

# SVENSK STANDARD

## SS-EN ISO/IEC 27040:2016



Fastställt/Approved: 2016-09-27

Publicerad/Published: 2016-10-03

Utgåva/Edition: 1

Språk/Language: engelska/English

ICS: 01.140.30; 03.120.10; 04.050; 33.040.40; 35.020; 35.040; 35.080

---

### **Informationsteknik – Säkerhetstekniker – Lagringssäkerhet (ISO/IEC 27040:2015, IDT)**

### **Information technology – Security techniques – Storage security (ISO/IEC 27040:2015, IDT)**

This preview is downloaded from [www.sis.se](http://www.sis.se). Buy the entire standard via <https://www.sis.se/std-8022631>

# Standarder får världen att fungera

*SIS (Swedish Standards Institute) är en fristående ideell förening med medlemmar från både privat och offentlig sektor. Vi är en del av det europeiska och globala nätverk som utarbetar internationella standarder. Standarder är dokumenterad kunskap utvecklad av framstående aktörer inom industri, näringsliv och samhälle och befrämjar handel över gränser, bidrar till att processer och produkter blir säkrare samt effektiviserar din verksamhet.*

## Delta och påverka

Som medlem i SIS har du möjlighet att påverka framtida standarder inom ditt område på nationell, europeisk och global nivå. Du får samtidigt tillgång till tidig information om utvecklingen inom din bransch.

## Ta del av det färdiga arbetet

Vi erbjuder våra kunder allt som rör standarder och deras tillämpning. Hos oss kan du köpa alla publikationer du behöver – allt från enskilda standarder, tekniska rapporter och standardpaket till handböcker och onlinetjänster. Genom vår webbtjänst e-nav får du tillgång till ett lättnavigerat bibliotek där alla standarder som är aktuella för ditt företag finns tillgängliga. Standarder och handböcker är källor till kunskap. Vi säljer dem.

## Utveckla din kompetens och lyckas bättre i ditt arbete

Hos SIS kan du gå öppna eller företagsinterna utbildningar kring innehåll och tillämpning av standarder. Genom vår närhet till den internationella utvecklingen och ISO får du rätt kunskap i rätt tid, direkt från källan. Med vår kunskap om standarders möjligheter hjälper vi våra kunder att skapa verklig nytta och lönsamhet i sina verksamheter.

**Vill du veta mer om SIS eller hur standarder kan effektivisera din verksamhet är du välkommen in på [www.sis.se](http://www.sis.se) eller ta kontakt med oss på tel 08-555 523 00.**



# Standards make the world go round

*SIS (Swedish Standards Institute) is an independent non-profit organisation with members from both the private and public sectors. We are part of the European and global network that draws up international standards. Standards consist of documented knowledge developed by prominent actors within the industry, business world and society. They promote cross-border trade, they help to make processes and products safer and they streamline your organisation.*

## Take part and have influence

As a member of SIS you will have the possibility to participate in standardization activities on national, European and global level. The membership in SIS will give you the opportunity to influence future standards and gain access to early stage information about developments within your field.

## Get to know the finished work

We offer our customers everything in connection with standards and their application. You can purchase all the publications you need from us - everything from individual standards, technical reports and standard packages through to manuals and online services. Our web service e-nav gives you access to an easy-to-navigate library where all standards that are relevant to your company are available. Standards and manuals are sources of knowledge. We sell them.

## Increase understanding and improve perception

With SIS you can undergo either shared or in-house training in the content and application of standards. Thanks to our proximity to international development and ISO you receive the right knowledge at the right time, direct from the source. With our knowledge about the potential of standards, we assist our customers in creating tangible benefit and profitability in their organisations.

**If you want to know more about SIS, or how standards can streamline your organisation, please visit [www.sis.se](http://www.sis.se) or contact us on phone +46 (0)8-555 523 00**



Europastandarden EN ISO/IEC 27040:2016 gäller som svensk standard. Detta dokument innehåller den officiella engelska versionen av EN ISO/IEC 27040:2016.

The European Standard EN ISO/IEC 27040:2016 has the status of a Swedish Standard. This document contains the official English version of EN ISO/IEC 27040:2016.

© Copyright/Upphovsrätten till denna produkt tillhör SIS, Swedish Standards Institute, Stockholm, Sverige. Användningen av denna produkt regleras av slutanvändarlicensen som återfinns i denna produkt, se standardens sista sidor.

