

DIN EN ISO/IEC 19790



ICS 35.030

Einsprüche bis 2019-12-18

Entwurf

**Informationstechnik –
Sicherheitstechniken –
Sicherheitsanforderungen für kryptografische Module
(ISO/IEC 19790:2012);
Englische Fassung prEN ISO/IEC 19790:2019**

Information technology –
Security techniques –
Security requirements for cryptographic modules (ISO/IEC 19790:2012);
English version prEN ISO/IEC 19790:2019

Technologies de l'information –
Techniques de sécurité –
Exigences de sécurité pour les modules cryptographiques (ISO/IEC 19790:2012);
Version anglaise prEN ISO/IEC 19790:2019

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-10-18 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin, Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 98 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO/IEC 19790:2012 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 19790:2019 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Gremium ist der Arbeitskreis NA 043-01-27-03 AK „Evaluationskriterien für IT-Sicherheit“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Dieses Dokument enthält unter Berücksichtigung des Präsidialbeschlusses 1/2004 nur die englische Originalfassung der ISO/IEC-Norm.

Für die in diesem Dokument zitierten internationalen Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO 10007:2003	siehe	DIN ISO 9000:2004-12
ISO/IEC 27001	siehe	DIN EN ISO/IEC 27001

Nationaler Anhang NA (informativ)

Begriffe

Die Benummerung der folgenden Begriffe und Abkürzungen sind identisch mit der Benummerung in der englischen Fassung.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1

Zugriffskontrollliste

ACL

(en: access control list)

Liste mit Berechtigungen, die den Zugriff auf ein Objekt erlauben

3.2

Administratorleitlinien

schriftliche Unterlagen, die vom Kryptobeauftragten und/oder anderen administrativen Rollen zur korrekten Konfiguration, Wartung und Administration des Krypto-Moduls herangezogen werden

3.3

automatisiert

ohne manuellen Eingriff oder manuelle Eingabe (z. B. elektronische Mittel, wie ein Computernetzwerk)

3.4

Genehmigungsinstanz

nationale oder internationale Organisation/Instanz, die befugt ist, Sicherheitsfunktionen zu genehmigen und/oder zu evaluieren

ANMERKUNG Eine Genehmigungsinstanz im Kontext dieser Definition evaluiert und genehmigt Sicherheitsfunktionen ausgehend von deren kryptographischen oder mathematischen Eigenschaften, es handelt sich dabei jedoch nicht um die Prüfstelle, die die Übereinstimmung mit dieser Internationalen Norm prüfen würde.

3.5

genehmigte Datenauthentisierungstechnik

genehmigtes Verfahren, das die Nutzung einer digitalen Signatur, eines Mitteilungsauthentisierungscode oder eines verschlüsselten Hashs (z. B. HMAC) beinhalten kann

3.6

genehmigte Integritätstechnik

genehmigter Hash, Mitteilungsauthentisierungscode oder Algorithmus für digitale Signaturen

3.7

genehmigter Betriebsmodus

Satz an Diensten, der mindestens einen Dienst beinhaltet, welcher eine genehmigte Sicherheitsfunktion oder einen genehmigten Sicherheitsprozess verwendet, und auch nicht sicherheitsrelevante Dienste enthalten kann

ANMERKUNG 1 Nicht zu verwechseln mit einem konkreten Modus einer genehmigten Sicherheitsfunktion, z. B. CBC-Modus (en: Cipher Block Chaining Mode)

ANMERKUNG 2 Nicht genehmigte Sicherheitsfunktionen oder -prozesse sind nicht eingeschlossen.

3.8

genehmigte Sicherheitsfunktion

Sicherheitsfunktion (z. B. kryptographischer Algorithmus), auf die in Anhang C verwiesen wird

3.9

asymmetrische Kryptographietechnik

kryptographische Technik, die zwei miteinander verbundene Transformationen nutzt: eine öffentliche Transformation (durch den öffentlichen Schlüssel definiert) und eine private Transformation (durch den privaten Schlüssel definiert)

ANMERKUNG Die beiden Transformationen haben die Eigenschaft, dass es aufgrund der öffentlichen Transformation im Hinblick auf Rechenleistung nicht machbar ist, innerhalb einer bestimmten begrenzten Zeit und mit einer bestimmten verfügbaren Rechenleistung daraus die private Transformation abzuleiten.

3.10

biometrisch

messbares körperliches Merkmal oder messbares Handlungsmuster, das zur Erkennung der Identität oder zur Überprüfung der vorgegebenen Identität eines Bedieners verwendet wird

3.11

Fähigkeit zum Umgehen

Vermögen eines Dienstes, die Anwendung einer kryptographischen Funktion auf sich selbst teilweise oder vollständig zu verhindern

3.12

Zertifikat

Daten einer Entität, die mittels des privaten oder geheimen Schlüssels einer Zertifizierungsinstanz fälschungssicher gemacht wurden

ANMERKUNG Nicht zu verwechseln mit einem Modulvalidierungszertifikat, das von einer Validierungsinstanz ausgestellt wird

3.13

kompromittieren

kritische Sicherheitsparameter unautorisiert offenlegen, modifizieren, ersetzen oder verwenden oder öffentliche Sicherheitsparameter unautorisiert modifizieren oder ersetzen

3.14

bedingter Selbsttest

von einem Krypto-Modul durchgeführte Überprüfung, wenn die für die Überprüfung festgelegten Bedingungen auftreten

3.15

Vertraulichkeit

Eigenschaft, Informationen nicht für Entitäten verfügbar zu machen oder offenzulegen, die nicht dafür autorisiert sind

3.16

Konfigurationsmanagementsystem

CMS

(en: configuration management system)

Management der Sicherheitsmerkmale und Vertrauenswürdigkeiten eines Krypto-Moduls durch gesteuerte Änderungen an dessen Hardware, Software und Dokumentation

3.17

Steuerinformation

Information, die zum Zweck der Steuerung des Betriebs des Krypto-Moduls in dieses Modul eingegeben wird

3.18

kritischer Sicherheitsparameter

CSP

(en: critical security parameter)

sicherheitsbezogene Information, deren Offenlegung oder Modifizierung die Sicherheit eines Krypto-Moduls kompromittieren kann

BEISPIEL Geheime und private kryptographische Schlüssel, Authentisierungsdaten wie Passwörter, PINs, Zertifikate oder andere Vertrauensanker

ANMERKUNG Ein CSP kann in Klartext gehalten oder verschlüsselt sein.

