WC

Title of the document : Information Security - Key Management Part 3: Mechanisms using Asymmetric Techniques Second Revision Amendment - 1

Document Type : Amendment to Indian Standard (IS/ISO/IEC 11770 : Part 3: 2021)

This document has following salient features which may require specific attention for your valuable comments:

1) Public key cryptosystems were first proposed in the seminal paper by Diffie and Hellman in 1976. The security of many such cryptosystems is based on the presumed intractability of solving the discrete logarithm problem over certain finite fields. Other public key cryptosystems such as RSA are based on the difficulty of the integer factorization problem.

Please examine the document and share your comments regarding further improvement in the document.

Last date for sharing the comments is : 30 November 2025

The comments should be shared in the prescribed template through this portal only; and the comments so received shall be taken up by the Sectional Committee for necessary action. For any other query, please write an email at litd@bis.gov.in to the undersigned at Bureau of Indian Standard, Manak Bhawan, 9, Bahadur Shah Zafar Marg, New Delhi.

In case no comments are received, we would presume your approval of the documents. However, in case we receive any comments on the document, the same shall be put up to the Sectional Committee for necessary action.

Thanking You,

**Yours faithfully,
(JITENDER KUMAR)
Head (Electronics and Information Technology Department)
Email: litd@bis.gov.in**

व्यापक परिचालन में मसौदा(दे)

हमारा सन्दर्भ : LITD/17/28867

दिनांक : 01-10-2025

तकनीकी समिति : Information Systems Security And Privacy Sectional Committee, LITD 17

प्राप्तकर्ता : रूचि रखने वाले सभी निकाय

महोदय/या,

निम्नलिखित मसौदा तैयार किया गया है :

प्रलेख संख्या : LITD 17 (28867) WC

शीर्षक :

कृपया इस/इन मानक(को)/संशोधन(नो) के मसौदे(दो) का अवलोकन करें और अपनी सम्मतियाँ यह बताते हुए भेजें कि यदि ये मानक(को) के संशोधन(नो) के रूप में प्रकाशित हो तो इन पर अमल करने में आपके व्यवसाय अथवा कारोबार में क्या कठिनाइयां आ सकती हैं।

सम्मतियाँ भेजने की अंतिम तिथि : 30 November 2025

सम्मतियाँ, यदि कोई हों तो, कृपया यहाँ क्लिक करके ऑनलाइन पोर्टल के माध्यम से ऊपर दी गयी अंतिम तिथि तक दर्ज कराएं।

यह/ये प्रलेख भारतीय मानक ब्यूरो की वेबसाइट www.bis.gov.in पर भी उपलब्ध है/हैं।

धन्यवाद।

भवदीय/भवदिया,

विभाग प्रमुख का नाम : JITENDER KUMAR
(Electronics and Information Technology Department)
ई-मेल : litd@bis.gov.in