© Copyright SIS, Swedish Standards Institute, Stockholm, Sweden. All rights reserved. The use of this product is governed by the end-user licence for this product. You will find the licence in the end of this document.

*Upplysningar om sakinnehållet i standarden lämnas av SIS, Swedish Standards Institute, telefon 08-555 520 00. Standarder kan beställas hos SIS Förlag AB som även lämnar allmänna upplysningar om svensk och utländsk standard.*

*Information about the content of the standard is available from the Swedish Standards Institute (SIS), telephone +46 8 555 520 00. Standards may be ordered from SIS Förlag AB, who can also provide general information about Swedish and foreign standards.*

Denna standard är framtagen av kommittén för Säkerhetsåtgärder och tjänster, SIS/TK 318/AG 41.

Har du synpunkter på innehållet i den här standarden, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standarder inom området? Gå in på [www.sis.se](http://www.sis.se) - där hittar du mer information.



EUROPEAN STANDARD

**EN ISO/IEC 27040**

NORME EUROPÉENNE

EUROPÄISCHE NORM

August 2016

---

ICS 35.040

English Version

**Information technology - Security techniques - Storage  
security (ISO/IEC 27040:2015)**

Technologie de l'information - Techniques de sécurité -  
Sécurité de stockage (ISO/IEC 27040:2015)

Informationstechnik - IT-Sicherheitsverfahren -  
Speichersicherheit (ISO/IEC 27040:2015)

This European Standard was approved by CEN on 19 June 2016.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION  
COMITÉ EUROPÉEN DE NORMALISATION  
EUROPÄISCHES KOMITEE FÜR NORMUNG

**CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels**



# Contents

Page

<b>European foreword</b> .....	<b>2</b>
<b>Introduction</b> .....	<b>vi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Symbols and abbreviated terms</b> .....	<b>7</b>
<b>5 Overview and concepts</b> .....	<b>11</b>
5.1 General.....	11
5.2 Storage concepts.....	12
5.3 Introduction to storage security.....	12
5.4 Storage security risks.....	14
5.4.1 Background.....	14
5.4.2 Data breaches.....	15
5.4.3 Data corruption or destruction.....	16
5.4.4 Temporary or permanent loss of access/availability.....	16
5.4.5 Failure to meet statutory, regulatory, or legal requirements.....	17
<b>6 Supporting controls</b> .....	<b>17</b>
6.1 General.....	17
6.2 Direct Attached Storage (DAS).....	17
6.3 Storage networking.....	18
6.3.1 Background.....	18
6.3.2 Storage Area Networks (SAN).....	18
6.3.3 Network Attached Storage (NAS).....	23
6.4 Storage management.....	24
6.4.1 Background.....	24
6.4.2 Authentication and authorization.....	26
6.4.3 Secure the management interfaces.....	27
6.4.4 Security auditing, accounting, and monitoring.....	28
6.4.5 System hardening.....	30
6.5 Block-based storage.....	31
6.5.1 Fibre Channel (FC) storage.....	31
6.5.2 IP storage.....	31
6.6 File-based storage.....	32
6.6.1 NFS-based NAS.....	32
6.6.2 SMB/CIFS-based NAS.....	33
6.6.3 Parallel NFS-based NAS.....	33
6.7 Object-based storage.....	34
6.7.1 Cloud computing storage.....	34
6.7.2 Object-based Storage Device (OSD).....	35
6.7.3 Content Addressable Storage (CAS).....	36
6.8 Storage security services.....	37
6.8.1 Data sanitization.....	37
6.8.2 Data confidentiality.....	40
6.8.3 Data reductions.....	42