3.19

Kryptobeauftragter

Rolle, die eine Person oder ein Prozess (d. h. ein Subjekt), der für eine Person agiert, inne hat, und die/der auf ein Krypto-Modul zugreift, um eine kryptographische Initialisierung oder Managementfunktionen für das Krypto-Modul durchzuführen

3.20

kryptographischer Algorithmus

klar definierte Computerprozedur, die anhand von variablen Eingaben, wozu auch kryptographische Schlüssel gehören können, eine Ausgabe erzeugt

3.21

kryptographische Begrenzung

explizit definierter Bereich, innerhalb von dessen Grenzen sich alle Komponenten (d. h., Satz an Hardware-, Software- oder Firmware-Komponenten) des Krypto-Moduls befinden

3.22

kryptographische Hashfunktion

recheneffiziente Funktion, die binäre Zeichenfolgen einer beliebigen Länge so zu binären Zeichenfolgen mit fester Länge zuordnet, dass es rechnerisch gesehen nicht machbar ist, dass dabei zwei unterschiedlichen Werten dieselbe feste Zeichenfolge zugeordnet wird

3.23

kryptographischer Schlüssel

Schlüssel

Abfolge von Symbolen, die den Ablauf einer kryptographischen Transformation steuert

BEISPIEL Zu kryptographischen Transformationen zählen unter anderem Verschlüsselung, Entschlüsselung, Berechnung kryptographischer Prüffunktionen sowie Generierung und Verifizierung von Signaturen.

3.24

Komponente des kryptographischen Schlüssels

Schlüsselkomponente

Parameter, der in Verbindung mit anderen Schlüsselkomponenten in einer genehmigten Sicherheitsfunktion zur Erzeugung eines Klartext-CSP oder zur Ausführung einer kryptographischen Funktion genutzt wird

3.25

kryptographisches Modul

Krypto-Modul

Hardware-, Software- und/oder Firmware-Satz, der Sicherheitsfunktionen implementiert und sich innerhalb der kryptographischen Begrenzung befindet

3.26

Sicherheitsleitlinie für kryptographische Module

Sicherheitsleitlinie

präzise Spezifikation der Sicherheitsregeln, nach denen ein Krypto-Modul arbeiten muss, einschließlich der aus den Anforderungen dieser Internationalen Norm abgeleiteten Regeln sowie weiteren Regeln, die von der Modul- oder Validierungsinstanz vorgegeben werden

ANMERKUNG Siehe Anhang B.

3.27

Datenweg

physische oder logische Route, entlang der sich Daten bewegen

ANMERKUNG Auf einem physischen Datenweg können mehrere logische Datenwege verlaufen.

3.28

eingeschränkter Betrieb

Betrieb, bei dem aufgrund der Rekonfiguration nach einem Fehlerzustand lediglich ein Teilsatz des gesamten Satzes an Algorithmen, Sicherheitsfunktionen, Diensten oder Prozessen verfügbar und/oder konfigurierbar ist

3.29

differentielle Stromverbrauchsanalyse

DPA

(en: differential power analysis)

Analyse der Schwankungen des Stromverbrauchs eines Krypto-Moduls mit dem Ziel, Informationen im Zusammenhang mit dem kryptographischen Betrieb zu erhalten

3.30

digitale Signatur

an eine Dateneinheit angefügte Daten oder eine kryptographische Transformation einer Dateneinheit, mit der ein Empfänger der Dateneinheit die Möglichkeit der Überprüfung der Quelle und Integrität der Dateneinheit erhält und die einen Schutz gegen Fälschung, z. B. durch den Empfänger, bietet

3.31

Direkteingabe

Eingabe eines SSP oder einer Schlüsselkomponente in ein Krypto-Modul über ein Gerät, wie z. B. eine Tastatur

3.32

Teilsignatur

(en: disjoint signature)

eine oder mehrere Signaturen, die zusammen einen vollständigen Codesatz darstellen

3.33

elektromagnetische Emanationen

EME

Informationen enthaltendes Signal, das, wenn es abgefangen und ausgewertet wird, möglicherweise die von einem beliebigen informationsverarbeitenden Gerät übertragenen, empfangenen, koordinierten oder anderweitig verarbeiteten Informationen preisgibt

3.34

elektronische Eingabe

Eingabe von SSP oder Schlüsselkomponenten in ein Krypto-Modul mit elektronischen Methoden

ANMERKUNG Es kann sein, dass der Bediener des Schlüssels keine Kenntnis über den eingegebenen Schlüsselwert hat.

3.35

Gesamtsignatur

(en: encompassing signature)

Einzelne Signatur für einen vollständigen Codesatz

3.36

verschlüsselter Schlüssel

kryptographischer Schlüssel, dessen Verschlüsselung unter Verwendung einer genehmigten Sicherheitsfunktion mit einem Schlüssel-Verschlüsselungsschlüssel (KEK) durchgeführt wurde. Wird als geschützt angesehen

3.37

Entität

Person, Gruppe, Gerät oder Prozess

3.38

Entropie

Messgröße für die Unordnung, Zufälligkeit oder Variabilität innerhalb eines abgeschlossenen Systems

ANMERKUNG Die Entropie einer Zufallsvariablen X ist eine mathematische Messgröße für die Menge an Informationen, die sich aus der Beobachtung von X ergibt.

3.39

Schutz vor umgebungsbedingtem Ausfall

EFP

(en: environmental failure protection)

Anwendung von Funktionen zum Schutz gegen das Kompromittieren der Sicherheit eines Krypto-Moduls aufgrund von Umgebungsbedingungen, die sich außerhalb des üblichen Betriebsbereichs des Krypto-Moduls befinden

3.40

Prüfung auf umgebungsbedingten Ausfall

EFT

(en: environmental failure testing)

Anwendung spezieller Methoden, um in angemessenem Umfang sichergehen zu können, dass die Sicherheit eines Krypto-Moduls nicht aufgrund von Umgebungsbedingungen, die sich außerhalb des üblichen Betriebsbereichs des Krypto-Moduls befinden, kompromittiert wird

3.41

Fehlererkennungscode

EDC

(en: error detection code)

aus Daten berechneter Wert, der aus redundanten Informationsbits besteht und dafür bestimmt ist, unbeabsichtigte Änderungen in den Daten zu erkennen, jedoch nicht zu korrigieren

3.42

ausführbare Form

Form des Codes, mit dem die Software oder Firmware vollständig von der Betriebsumgebung des Krypto-Moduls verwaltet und gesteuert wird und die keine Kompilierung (z. B. keinen Quellcode, Objektcode oder per JIT kompilierten Code) erfordert

3.43

Fehlerinjektion

Technik, bei der mittels Einsatz von Spannungsimpulsen, Strahlung, Laser oder Taktversatz Änderungen des Betriebsverhaltens der Hardware hervorgerufen werden

