SYNOPSIS

Number and Title of the Indian Standard: IS/ISO/IEC TS 20540:2018
INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — TESTING CRYPTOGRAPHIC MODULES IN THEIR OPERATIONAL ENVIRONMENT

a) Scope: This document provides recommendations and checklists which can be used to support the specification and operational testing of cryptographic modules in their operational environment within an organization's security system.

The cryptographic modules have four security levels which ISO/IEC 19790 defines to provide for a wide spectrum of data sensitivity (e.g. low-value administrative data, million-dollar funds transfers, life-protecting data, personal identity information, and sensitive information used by government) and a diversity of application environments (e.g. a guarded facility, an office, removable media, and a completely unprotected location).

This document includes:

a) recommendations to perform secure assessing for cryptographic module installation, configuration and operation;

b) recommendations to inspecting the key management system, protection of authentication credentials, and public and critical security parameters in the operational environment;

c) recommendations for identifying cryptographic module vulnerabilities;

d) checklists for the cryptographic algorithm policy, security guidance and regulation, security manage requirements, security level for each of the 11 requirement areas, the strength of the security function, etc.; and

e) recommendations to determine that the cryptographic module's deployment satisfies the security requirements of the organization.

This document assumes that the cryptographic module has been validated as conformant with ISO/IEC 19790.

It can be used by an operational tester along with other recommendations if needed.

This document is limited to the security related to the cryptographic module. It does not include assessing the security of the operational or application environment. It does not define techniques for the identification, assessment and acceptance of the organization's operational risk.

The organization's accreditation, deployment and operation processes, shown in Figure 1, is not included to the scope of this document.

This document addresses operational testers who perform the operational testing for the cryptographic modules in their operational environment authorizing officials of cryptographic modules.

b) Salient features of content:

The purpose of this document is to describe the recommendations and checklists which help in the selection of cryptographic modules for deployment in a diversity of application