<b>7</b>	<b>Guidelines for the design and implementation of storage security</b>	<b>43</b>
7.1	General	43
7.2	Storage security design principles	43
7.2.1	Defence in depth	43
7.2.2	Security domains	44
7.2.3	Design resilience	45
7.2.4	Secure initialization	45
7.3	Data reliability, availability, and resilience	45
7.3.1	Reliability	45
7.3.2	Availability	46
7.3.3	Backups and replication	46
7.3.4	Disaster Recovery and Business Continuity	47
7.3.5	Resilience	48
7.4	Data retention	48
7.4.1	Long-term retention	48
7.4.2	Short to medium-term retention	49
7.5	Data confidentiality and integrity	50
7.6	Virtualization	52
7.6.1	Storage virtualization	52
7.6.2	Storage for virtualized systems	53
7.7	Design and implementation considerations	54
7.7.1	Encryption and key management issues	54
7.7.2	Align storage and policy	55
7.7.3	Compliance	55
7.7.4	Secure multi-tenancy	56
7.7.5	Secure autonomous data movement	57
	<b>Annex A (normative) Media sanitization</b>	<b>60</b>
	<b>Annex B (informative) Selecting appropriate storage security controls</b>	<b>75</b>
	<b>Annex C (informative) Important security concepts</b>	<b>96</b>
	<b>Bibliography</b>	<b>109</b>



## **European foreword**

The text of ISO/IEC 27040:2015 has been prepared by Technical Committee ISO/IEC JTC 1 “Information technology” of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) and has been taken over as EN ISO/IEC 27040:2016.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by February 2017, and conflicting national standards shall be withdrawn at the latest by February 2017.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN [and/or CENELEC] shall not be held responsible for identifying any or all such patent rights.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

### **Endorsement notice**

The text of ISO/IEC 27040:2015 has been approved by CEN as EN ISO/IEC 27040:2016 without any modification.

## Introduction

Many organizations face the challenge of implementing data protection and security measures to meet a wide range of requirements, including statutory and regulatory compliance. Too often the security associated with storage systems and infrastructure has been missed because of misconceptions and limited familiarity with the storage technology, or in the case of storage managers and administrators, a limited understanding of the inherent risks or basic security concepts. The net result of this situation is that digital assets are needlessly placed at risk of compromise due to data breaches, intentional corruption, being held hostage, or other malicious events.

Data storage has matured in an environment where security has been a secondary concern due to its historical reliance on isolated connectivity, specialized technologies, and the physical security of data centres. Even as storage connectivity evolved to use technologies such as storage protocols over Transmission Control Protocol/Internet Protocol (TCP/IP), few users took advantage of either the inherent security mechanisms or the recommended security measures.

This International Standard provides guidelines for storage security in an organization, supporting in particular the requirements of an Information Security Management System (ISMS) according to ISO/IEC 27001. This International Standard recommends the information security risk management approach as defined in ISO/IEC 27005. It is up to the organization to define their approach to risk management, depending for example on the scope of the ISMS, context of risk management, or industry sector. A number of existing methodologies can be used under the framework described in this International Standard to implement the requirements of an ISMS.

This International Standard is relevant to managers and staff concerned with information security risk management within an organization and, where appropriate, external parties supporting such activities.

The objectives for this International Standard are the following:

- help draw attention to the risks;
- assist organizations in better securing their data when stored;
- provide a basis for auditing, designing, and reviewing storage security controls.

It is emphasized that ISO/IEC 27040 provides further detailed implementation guidance on the storage security controls that are described at a basic standardized level in ISO/IEC 27002.

It should be noted that this International Standard is not a reference or normative document for regulatory and legislative security requirements. Although it emphasizes the importance of these influences, it cannot state them specifically, since they are dependent on the country, the type of business, etc.

# Information technology — Security techniques — Storage security

## 1 Scope

This International Standard provides detailed technical guidance on how organizations can define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation, and implementation of data storage security. Storage security applies to the protection (security) of information where it is stored and to the security of the information being transferred across the communication links associated with storage. Storage security includes the security of devices and media, the security of management activities related to the devices and media, the security of applications and services, and security relevant to end-users during the lifetime of devices and media and after end of use.

Storage security is relevant to anyone involved in owning, operating, or using data storage devices, media, and networks. This includes senior managers, acquirers of storage product and service, and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for information security or storage security, storage operation, or who are responsible for an organization's overall security program and security policy development. It is also relevant to anyone involved in the planning, design, and implementation of the architectural aspects of storage network security.

This International Standard provides an overview of storage security concepts and related definitions. It includes guidance on the threat, design, and control aspects associated with typical storage scenarios and storage technology areas. In addition, it provides references to other International Standards and technical reports that address existing practices and techniques that can be applied to storage security.

## 2 Normative references

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

ITU-TY.3500 | ISO/IEC 17788:2014, *Information technology — Cloud computing — Overview and vocabulary*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 27005, and the following apply.