3.44.

endlicher Automat

EA

mathematisches Modell einer sequenziellen Maschine, die über einen endlichen Satz an Eingabeereignissen, einen endlichen Satz an Ausgabeereignissen, einen endlichen Satz an Zuständen, eine Funktion, die Zustände und Eingaben den Ausgaben zuordnet (Zustandsübergangsfunktion) und eine den ursprünglichen Zustand beschreibende Funktion verfügt

3.45

Firmware

ausführbarer Code eines Krypto-Moduls, der auf innerhalb der kryptographischen Begrenzung befindlichen Hardware gespeichert ist und während seiner Ausführung beim Betrieb in einer nicht modifizierbaren oder begrenzten Betriebsumgebung nicht dynamisch geschrieben oder modifiziert werden kann

BEISPIEL Speicher-Hardware kann u. a. sein: PROM, EEPROM, FLASH, Solid-State-Speicher, Festplatten usw.

3.46

Firmwaremodul

Modul, das ausschließlich aus Firmware besteht

3.47

Funktionsspezifikation

allgemeine Beschreibung der für den Bediener sichtbaren Anschlüsse und Schnittstellen und allgemeine Beschreibung des Verhaltens des Krypto-Moduls

3.48

Funktionsprüfung

Prüfung der in der Funktionsspezifikation definierten Funktionen des Krypto-Moduls

3.49

hart/Härte

relative Widerstandsfähigkeit eines Metalls oder anderen Werkstoffs gegenüber Einkerbungen, Kratzern oder Verbiegen; physisch gehärtet; robust und widerstandsfähig

ANMERKUNG Die relative Widerstandsfähigkeit des Werkstoffs gegenüber dem Eindringen eines anderen Objekts.

3.50

Hardware

physische Einrichtungen/Komponenten innerhalb der kryptographischen Begrenzung, mit denen Programme und Daten verarbeitet werden

3.51

Hardwaremodul

Modul, das hauptsächlich aus Hardware besteht und auch Firmware enthalten kann

3.52

Hardwaremodul-Schnittstelle

HMI

(en: hardware module interface)

gesamter Befehlssatz zur Anforderung der Dienste des Hardwaremoduls, einschließlich Parametern, die im Rahmen des angeforderten Dienstes die kryptographische Begrenzung des Moduls in beliebiger Richtung passieren

3.53

Hash-Wert

Ausgabe einer kryptographischen Hashfunktion

3.54

Hybridmodul

Modul, dessen kryptographische Begrenzung den Verbund einer Software- oder Firmwarekomponente und einer separaten Hardwarekomponente abgrenzt

3.55

Hybridfirmwaremodul-Schnittstelle

HFMI

(en: hybrid firmware module interface)

gesamter Befehlssatz zur Anforderung der Dienste des Hybridfirmwaremoduls, einschließlich Parametern, die im Rahmen des angeforderten Dienstes die kryptographische Begrenzung des Moduls in beliebiger Richtung passieren

3.56

Hybridsoftwaremodul-Schnittstelle

HSMI

(en: hybrid software module interface)

gesamter Befehlssatz zur Anforderung der Dienste des Hybridsoftwaremoduls, einschließlich Parametern, die im Rahmen des angeforderten Dienstes die kryptographische Begrenzung des Moduls in beliebiger Richtung passieren

3.57

Eingabedaten

Information, die in ein Krypto-Modul eingegeben wird und unter Verwendung einer genehmigten Sicherheitsfunktion zum Zweck der Transformation oder Berechnung eingesetzt werden kann

3.58

Integrität

Eigenschaft, dass Daten nicht auf unautorisierte und unbemerkte Weise modifiziert oder gelöscht worden sind

3.59

Schnittstelle

logischer Eingangs- oder Ausgangspunkt eines Krypto-Moduls, der logischen Informationsströmen den Zugang zum Modul ermöglicht

3.60

von ISO/IEC übernommen

Sicherheitsfunktion, die entweder

- in einer ISO/IEC-Norm festgelegt ist, oder
- in eine ISO/IEC-Norm übernommen wurde oder darin empfohlen wird und entweder in einem Anhang der ISO/IEC-Norm oder in einem Dokument, auf das die ISO/IEC-Norm verweist, festgelegt ist

3.61

Schlüsselübereinstimmung

Verfahren zur SSP-Bereitstellung, bei dem der entstehende Schlüssel aus Informationen von zwei oder mehr Teilnehmern abgeleitet wird, so dass keine Partei vorab mithilfe von automatisierten Methoden den Wert des Schlüssels ohne Kenntnis des Beitrags der anderen Partei(en) bestimmen kann

3.62

Schlüssel-Verschlüsselungsschlüssel

KEK

(en: key encryption key)

kryptographischer Schlüssel, der für die Ver- oder Entschlüsselung anderer Schlüssel genutzt wird

3.63

Schlüsseleingabegerät

(en: key loader)

eigenständiges Gerät, das in der Lage ist, mindestens einen in Klartext gehaltenen oder verschlüsselten SSP oder eine solche Schlüsselkomponente zu speichern, die auf Anforderung in ein Krypto-Modul übertragen werden kann

ANMERKUNG Der Einsatz eines Schlüsseleingabegeräts erfordert das Eingreifen durch eine Person.

3.64

Schlüsselverwaltung

Administration und Anwendung von Erzeugung, Registrierung, Zertifizierung, Deregistrierung, Verteilung, Installierung, Speicherung, Archivierung, Zurückziehen, Ableiten und Vernichtung von Schlüsselmaterial in Übereinstimmung mit einer Sicherheitsleitlinie

3.65

Schlüsseltransport

Prozess der Übertragung eines Schlüssels von einer Entität zu einer anderen Entität mithilfe automatischer Methoden

3.66

begrenzte Betriebsumgebung

Betriebsumgebung, die so ausgelegt ist, dass sie nur kontrollierte Firmwareänderungen akzeptiert und nur dann, wenn diese die Prüfung zum Laden von Software/Firmware erfolgreich bestanden haben

3.67

detaillierte Prüfung

Prüfung der einzelnen Komponenten oder Komponentengruppen des Krypto-Moduls und ihrer physischen Anschlüsse und logischen Schnittstellen

3.68

Wartungsrolle

Rolle, die eingenommen wird, um physische und/oder logische Wartungsmaßnahmen durchzuführen

BEISPIEL Zu Wartungsmaßnahmen zählt u. a. die Hardware- und/oder Softwarediagnostik

