भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
मानक : पथप्रदर्शक :
मानक भवन, 9 बहादुरशाह ज़फर मार्ग, नई दिल्ली – 110002
Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi-110002
दूरभाष Phones 2323 0131 2323 3375 2323 9402
Website : www.bis.org.in
e-mail :
तार : मानकसंस्था
Grams : Manaksanstha

व्यापकपरिचालनमसौदा

प्रलेखप्रेक्षणसंज्ञापन	
संदर्भ	दिनांक
एलआईटीडी17/टी-99	14-06-2018

तकनीकीसमिति:एलआईटीडी17

पानेवालेकानाम:

1)सूचनाप्रणालीसुरक्षाएवंबॉयोमैट्रिकविषयसमितिएलआईटीडी 17
2) इलैक्ट्रॉनिकीएवंसूचनाप्रौद्योगिकीविभागपरिषदएलआईटीडीसीकेप्रधानसदस्य
3)अन्यरुचिरखनेवाले

महोदय(यों)

निम्नलिखितप्रलेखकाअवलोकनकरें:

एलआईटीडी17(12714)(संशोधन-1) **आईएसओ/आईईसी 18033-2 :2006**	**(संशोधन-1)सूचना प्रौद्योगिकी– सुरक्षा तकनीक – एन्क्रिप्शन एल्गोरिथम्स - भाग 2 एसिमेट्रिक सिफर एमेसमेंट टारगेट्स**

कृपयाइसमसौदेकाअवलोकनकरेंऔरअपनीसम्मतियाँ,
यहबतातेहुएकियदियहभारतीयमानकप्रकाशितहोंतोअमलकरनेमेंआपकेव्यवसायमेंक्याकठिनाईयाँआसकतीहैं, भेजें।

सम्मतियाँभेजनेकीअंतिमतिथि**13-08-2018**

यदिकोईसम्मतिप्राप्तनहींहोतीयासम्मतिसम्पादकीयप्रकृतिकीहोतीहैतोकृपयायथाअनांन्तिमहेतुउपरोक्तमसौदेकेलिएआपकाअनुमोदनमानलेनेकीअनुमतीदें।तथापि,
यदिआपकीसम्मतिकीप्रकृतितकनीकीहैतोयदिचेयरमैनविषयसमितिद्वाराऐसारहनावांछितहोतोइसेआगेकीआवश्यककार्रवाईकेलिएचेयरमैनविषयसमितिकेपासपरामर्शहेतुयाविषयसमितिकेपासअवलोकार्थकरकेअनांन्तिमकियाजाएगा।

धन्यवाद,

भवदीया,

(रीनागर्ग)
प्रमुख(इलैक्ट्रॉनिकीवआईटी)
ईमेल: hlitd@bis.org.in,
litd17@bis.org.in
टेलिफैक्स: 01123237093

संलग्नक : उपरोक्त

भारतीय मानक ब्यूरो
BUREAU OF INDIAN STANDARDS
मानक : पथप्रदर्शक :
मानक भवन, 9 बहादुरशाह ज़फर मार्ग, नई दिल्ली – 110002
Manak Bhavan, 9 Bahadur Shah Zafar Marg, New Delhi-110002
दूरभाष Phones 2323 0131 2323 3375 2323 9402
Website : www.bis.org.in
e-mail :
तार Grams : मानकसंस्था Manaksanstha

DRAFT IN WIDE CIRCULATION

Technical Committee: LITD 17

Document Dispatch Advice	
Ref	Date
LITD17/T- 99	14-06-2018

ADDRESSED TO:

1. All Members of Information Systems Security and Biometric Sectional Committee, LITD 17
2. All Principal Members of Electronics and Information Technology Division Council (LITDC)
3. All others interested

Dear Madam/Sir(s),

Please find enclosed the following draft Indian Standard:

LITD)17(12714) Amendment no 1 toISO/IEC 18033-2 :2006	**Information Technology –Security Techniques – Encryption Algorithms- Part 2: Asymmetric Ciphers- Amendment No 1**

Kindly examine this draft standard and forward your views stating any difficulties, which you are likely to experience in your business or profession, if this is finally adopted as National Standard.

Last Date for comments: 13-08-2018

Comments if any, may please be made in the format indicated and mailed to the undersigned. In case no comments are received or comments received are of editorial nature, You will kindly permit us to presume your approval for the above document as finalized. However, in case of comments of technical in nature are received then it may be finalized either in consultation with the Chairman, Sectional Committee or referred to the Sectional committee for further necessary action if so desired by the Chairman, Sectional Committee.

Thanking you,

Yours faithfully,

(Reena Garg)
Head (Electronics & IT)

Encl: As above

E-mail: litd17@bis.org.in
hlitd@bis.org.in
Telefax: 011-23237093

Doc. No. : LITD 17 (12714)

BUREAU OF INDIAN STANDARDS

DRAFT FOR COMMENTS ONLY

DRAFT AMENDMENT NO. 1

TO

INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — ENCRYPTION ALGORITHMS —PART 2: ASYMMETRIC CIPHERS

ICS 35.040

Last date for receipt of comments is: 13 August 2018

Information Systems Security and Biometrics Sectional Committee, LITD 17

This amendment no. 1 is identical with Amendment no 1 of ISO/IEC 18033-2:2006 issued in 2017 issued by International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

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 Amendment no 1 of ISO/IEC 18033-2:2006 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

TEMPLATE FOR SENDING COMMENTS ON BIS DOCUMENTS

Date:		Document No.:		Title of the Document:	
Name of the Commentator/ Organization:				Abbreviation of the Commentator/Organization:	

(Comments on each clause/subclause/table/fig, etc be started on a fresh box. Information in column 5 should include reasons for the comments/suggestions for modified wordings of the clauses when the existing text/provision is found not acceptable. Adherence to this format facilitates Secretariat's work)

Abbreviation of the Commentator/ Organization	**Clause/ Subclause No.** (e.g. 3.1)	**Paragraph No. / Figure No. / Table No.** (e.g. Table 1)	**Type of Comment**[1)]	**Comments/Suggestions along with Justification for the Proposed Change**	**Proposed Change/Modified Wordings**
(1)	**(2)**	**(3)**	**(4)**	**(5)**	**(6)**

1) **Type of comment:** **ge** = general **te** = technical **ed** = editorial