### 3.1

#### **block**

unit in which data is *stored* (3.50) and retrieved on disk and tape *devices* (3.14)

### 3.2 clear

*sanitize* (3.38) using logical techniques on data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques using the same interface available to the user

### 3.3 compression

process of removing redundancies in digital data to reduce the amount that should be *stored* (3.50) or transmitted

[SOURCE: ISO/TR 12033:2009, 3.1]

Note 1 to entry: For *storage* (3.43), lossless compression (i.e., compression using a technique that preserves the entire content of the original data, and from which the original data can be reconstructed exactly) is required.

### 3.4 cryptographic erase

method of *sanitization* (3.37) in which the encryption key for the encrypted *target data* (3.52) is *sanitized* (3.38), making recovery of the decrypted *target data* (3.52) infeasible

### 3.5 cryptoperiod

defined period of time during which a specific cryptographic key is authorized for use, or during which time the cryptographic keys in a given system can remain in effect

[SOURCE: ISO 16609:2004, 3.9]

### 3.6 data at rest

data *stored* (3.50) on stable *non-volatile storage* (3.30)

### 3.7 data breach

compromise of security that leads to the accidental or unlawful *destruction* (3.13), loss, alteration, unauthorized disclosure of, or access to protected data transmitted, *stored* (3.50), or otherwise processed

### 3.8 data in motion

data being transferred from one location to another

Note 1 to entry: These transfers typically involve interfaces that are accessible and do not include internal transfers (i.e., never exposed to outside of an interface, chip, or device).

### 3.9 data integrity

property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO 7498-2:1989, 3.3.21]

### 3.10 deduplication

method of reducing *storage* (3.43) needs by eliminating redundant data, which is replaced with a pointer to the unique data copy

Note 1 to entry: Deduplication is sometimes considered a form of *compression* (3.3).

### 3.11 degauss

render data unreadable by applying a strong magnetic field to the media

### 3.12

#### **destruct**

*sanitize* (3.38) using physical techniques that make recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for *storage* (3.43) of data

Note 1 to entry: *Disintegrate* (3.15), *incinerate* (3.21), *melt* (3.25), *pulverize* (3.34), and *shred* (3.41) are destruct forms of *sanitization* (3.37).

### 3.13

#### **destruction**

result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible or prohibitively expensive to recover

### 3.14

#### **device**

mechanical, electrical, or electronic contrivance with a specific purpose

[SOURCE: ISO/IEC 14776-372:2011, 3.1.10]

### 3.15

#### **disintegrate**

*destruct* (3.12) by separating media into its component parts

### 3.16

#### **Electronically Stored Information**

data or information of any kind and from any source, whose temporal existence is evidenced by being *stored* (3.50) in, or on, any electronic medium

Note 1 to entry: Electronically Stored Information (ESI) includes traditional e-mail, memos, letters, spreadsheets, databases, office documents, presentations, and other electronic formats commonly found on a computer. ESI also includes system, application, and file-associated *metadata* (3.26) such as timestamps, revision history, file type, etc.

Note 2 to entry: Electronic medium can take the form of, but is not limited to, *storage devices* (3.45) and *storage elements* (3.47).

### 3.17

#### **Fibre Channel**

serial I/O interconnect capable of supporting multiple protocols, including access to open system *storage* (3.43), access to mainframe *storage* (3.43), and networking

Note 1 to entry: Fibre Channel supports point to point, arbitrated loop, and switched topologies with a variety of copper and optical links running at speeds from 1 gigabit per second to over 10 gigabits per second.

### 3.18

#### **Fibre Channel Protocol**

serial Small Computer System Interface (SCSI) transport protocol used on *Fibre Channel* (3.17) interconnects

### 3.19

#### **gateway**

*device* (3.14) that converts a protocol to another protocol

### 3.20

#### **in-band**

communication or transmission that occurs within a previously established communication method or channel

Note 1 to entry: The communications or transmissions often take the form of a separate protocol, such as a management protocol over the same medium as the primary data protocol.

### 3.21

#### **incinerate**

*destruct* (3.12) by burning media completely to ashes

### 3.22

#### **malware**

malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity, or availability

Note 1 to entry: Viruses and Trojan horses are examples of malware.

[SOURCE: ISO/IEC 27033-1:2009, 3.22]

### 3.23

#### **Mean Time Between Failures**

expected time between consecutive failures in a system or component

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.1713, modified — The term was capitalized.]