3.69

manuell

Eingreifen einer bedienenden Person erfordernd

3.70

Mitteilungsauthentisierungscode MAC

(en: message authentication code)

kryptographische Prüfsumme für Daten, die mithilfe eines symmetrischen Schlüssels sowohl versehentliche als auch vorsätzliche Modifikationen dieser Daten aufdeckt

BEISPIEL Ein Hash-basierter Mitteilungsauthentisierungscode

3.71

Mikrocode

Prozessoranweisungen, die einer ausführbaren Programmanweisung entsprechen

BEISPIEL Assembler-Code

3.72

minimale Entropie

untere Entropiegrenze, die bei der Bestimmung der ungünstigsten Schätzung einer Beispielentropie noch hilfreich ist

3.73

modifizierbare Betriebsumgebung

Betriebsumgebung, die so ausgelegt ist, dass sie funktionale Änderungen akzeptiert, die möglicherweise nicht kontrollierte Software (z. B. nicht vertrauenswürdig) enthalten

3.74

Mehrfaktor-Authentifizierung

Authentifizierung durch mindestens zwei voneinander unabhängige Authentifizierungsfaktoren

ANMERKUNG 1 Ein Authentifizierungsfaktor ist eine Information und ein Prozess, mit denen die Identität einer Entität authentifiziert oder verifiziert wird.

ANMERKUNG 2 Kategorien für unabhängige Authentifizierungsfaktoren sind: die Kenntnis der Entität von etwas, etwas, das im Besitz der Entität ist und eine Eigenschaft der Entität.

3.75

eingebettetes Multichip-Krypto-Modul

physische Ausführung, bei der zwei oder mehr integrierte Schaltkreise miteinander verbunden und in ein Gehäuse oder ein Produkt eingebettet sind, das möglicherweise nicht über einen physischen Schutz verfügt

BEISPIEL Adapter und Erweiterungskarten (Expansion Boards)

3.76

eigenständiges Multichip-Krypto-Modul

physische Ausführung, bei der zwei oder mehr integrierte Schaltkreise miteinander verbunden sind und das gesamte Gehäuse physisch geschützt ist

BEISPIEL Router mit verschlüsselter Übertragung oder gesicherte Funkanlagen

3.77

Anwenderleitlinien

schriftliche Unterlagen, die vom Anwender und/oder anderen nicht administrativen Rollen für das Betreiben des Krypto-Moduls in einem genehmigten Betriebsmodus herangezogen werden

ANMERKUNG Die Anwenderleitlinien beschreiben die Sicherheitsfunktionen des Krypto-Moduls und enthalten Informationen und Verfahren hinsichtlich der sicheren Nutzung des Krypto-Moduls, darunter Anweisungen, Leitlinien und Warnhinweise.

3.78

nicht-invasiver Angriff

Angriff auf ein Krypto-Modul ohne direkten physischen Kontakt mit den Komponenten innerhalb der kryptographischen Begrenzung des Moduls

ANMERKUNG Ein Angriff, der den Zustand des Krypto-Moduls nicht abwandelt oder ändert.

3.79

nicht modifizierbare Betriebsumgebung

Betriebsumgebung, die so ausgelegt ist, dass sie keine Veränderungen an der Firmware akzeptiert

3.80

nicht sicherheitsrelevant

so implementiert, dass der genehmigte sichere Betrieb des Krypto-Moduls nicht gestört oder kompromittiert wird

3.81

Normalbetrieb

Betrieb, bei dem der gesamte Satz an Algorithmen, Sicherheitsfunktionen, Diensten oder Prozessen verfügbar und/oder konfigurierbar ist

3.82

opak

lichtundurchlässig (d. h. für Licht innerhalb des sichtbaren Spektrums mit Wellenlängen von 400 nm bis 750 nm); im sichtbaren Spektrum weder transparent noch durchscheinend

3.83

Betriebsumgebung

Satz der gesamten Software und Hardware, bestehend aus einem Betriebssystem und einer Hardware-Plattform, die für den sicheren Betrieb des Krypto-Moduls erforderlich ist

3.84

Betriebszustand

Zustand, in dem von einem Bediener Dienste oder Funktionen angefordert und die Ergebnisdaten auf der Datenausgabeschnittstelle des Krypto-Moduls ausgegeben werden können

3.85

Bediener

Einzelperson oder im Auftrag einer Einzelperson handelnder Prozess (Subjekt), die/der für die Annahme einer oder mehrerer Rollen autorisiert ist

3.86

Ausgabedaten

Informationen oder berechnete Ergebnisse, die von einem Krypto-Modul erzeugt werden

3.87

Passivierung

Effekt eines reaktiven Prozesses an Verbindungspunkten, Oberflächen oder Komponenten von Halbleitern sowie integrierten Schaltkreisen, die so ausgelegt sind, dass sie Erkennungs- und Schutzmaßnahmen beinhalten

BEISPIEL Quarzglas oder Phosphorglas

ANMERKUNG Eine Passivierung kann das Verhalten des Schaltkreises beeinflussen. Der für die Passivierung verwendete Werkstoff ist von der genutzten Technologie abhängig.

3.88

Passwort

Zeichenfolge, die für die Authentifizierung einer Identität oder für die Verifizierung einer Zugriffsautorisierung genutzt wird

BEISPIEL Buchstaben, Zahlen und andere Symbole

3.89

persönliche Identifikationsnummer

PIN

numerischer Code, der für die Authentifizierung einer Identität genutzt wird

3.90

physischer Schutz

Sicherung eines Krypto-Moduls, von CSP und von PSP mithilfe physischer Mittel

3.91

Klartext-Schlüssel

unverschlüsselter kryptographischer Schlüssel oder kryptographischer Schlüssel, der als ungeschützt angesehen wird, da er mit nicht genehmigten Methoden unkenntlich gemacht wurde

3.92

Anschluss

physischer/logischer Eingangs- oder Ausgangspunkt eines Krypto-Moduls, der den Zugang zum Modul ermöglicht

3.93

vorbetrieblicher Selbsttest

Überprüfung, die von einem Krypto-Modul zwischen dem Zeitpunkt des Einschaltens oder Instantiierens (nach dem Ausschalten, Zurücksetzen, einem Reboot, Kaltstart, Stromausfall usw.) des Moduls und dem Übergang in den Betriebszustand ausgeführt wird

3.94

privater Schlüssel

Schlüssel des asymmetrischen Schlüsselpaars einer Entität, der ausschließlich von dieser Entität verwendet werden sollte

ANMERKUNG Im Fall eines asymmetrischen Signatursystems definiert der private Schlüssel die Signaturtransformation. Bei einem asymmetrischen Verschlüsselungssystem definiert der private Schlüssel die Entschlüsselungstransformation.

