भारतीय मानक ब्यूरो
(उपभोक्ता मामले, खाद्य एवं सार्वजनिक वितरण मंत्रालय, भारत सरकार)
BUREAU OF INDIAN STANDARDS
(Ministry of Consumer Affairs, Food & Public Distribution, Govt. of India)
मानक: पथप्रदर्शक:
मानक भवन, 9 बहादुरशाह जफर मार्ग नई, दिल्ली-110002
Manak Bhavan ,9 Bahadur Shah Zafar Marg, New Delhi-110002
Phones: 23230131 / 23233375 / 23239402
Website: www.bis.org.in , www.bis.gov.in

DRAFT INDIAN STANDARD IN WIDE CIRCULATION

Reference : SSD 10/T-18 **Date : 23 August 2024**

TECHNICAL COMMITTEE : IT & IT enabled Services, SSD 10

To,

All concerned

Dear Madam/Sir,

The following document has been prepared by the IT & IT enabled Services Sectional Committee, SSD 10. Please click here to view the document.

Document Number : SSD 10 (25838) WC
Title of the document : ELECTRONIC SIGNATURES AND INFRASTRUCTURES ESI CRYPTOGRAPHIC SUITES
Document Type : New Indian Standard

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

1) This draft standard specifies cryptographic suites used for the creation and validation of digital signatures and electronic time stamps and related certificates. The standard builds on the agreed cryptographic mechanisms from SOG IS. It may be used also for electronic registered delivery services in the future. The standard focuses on interoperability issues. It instead provides guidance on the selection of concrete cryptographic suites that use agreed mechanisms. The use of SOG-IS agreed mechanisms is meant to help ensure a high level of security in the recommended cryptographic suites, while the focus on specific suites of mechanisms is meant to increase interoperability and simplify design choices. There is no normative requirement on selection among the alternatives for cryptographic suites given here but for all of them normative requirements apply to ensure security and interoperability. The standard also provides guidance on hash functions, digital signature schemes and digital

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

Last date for sharing the comments is : 22 October 2024

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 ssd@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,

(S K KANOGIA)
Head (Service Sector Department)
Email: ssd@bis.gov.in

व्यापक परिचालन में मसौदा(दे)

हमारा सन्दर्भ : SSD 10/T-18 दिनांक : 23-08-2024

तकनीकी समिति : IT & IT enabled Services Sectional Committee, SSD 10

प्राप्तकर्ता : रूचि रखने वाले सभी निकाय

महोदय/या,

निम्नलिखित मसौदा तैयार किया गया है :

प्रलेख संख्या : SSD 10 (25838) WC
शीर्षक :

कृपया इस/इन मानक(को)/संसोधन(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।

सम्मत्तियाँ भेजने की अंतिम तिथि : 22 October 2024

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 : S K KANOGIA
(Service Sector Department)
ई-मेल : ssd@bis.gov.in