### 3.24

#### **Mean Time To Repair**

expected or observed duration to return a malfunctioning system or component to normal operations

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.1714, modified — The term was capitalized.]

### 3.25

#### **melt**

*destruct* (3.12) by changing media from a solid to a liquid state generally by the application of heat

### 3.26

#### **metadata**

data that define and describe other data

[SOURCE: ISO/IEC 11179-1:2004, 3.2.16]

### 3.27

#### **multi-factor authentication**

authentication using two or more of the following factors:

- knowledge factor, “something an individual knows”;
- possession factor, “something an individual has”;
- biometric factor, “something an individual is or is able to do”.

[SOURCE: ISO 19092:2008, 4.42]

### 3.28

#### **multi-tenancy**

allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another

[SOURCE: Recommendation ITU-T Y.3500 | ISO/IEC 17788:2014, 3.2.27]

### 3.29

#### **Network Attached Storage**

*storage device* (3.45) or system that connects to a network and provide file access services to computer systems

### 3.30

#### **non-volatile storage**

*storage* (3.43) that retains its contents even after power is removed

### 3.31

#### **out-of-band**

communication or transmission that occurs outside of a previously established communication method or channel

### 3.32

#### **over provisioning**

technique used by *storage elements* (3.47) and *storage devices* (3.45) in which a subset of the available media is exposed through the interface

Note 1 to entry: *Storage media* (3.48) is used internally and independently by the *storage element* (3.47) to improve performance, endurance, or reliability.

### 3.33

#### **point of encryption**

location within the Information and Communications Technology (ICT) infrastructure where data are encrypted on its way to *storage* (3.43) and, conversely, where data are decrypted when accessed from *storage* (3.43)

Note 1 to entry: The point of encryption is only applicable for *data at rest* (3.6).

### 3.34

#### **pulverize**

*destruct* (3.12) by grinding media to a powder or dust

### 3.35

#### **purge**

*sanitize* (3.38) using physical techniques that make recovery infeasible using state of the art laboratory techniques, but which preserves the *storage media* (3.48) in a potentially reusable state

### 3.36

#### **reliability**

ability of a system or component to perform its required functions under stated conditions for a specified period of time

[SOURCE: ISO/IEC/IEEE 24765:2010, 3.2467, modified — The second definition from ISO/IEC 9126-1:2001 and the cf. entry were not included.]

### 3.37

#### **sanitization**

process or method to *sanitize* (3.38)

### 3.38

#### **sanitize**

render access to *target data* (3.52) on *storage media* (3.48) infeasible for a given level of effort

Note 1 to entry: *Clear* (3.2), *purge* (3.35), and *destruct* (3.12) are actions that can be taken to *sanitize* (3.38) *storage media* (3.48).

### 3.39

#### **secure multi-tenancy**

type of *multi-tenancy* (3.28) that employs security controls to explicitly guard against *data breaches* (3.7) and provides validation of these controls for proper governance

Note 1 to entry: Secure multi-tenancy exists when the risk profile of an individual tenant is no greater than it would be in a dedicated, single-tenant environment.

Note 2 to entry: In very secure environments even the identity of the tenants is kept secret.

### 3.40

#### **security strength**

number associated with the amount of work that is required to break a cryptographic algorithm or system

### 3.41

#### **shred**

*destruct* (3.12) by cutting or tearing media into small particles

### 3.42

#### **single point of failure**

element or component of a system, a path in a system, or a system that, if it fails, the whole system or an array of systems are unable to perform their primary functions

Note 1 to entry: A single point of failure is often considered a design flaw associated with a critical element.

### 3.43

#### **storage**

*device* (3.14), function, or service supporting data entry and retrieval

### 3.44

#### **Storage Area Network**

network whose primary purpose is the transfer of data between computer systems and *storage devices* (3.45) and among *storage devices* (3.45)

Note 1 to entry: A SAN consists of a communication infrastructure, which provides physical connections, and a management layer, which organizes the connections, *storage devices* (3.45), and computer systems so that data transfer is secure and robust.

### 3.45

#### **storage device**

any *storage element* (3.48) or aggregation of *storage elements* (3.47), designed and built primarily for the purpose of data *storage* (3.43) and delivery

### 3.46

#### **storage ecosystem**

complex system of interdependent components that work together to enable *storage* (3.43) services and capabilities

Note 1 to entry: The components often include *storage devices* (3.45), storage elements (3.47), storage networks, storage management, and other Information and Communications Technology (ICT) infrastructure.