3.95

Produktionsqualität

Produkt, Komponente oder Software, das/die eine Prüfung auf Übereinstimmung mit den Betriebsspezifikationen bestanden hat

3.96

öffentlicher Schlüssel

Schlüssel des asymmetrischen Schlüsselpaars einer Entität, der öffentlich gemacht werden kann

ANMERKUNG 1 Im Fall eines asymmetrischen Signatursystems definiert der öffentliche Schlüssel die Verifizierungstransformation. Bei einem asymmetrischen Verschlüsselungssystem definiert der öffentliche Schlüssel die Verschlüsselungstransformation. Ein „öffentlich bekannter“ Schlüssel ist nicht notwendigerweise auch überall verfügbar. Es kann sein, dass der Schlüssel ausschließlich allen Mitgliedern einer vordefinierten Gruppe zur Verfügung steht.

ANMERKUNG 2 Für die Anwendung dieser Internationalen Norm werden öffentliche Schlüssel nicht als CSP betrachtet.

3.97

Zertifikat eines öffentlichen Schlüssels

Informationen eines öffentlichen Schlüssels einer Entität, die von einer entsprechenden Zertifizierungsinstanz signiert und auf diese Weise fälschungssicher gemacht wurden

3.98

kryptographischer Algorithmus mit öffentlichem Schlüssel (asymmetrischer Algorithmus)

kryptographischer Algorithmus, der zwei zusammenhängende Schlüssel, einen öffentlichen und einen privaten, nutzt

ANMERKUNG Die beiden Schlüssel haben die Eigenschaft, dass es hinsichtlich Rechenleistung nicht machbar ist, den privaten Schlüssel aus dem öffentlichen Schlüssel abzuleiten.

3.99

öffentlicher Sicherheitsparameter

PSP

(en: public security parameter)

sicherheitsbezogene öffentliche Information, deren Modifizierung die Sicherheit eines Krypto-Moduls kompromittieren kann

BEISPIEL Öffentliche kryptographische Schlüssel, Zertifikate von öffentlichen Schlüsseln, selbstsignierte Zertifikate, Vertrauensanker, Einmal-Passwörter mit zugeordnetem Zähler sowie intern vorgehaltene Datums- und Uhrzeitangaben

ANMERKUNG Ein PSP gilt als geschützt, wenn er nicht modifiziert werden kann oder eine solche Modifizierung vom Modul bestimmbar ist.

3.100

Zufallsbitgenerator

RGB

(en: random bit generator)

Gerät oder Algorithmus, das/der eine anscheinend statistisch unabhängige und von systematischen Fehlern freie Bitfolge ausgibt

3.101

entfernbarer Abdeckung

physisches Mittel, das gezielt so gestaltet ist, dass es einen nicht beschädigenden Zugang zu den physischen Komponenten eines Krypto-Moduls erlaubt

3.102

Rolle

Sicherheitsattribut, das einem Anwender zugeordnet ist und das die Zugriffsrechte bzw. -beschränkungen hinsichtlich der Dienste eines Krypto-Moduls für Anwender definiert

ANMERKUNG Einer Rolle können einer oder mehrere Dienste zugeordnet sein. Eine Rolle kann einem oder mehreren Anwendern zugeordnet sein und ein Anwender kann eine oder mehrere Rollen haben.

3.103

rollenbasierte Zugriffskontrolle

RBAC

(en: role-based access control)

Berechtigungen, die einer Rolle zugeordnet sind und dieser den Zugriff auf ein Objekt erlauben

3.104

Laufzeitumgebung

virtueller Gerätezustand, der zur Laufzeit eines Computers Software-Dienste für Prozesse oder Programme bereitstellt

ANMERKUNG Der Begriff kann sich auf das Betriebssystem selbst oder auf die Software beziehen, auf der das Betriebssystem aufgesetzt ist. Hauptziel ist es, eine „plattformunabhängige“ Programmierung zu ermöglichen.

3.105

geheimer Schlüssel

kryptographischer Schlüssel, der mit einem einer oder mehreren Entitäten eindeutig zugeordneten kryptographischen Secret-Key-Algorithmus verwendet wird und nicht öffentlich verbreitet werden sollte

3.106

Sicherheitsfunktion

kryptographische Algorithmen in Kombination mit Betriebsmodi, wie beispielsweise Blockverschlüsselung, Stromverschlüsselung, Algorithmen mit symmetrischen oder asymmetrischen Schlüsseln, Mitteilungs-authentisierungs-codes, Hashfunktionen oder andere Sicherheitsfunktionen, Zufallsbitgeneratoren, Authentisierung von Entitäten sowie SSP-Erzeugung und -Bereitstellung, die alle entweder von ISO/IEC oder einer Genehmigungsinstanz genehmigt wurden

ANMERKUNG Siehe Anhang C.

3.107

Startwert

Seed

geheimer Wert, mit dem ein Zufallsbitgenerator initialisiert wird

3.108

Selbsttest

vor dem Betrieb oder unter bestimmten Bedingungen durchgeführte Prüfung, die vom Krypto-Modul ausgeführt wird

3.109

sensible Daten

Daten, die nach Ansicht des Anwenders Schutz erfordern

3.110

sensible Sicherheitsparameter

SSP

(en: sensitive security parameters)

kritische Sicherheitsparameter (CSP) und öffentliche Sicherheitsparameter (PSP)

3.111

Dienst

von einem Bediener extern ausgelöste(r) Vorgang oder Funktion, der/die von einem Krypto-Modul ausgeführt werden kann

3.112

Diensteingabe

vom Krypto-Modul verwendete Daten oder Steuerinformationen, die bestimmte Vorgänge oder Funktionen initiieren oder anfordern

3.113

Dienstausgabe

Daten oder Statusinformationen, die das Ergebnis von mittels Diensteingabe initiierten oder angeforderten Vorgängen oder Funktionen sind

3.114

einfache Stromverbrauchsanalyse

SPA

(en: simple power analysis)

direkte (hauptsächlich visuelle) Analyse der Muster von Anweisungsausführungen (oder der Ausführung einzelner Anweisungen) im Zusammenhang mit dem Stromverbrauch eines Krypto-Moduls mit dem Ziel, Informationen im Zusammenhang mit dem kryptographischen Betrieb zu erhalten

3.115

Einzelchip-Krypto-Modul

physische Ausführung, bei der ein einzelner integrierter Schaltkreis als eigenständiges Gerät verwendet oder in ein Gehäuse oder ein Produkt eingebettet sein kann, das möglicherweise nicht über einen physischen Schutz verfügt

BEISPIEL Chips mit integriertem Einzelschaltkreis oder Chipkarten mit integriertem Einzelschaltkreis

3.116

Software

ausführbarer Code eines Krypto-Moduls, der auf löschbaren Medien gespeichert ist und während der Ausführung beim Betrieb in einer modifizierbaren Betriebsumgebung dynamisch geschrieben oder modifiziert werden kann

BEISPIEL Löschrare Medien können u. a. sein: Solid-State-Speicher, Festplatten usw.

3.117

Softwaremodul

Modul, das ausschließlich aus Software besteht

3.118

Prüfung zum Laden von Software/Firmware

Reihe von Prüfungen, die mit Software oder Firmware durchgeführt und erfolgreich bestanden werden muss, bevor diese Soft-/Firmware von einem Krypto-Modul ausgeführt werden kann

ANMERKUNG Nicht anwendbar, wenn die Software oder Firmware ein vollständiges Image darstellt und ausschließlich nach einem Power Cycling des Moduls ausgeführt wird

3.119

Software-/Firmwaremodul-Schnittstelle

SFMI

(en: software/firmware module interface)

Befehlssatz zur Anforderung der Dienste des Software- oder Firmwaremoduls, einschließlich Parametern, die im Rahmen des angeforderten Dienstes die kryptographische Begrenzung des Moduls in beliebiger Richtung passieren

3.120

Secret-Sharing

Geheimnisteilung

Technik, bei der ein kryptographischer Schlüssel in mehrere Schlüsselkomponenten aufgeteilt wird, die jeweils keine Auskunft über die anderen Komponenten geben und die anschließend von separaten Entitäten in ein Krypto-Modul eingegeben oder von diesem ausgegeben werden können und in Kombination wieder den ursprünglichen kryptographischen Schlüssel bilden

ANMERKUNG Zur Ausführung dieser Kombination können alle oder nur eine Teilmenge der Komponenten erforderlich sein.

3.121

SSP-Bereitstellung

Vorgang, bei dem ein gemeinsamer SSP für eine oder mehrere Entitäten verfügbar gemacht wird

ANMERKUNG Die SSP-Bereitstellung umfasst SSP-Übereinstimmung, SSP-Transport und SSP-Eingabe oder -Ausgabe.

3.122

Zustandsinformation

Information, die zum Zweck der Anzeige bestimmter Betriebsmerkmale oder -zustände des Krypto-Moduls von diesem Modul ausgegeben wird

3.123

widerstandsfähig

nicht einfach zu besiegen, über mehr als erwartungsgemäße oder überdurchschnittliche Kraft oder Stärke verfügend, widerstandsfähig gegenüber einem Angriff oder solide gebaut

3.124

symmetrische Kryptographietechnik

Kryptographietechnik, bei der sowohl für die Verschlüsselungs- als auch für die Entschlüsselungstransformation derselbe geheime Schlüssel verwendet wird

3.125

Manipulationserkennung

automatisches Bestimmen durch ein Krypto-Modul, dass ein Versuch unternommen wurde, die Sicherheit des Moduls zu kompromittieren

3.126

Manipulationsschutz

beobachtbare Anzeige, dass ein Versuch unternommen wurde, die Sicherheit eines Krypto-Moduls zu kompromittieren

3.127

Manipulationsreaktion

automatische Aktion, die ein Krypto-Modul durchführt, wenn eine Manipulationserkennung stattgefunden hat

3.128

Vertrauensanker

vertrauenswürdige Information, die einen Algorithmus für einen öffentlichen Schlüssel, den Wert eines öffentlichen Schlüssels, einen Ausstellernamen und optional weitere Parameter umfasst

BEISPIEL Zu weiteren Parametern kann u. a. ein Gültigkeitszeitraum zählen

ANMERKUNG Ein Vertrauensanker kann in Form eines selbstsignierten Zertifikats bereitgestellt werden.

3.129

vertrauenswürdiger Kanal

vertrauenswürdige und sichere Kommunikationsverbindung, die zwischen dem Krypto-Modul und einem Absender oder Empfänger aufgebaut ist, um auf sichere Weise ungeschützte Klartext-CSP, Schlüsselkomponenten und Authentisierungsdaten zu übertragen

ANMERKUNG Ein vertrauenswürdiger Kanal schützt vor Abfangversuchen und physischer oder logischer Manipulation durch unerwünschte Bediener/Entitäten, Prozesse oder andere Geräte zwischen den definierten

Eingabe- oder Ausgabeanschlüssen des Krypto-Moduls und entlang der Kommunikationsverbindung mit dem beabsichtigten Endpunkt.

3.130

Anwender

Rolle, die eine Person oder ein Prozess (d. h. ein Subjekt), der für eine Person agiert, inne hat, die/der auf ein Krypto-Modul zugreift, um Kryptographie-Dienste anzufordern

3.131

validiert

mit Sicherheit von einer Validierungsinstanz auf Konformität geprüft

3.132

Validierungsinstanz

Entität, die die Prüfergebnisse zur Konformität mit dieser Internationalen Norm validiert

3.133

Anbieter

Entität, Gruppe oder Vereinigung, die das Krypto-Modul zur Prüfung und Validierung einreicht

ANMERKUNG Der Anbieter hat Zugriff auf alle relevanten Unterlagen und Entwurfsnachweise, ungeachtet dessen, ob er das Krypto-Modul tatsächlich entworfen oder entwickelt hat oder nicht.

3.134

Löschen/Vernichten

Methode des Zerstörens gespeicherter Daten und ungeschützter SSP, um deren Wiederherstellung und Wiederverwendung zu verhindern

Nationaler Anhang NB (informativ)

Literaturhinweise

DIN EN ISO/IEC 27001, *Informationstechnik — Sicherheitsverfahren — Informationssicherheitsmanagementsysteme — Anforderungen*

DIN ISO 9000:2004-12, *Qualitätsmanagement — Leitfaden für Konfigurationsmanagement (ISO 10007:2003)*