### 3.47

#### **storage element**

component that is used to build *storage devices* (3.45) and which contributes to data *storage* (3.43) and delivery

Note 1 to entry: Common examples of a storage element include a disk or tape drive.

### 3.48

#### **storage medium**

#### **storage media**

material on which *Electronically Stored Information* (3.16) or digital data are or can be recorded

### 3.49

#### **storage security**

application of physical, technical, and administrative controls to protect storage systems and infrastructure as well as the data *stored* (3.50) within them

Note 1 to entry: Storage security is focused on protecting data (and its storage infrastructure) against unauthorized disclosure, modification, or destruction while assuring its availability to authorized users.

Note 2 to entry: These controls may be preventive, detective, corrective, deterrent, recovery, or compensatory in nature.



**3.50  
store**

record data on *volatile storage* (3.53) or *non-volatile storage* (3.30)

**3.51  
strong authentication**

authentication by means of cryptographically derived credentials

[SOURCE: ISO/TS 22600-1:2006, 2.23]

**3.52  
target data**

information subject to a given process, typically including most or all information on a piece of *storage media* (3.48)

**3.53  
volatile storage**

*storage* (3.43) that fails to retain its contents after power is removed

**3.54  
weak key**

key that interacts with some aspect of a particular cipher's definition in such a way that it weakens the *security strength* (3.40) of the cipher

## 4 Symbols and abbreviated terms

ACE	Access Control Entry
ACL	Access Control List
AD	Active Directory
AES	Advanced Encryption Standard
ATA	Advanced Technology Attachment
BC	Business Continuity
BCM	Business Continuity Management
CAS	Content Addressable Storage
CBC	Cipher Block Chaining
CCM	Counter with Cipher block chaining Message authentication code
CDMI	Cloud Data Management Interface
CDP	Continuous Data Protection
CHAP	Challenge Handshake Authentication Protocol
CIFS	Common Internet File System
CLI	Command Line Interface
CNA	Converged Network Adaptor
DAC	Discretionary Access Control

DAS	Direct Attached Storage
DDoS	Distributed Denial of Service
DH-CHAP	Diffie Hellman – Challenge Handshake Authentication Protocol
DES	Data Encryption Standard
DLM	Data Lifecycle Management
DMZ	De-Militarized Zone
DNS	Domain Name System
DoS	Denial of Service
DR	Disaster Recovery
DRP	Disaster Recovery Planning
EHR	Electronic Healthcare Record
ESI	Electronically Stored Information
ESP	Encapsulating Security Payload
FC	Fibre Channel
FC-SP	Fibre Channel – Security Protocol
FCAP	Fibre Channel Certificate Authentication Protocol
FCEAP	Fibre Channel Extensible Authentication Protocol
FCIP	Fibre Channel over TCP/IP
FCoE	Fibre Channel over Ethernet
FCP	Fibre Channel Protocol
FCPAP	Fibre Channel Password Authentication Protocol
FCS	Fixed Content Storage
FDE	Full Disk Encryption
GCM	Galois/Counter Mode
GUI	Graphical User Interface
HAMR	Heat Assisted Magnetic Recording
HBA	Host Bus Adapter
HDD	Hard Disk Drive
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communications Technology
ID	Identifier

IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
ILM	Information Lifecycle Management
I/O	Input/Output
IP	Internet Protocol
IPS	Intrusion Prevention System
IPOCM	Incident Preparedness and Operational Continuity Management
IPsec	Internet Protocol Security
IRBC	ICT Readiness for Business Continuity
iSCSI	Internet Small Computer Systems Interface
ISL	Inter-Switch Link
ISMS	Information Security Management System
iSNS	Internet Storage Name Service
KEK	Key Encryption Key
KMIP	Key Management Interoperability Protocol
LAN	Local Area Network
LBA	Logical Block Address
LDAP	Lightweight Directory Access Protocol
LUN	Logical UNit
MAC	Mandatory Access Control
MD5	Message-Digest algorithm 5
MEK	Media Encryption Key
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
NAS	Network Attached Storage
NAT	Network Address Translation
NFS	Network File System
NIC	Network Interface Card