— Leerseite —

Contents

Page

1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviated terms	15
5	Cryptographic module security levels	15
5.1	Security Level 1	15
5.2	Security Level 2	16
5.3	Security Level 3	16
5.4	Security Level 4	17
6	Functional security objectives	17
7	Security requirements	18
7.1	General	18
7.2	Cryptographic module specification	20
7.2.1	Cryptographic module specification general requirements	20
7.2.2	Types of cryptographic modules	20
7.2.3	Cryptographic boundary	21
7.2.4	Modes of operations	22
7.3	Cryptographic module interfaces	23
7.3.1	Cryptographic module interfaces general requirements	23
7.3.2	Types of interfaces	24
7.3.3	Definition of interfaces	24
7.3.4	Trusted channel	25
7.4	Roles, services, and authentication	25
7.4.1	Roles, services, and authentication general requirements	25
7.4.2	Roles	26
7.4.3	Services	26
7.4.4	Authentication	28
7.5	Software/Firmware security	29
7.6	Operational environment	31
7.6.1	Operational environment general requirements	31
7.6.2	Operating system requirements for limited or non-modifiable operational environments	33
7.6.3	Operating system requirements for modifiable operational environments	33
7.7	Physical security	35
7.7.1	Physical security embodiments	35
7.7.2	Physical security general requirements	37
7.7.3	Physical security requirements for each physical security embodiment	39
7.7.4	Environmental failure protection/testing	42
7.8	Non-invasive security	43
7.9	Sensitive security parameter management	44
7.9.1	Sensitive security parameter management general requirements	44
7.9.2	Random bit generators	44
7.9.3	Sensitive security parameter generation	44
7.9.4	Sensitive security parameter establishment	45
7.9.5	Sensitive security parameter entry and output	45
7.9.6	Sensitive security parameter storage	46

ISO/IEC 19790:2012(E)

7.9.7	Sensitive security parameter zeroisation.....	46
7.10	Self-tests.....	47
7.10.1	Self-test general requirements.....	47
7.10.2	Pre-operational self-tests.....	47
7.10.3	Conditional self-tests	48
7.11	Life-cycle assurance	50
7.11.1	Life-cycle assurance general requirements.....	50
7.11.2	Configuration management.....	51
7.11.3	Design.....	51
7.11.4	Finite state model	51
7.11.5	Development	52
7.11.6	Vendor testing.....	53
7.11.7	Delivery and operation	54
7.11.8	End of life.....	54
7.11.9	Guidance documents	54
7.12	Mitigation of other attacks	55
Annex A (normative)	Documentation requirements	56
A.1	Purpose.....	56
A.2	Items.....	56
A.2.1	General.....	56
A.2.2	Cryptographic module specification	56
A.2.3	Cryptographic module interfaces	57
A.2.4	Roles, services, and authentication	57
A.2.5	Software/Firmware security	57
A.2.6	Operational environment	58
A.2.7	Physical security	58
A.2.8	Non-invasive security.....	58
A.2.9	Sensitive security parameter management	58
A.2.10	Self-tests.....	59
A.2.11	Life-cycle assurance	60
A.2.12	Mitigation of other attacks	61
Annex B (normative)	Cryptographic module security policy.....	62
B.1	General.....	62
B.2	Items.....	62
B.2.1	General.....	62
B.2.2	Cryptographic module specification	62
B.2.3	Cryptographic module interfaces	63
B.2.4	Roles, services, and authentication	63
B.2.5	Software/Firmware security	64
B.2.6	Operational environment	64
B.2.7	Physical security	64
B.2.8	Non-invasive security.....	65
B.2.9	Sensitive security parameters management	65
B.2.10	Self-tests.....	66
B.2.11	Life-cycle assurance	66
B.2.12	Mitigation of other attacks	66
Annex C (normative)	Approved security functions.....	67
C.1	Purpose.....	67
C.1.1	Block ciphers	67
C.1.2	Stream ciphers.....	67
C.1.3	Asymmetric algorithms and techniques	67
C.1.4	Message authentication codes.....	67
C.1.5	Hash functions.....	67
C.1.6	Entity authentication	68

C.1.7	Key management	68
C.1.8	Random bit generation.....	68
Annex D (normative) Approved sensitive security parameter generation and establishment methods		69
D.1	Purpose.....	69
D.1.1	Sensitive security parameter generation	69
D.1.2	Sensitive security parameter establishment methods	69
Annex E (normative) Approved authentication mechanisms		70
E.1	Purpose.....	70
E.1.1	Authentication mechanisms.....	70
Annex F (normative) Approved non-invasive attack mitigation test metrics		71
F.1	Purpose.....	71
F.1.1	Non-invasive attack mitigation test metrics	71

ISO/IEC 19790:2012(E)

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

Technical corrigendum 1 to ISO/IEC 19790:2012 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This corrected version of Technical corrigendum 1 to ISO/IEC 19790:2012 cancels and replaces the first edition (ISO/IEC 19790:2012/Cor 1:2015), incorporating the same technical revisions and miscellaneous editorial corrections showing in **red** text instead of black underlining:

- 3.21: The term "cryptographic boundary" is corrected;
- 3.80: The term "non-security relevant" is corrected;
- 3.108: The term "self-test" is corrected;
- 7.2.2: The requirements **[02.04]**, **[02.05]** and **[02.06]** are corrected;
- 7.2.4.3: The requirement **[02.31]** is corrected;
- 7.3.3: The requirement **[03.14]** is corrected;
- 7.5: The requirements **[05.06]** and **[05.07]** are added. The requirements **[05.08]**, **[05.13]** and **[05.17]** through **[05.23]** are corrected;
- 7.6.3: The requirement **[06.06]** is corrected;

- 7.8: The requirement [08.04] is corrected;
- 7.9.1: The requirement [09.04] is corrected;
- 7.9.7: The requirement [09.37] is corrected;
- 7.10.2.2: The requirement [10.17] is corrected;
- 7.11.5: The requirement [11.26] is corrected;
- 7.11.7: The requirement [11.35] is corrected;
- 7.11.9: The requirement [11.38] is corrected;
- A.2.5: The requirements of the 1st and 2nd bullets are corrected;
- A.2.7: The requirement of the 3rd bullet is corrected;
- A.2.10: The requirement of the 4th bullet is corrected;
- B.2.4: The requirement of the 9th bullet is corrected;
- B.2.5: The requirement of the 1st bullet is corrected;
- B.2.7: The requirement of the 2nd level 6th bullet is corrected;
- D.1: Duplicate text is removed;
- D.1.2: The reference to ISO/IEC 15946-3 is removed;
- E.1: Duplicate text is removed; and
- F.1: Duplicate text is removed.

ISO/IEC 19790:2012(E)**Introduction**

In Information Technology there is an ever-increasing need to use cryptographic mechanisms such as the protection of data against unauthorised disclosure or manipulation, for entity authentication and for non-repudiation. The security and reliability of such mechanisms are directly dependent on the cryptographic modules in which they are implemented.

This International Standard provides for four increasing, qualitative levels of security requirements intended to cover a wide range of potential applications and environments. The cryptographic techniques are identical over the four security levels. The security requirements cover areas relative to the design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module interfaces; roles, services, and authentication; software/firmware security; operational environment; physical security; non-invasive security; sensitive security parameter management; self-tests; life-cycle assurance; and mitigation of other attacks.

The overall security rating of a cryptographic module must be chosen to provide a level of security appropriate for the security requirements of the application and environment in which the module is to be utilised and for the security services that the module is to provide. The responsible authority in each organization should ensure that their computer and telecommunication systems that utilise cryptographic modules provide an acceptable level of security for the given application and environment. Since each authority is responsible for selecting which approved security functions are appropriate for a given application, compliance with this International Standard does not imply either full interoperability or mutual acceptance of compliant products. The importance of security awareness and of making information security a management priority should be communicated to all concerned.

Information security requirements vary for different applications; organizations should identify their information resources and determine the sensitivity to and the potential impact of a loss by implementing appropriate controls. Controls include, but are not limited to:

- physical and environmental controls;
- access controls;
- software development;
- backup and contingency plans; and
- information and data controls.

These controls are only as effective as the administration of appropriate security policies and procedures within the operational environment.

Information technology — Security techniques — Security requirements for cryptographic modules

1 Scope

This International Standard specifies the security requirements for a cryptographic module utilised within a security system protecting sensitive information in computer and telecommunication systems. This International Standard defines four security levels for cryptographic modules 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 International Standard specifies four security levels for each of 11 requirement areas with each security level increasing security over the preceding level.

This International Standard specifies security requirements specified intended to maintain the security provided by a cryptographic module and compliance to this International Standard is not sufficient to ensure that a particular module is secure or that the security provided by the module is sufficient and acceptable to the owner of the information that is being protected.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

The documents listed in ISO/IEC 19790 Annexes C, D, E and F *Information technology – Security techniques – Security requirements for cryptographic modules*

3 Terms and definitions

For the purposes of this International Standard, the following terms and definitions apply.

- 3.1**
access control list
ACL
list of permissions to grant access to an object
- 3.2**
administrator guidance
written material that is used by the Crypto Officer and/or other administrative roles for the correct configuration, maintenance, and administration of the cryptographic module
- 3.3**
automated
without manual intervention or input (e.g. electronic means such as through a computer network)

ISO/IEC 19790:2012(E)**3.4****approval authority**

any national or international organisation/authority mandated to approve and/or evaluate security functions

NOTE An approval authority in the context of this definition evaluates and approves security functions based on their cryptographic or mathematical merits but is not the testing entity which would test for conformance to this International Standard.

3.5**approved data authentication technique**

approved method that may include the use of a digital signature, message authentication code or keyed hash (e.g. HMAC)

3.6**approved integrity technique**

approved hash, message authentication code or a digital signature algorithm

3.7**approved mode of operation**

set of services which includes at least one service that utilises an approved security function or process and can include non-security relevant services

NOTE 1 Not to be confused with a specific mode of an approved security function, e.g. Cipher Block Chaining (CBC) mode

NOTE 2 Non-approved security functions or processes are excluded.

3.8**approved security function**

security function (e.g. cryptographic algorithm) that is referenced in Annex C

3.9**asymmetric cryptographic technique**

cryptographic technique that uses two related transformations; a public transformation (defined by the public key) and a private transformation (defined by the private key).

NOTE The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation in a given limited time and with given computational resources.

3.10**biometric**

measurable, physical characteristic or personal behavioral trait used to recognise the identity, or verify the claimed identity, of an operator

3.11**bypass capability**

ability of a service to partially or wholly circumvent a cryptographic function

3.12**certificate**

entity's data rendered unforgeable with the private or secret key of a certification authority

NOTE Not to be confused with a modules validation certificate issued by a validation authority

3.13**compromise**

unauthorised disclosure, modification, substitution, or use of critical security parameters or the unauthorised modification or substitution of public security parameters

3.14

conditional self-test

test performed by a cryptographic module when the conditions specified for the test occur

3.15

confidentiality

property that information is not made available or disclosed to unauthorised entities

3.16

configuration management system

CMS

management of security features and assurances through control of changes made to hardware, software and documentation of a cryptographic module

3.17

control information

information that is entered into a cryptographic module for the purposes of directing the operation of the module

3.18

critical security parameter

CSP

security related information whose disclosure or modification can compromise the security of a cryptographic module

EXAMPLE

Secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other trust anchors

NOTE

A CSP can be plaintext or encrypted.

3.19

crypto officer

role taken by an individual or a process (i.e. subject) acting on behalf of an individual that accesses a cryptographic module in order to perform cryptographic initialisation or management functions of a cryptographic module

3.20

cryptographic algorithm

well-defined computational procedure that takes variable inputs, which may include cryptographic keys, and produces an output

3.21

cryptographic boundary

explicitly defined perimeter that establishes the boundary of all components (i.e. set of hardware, software or firmware components) of the cryptographic module

3.22

cryptographic hash function

computationally efficient function mapping binary strings of arbitrary length to binary strings of fixed length, such that it is computationally infeasible to find two distinct values that hash into a common value

3.23

cryptographic key

key

sequence of symbols that controls the operation of a cryptographic transformation

EXAMPLE

A cryptographic transformation can include but not limited to encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification.

ISO/IEC 19790:2012(E)**3.24****cryptographic key component****key component**

parameter used in conjunction with other key components in an approved security function to form a plaintext CSP or perform a cryptographic function

3.25**cryptographic module****module**

set of hardware, software, and/or firmware that implements security functions and are contained within the cryptographic boundary

3.26**cryptographic module security policy****security policy**

precise specification of the security rules under which a cryptographic module shall operate, including the rules derived from the requirements of this International Standard and additional rules imposed by the module or validation authority

NOTE See Annex B

3.27**data path**

physical or logical route over which data passes

NOTE A physical data path can be shared by multiple logical data paths.

3.28**degraded operation**

operation where a subset of the entire set of algorithms, security functions, services or processes are available and/or configurable as a result of reconfiguration from an error state

3.29**differential power analysis****DPA**

analysis of the variations of the electrical power consumption of a cryptographic module, for the purpose of extracting information correlated to cryptographic operation

3.30**digital signature**

data appended to, or a cryptographic transformation of a data unit that allows the recipient of the data unit to prove the origin and integrity of the data unit and protect against forgery (e.g. by the recipient)

3.31**direct entry**

entry of a SSP or key component into a cryptographic module, using a device such as a keyboard

3.32**disjoint signature**

one or more signatures which together represent an entire set of code

3.33**electromagnetic emanations****EME**

intelligence-bearing signal, which, if intercepted and analyzed, potentially discloses the information that is transmitted, received, handled, or otherwise processed by any information-processing equipment