

CompTIA Security+ Acronyms

The following is a list of acronyms that appear on the CompTIA Security+ exam. Candidates are encouraged to review the complete list and attain a working knowledge of all listed acronyms as a part of a comprehensive exam preparation program.

ACRONYM	SPELLED OUT	ACRONYM	SPELLED OUT
3DES	Triple Digital Encryption Standard	CER	Cross-over Error Rate
AAA	Authentication, Authorization, and Accounting	CERT	Computer Emergency Response Team
ABAC	Attribute-based Access Control	CFB	Cipher Feedback
ACL	Access Control List	CHAP	Challenge Handshake Authentication Protocol
AES	Advanced Encryption Standard	CIO	Chief Information Officer
AES256	Advanced Encryption Standards 256bit	CIRT	Computer Incident Response Team
AH	Authentication Header	CMS	Content Management System
ALE	Annualized Loss Expectancy	COOP	Continuity of Operations Plan
AP	Access Point	COPE	Corporate Owned, Personally Enabled
API	Application Programming Interface	CP	Contingency Planning
APT	Advanced Persistent Threat	CRC	Cyclical Redundancy Check
ARO	Annualized Rate of Occurrence	CRL	Certificate Revocation List
ARP	Address Resolution Protocol	CSIRT	Computer Security Incident Response Team
ASLR	Address Space Layout Randomization	CSO	Chief Security Officer
ASP	Application Service Provider	CSP	Cloud Service Provider
AUP	Acceptable Use Policy	CSR	Certificate Signing Request
AV	Antivirus	CSRF	Cross-site Request Forgery
AV	Asset Value	CSU	Channel Service Unit
BAC	Business Availability Center	CTM	Counter-Mode
BCP	Business Continuity Planning	CTO	Chief Technology Officer
BIA	Business Impact Analysis	CTR	Counter
BIOS	Basic Input/Output System	CYOD	Choose Your Own Device
BPA	Business Partners Agreement	DAC	Discretionary Access Control
BPDU	Bridge Protocol Data Unit	DBA	Database Administrator
BYOD	Bring Your Own Device	DDoS	Distributed Denial of Service
CA	Certificate Authority	DEP	Data Execution Prevention
CAC	Common Access Card	DER	Distinguished Encoding Rules
CAN	Controller Area Network	DES	Digital Encryption Standard
CAPTCHA	Completely Automated Public Turing Test to Tell Computers and Humans Apart	DFIR	Digital Forensics and Investigation Response
CAR	Corrective Action Report	DHCP	Dynamic Host Configuration Protocol
CBC	Cipher Block Chaining	DHE	Data-Handling Electronics
CCMP	Counter-Mode/CBC-Mac Protocol	DHE	Diffie-Hellman Ephemeral
CCTV	Closed-circuit Television	DLL	Dynamic Link Library
CER	Certificate	DLP	Data Loss Prevention
		DMZ	Demilitarized Zone

DNAT	Destination Network Address Transaction	IDEA	International Data Encryption Algorithm
DNS	Domain Name Service (Server)	IDF	Intermediate Distribution Frame
DoS	Denial of Service	IdP	Identity Provider
DRP	Disaster Recovery Plan	IDS	Intrusion Detection System
DSA	Digital Signature Algorithm	IEEE	Institute of Electrical and Electronic Engineers
DSL	Digital Subscriber Line	IIS	Internet Information System
DSU	Data Service Unit	IKE	Internet Key Exchange
EAP	Extensible Authentication Protocol	IM	Instant Messaging
ECB	Electronic Code Book	IMAP4	Internet Message Access Protocol v4
ECC	Elliptic Curve Cryptography	IoT	Internet of Things
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral	IP	Internet Protocol
ECDSA	Elliptic Curve Digital Signature Algorithm	IPSec	Internet Protocol Security
EFS	Encrypted File System	IR	Incident Response
EMI	Electromagnetic Interference	IR	Infrared
EMP	Electro Magnetic Pulse	IRC	Internet Relay Chat
ERP	Enterprise Resource Planning	IRP	Incident Response Plan
ESN	Electronic Serial Number	ISA	Interconnection Security Agreement
ESP	Encapsulated Security Payload	ISP	Internet Service Provider
EF	Exposure Factor	ISSO	Information Systems Security Officer
FACL	File System Access Control List	ITCP	IT Contingency Plan
FAR	False Acceptance Rate	IV	Initialization Vector
FDE	Full Disk Encryption	KDC	Key Distribution Center
FRR	False Rejection Rate	KEK	Key Encryption Key
FTP	File Transfer Protocol	L2TP	Layer 2 Tunneling Protocol
FTPS	Secured File Transfer Protocol	LAN	Local Area Network
GCM	Galois Counter Mode	LDAP	Lightweight Directory Access Protocol
GPG	Gnu Privacy Guard	LEAP	Lightweight Extensible Authentication Protocol
GPO	Group Policy Object	MaaS	Monitoring as a Service
GPS	Global Positioning System	MAC	Mandatory Access Control
GPU	Graphic Processing Unit	MAC	Media Access Control
GRE	Generic Routing Encapsulation	MAC	Message Authentication Code
HA	High Availability	MAN	Metropolitan Area Network
HDD	Hard Disk Drive	MBR	Master Boot Record
HIDS	Host-based Intrusion Detection System	MD5	Message Digest 5
HIPS	Host-based Intrusion Prevention System	MDF	Main Distribution Frame
HMAC	Hashed Message Authentication Code	MDM	Mobile Device Management
HOTP	HMAC-based One-Time Password	MFA	Multi-Factor Authentication
HSM	Hardware Security Module	MFD	Multi-function Device
HTML	Hypertext Markup Language	MITM	Man-in-the-Middle
HTTP	Hypertext Transfer Protocol	MMS	Multimedia Message Service
HTTPS	Hypertext Transfer Protocol over SSL/TLS	MOA	Memorandum of Agreement
HVAC	Heating, Ventilation and Air Conditioning	MOU	Memorandum of Understanding
IaaS	Infrastructure as a Service	MPLS	Multi-protocol Label Switching
ICMP	Internet Control Message Protocol	MSCHAP	Microsoft Challenge Handshake Authentication Protocol
ICS	Industrial Control Systems		
ID	Identification	MSP	Managed Service Provider

ACRONYM	SPELLED OUT
MTBF	Mean Time Between Failures
MTTF	Mean Time to Failure
MTTR	Mean Time to Recover or Mean Time to Repair
MTU	Maximum Transmission Unit
NAC	Network Access Control
NAT	Network Address Translation
NDA	Non-disclosure Agreement
NFC	Near Field Communication
NGAC	Next Generation Access Control
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards & Technology
NTFS	New Technology File System
NTLM	New Technology LAN Manager
NTP	Network Time Protocol
OAuth	Open Authorization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OS	Operating System
OTA	Over The Air
OVAL	Open Vulnerability Assessment Language
P12	PKCS #12
P2P	Peer to Peer
PaaS	Platform as a Service
PAC	Proxy Auto Configuration
PAM	Pluggable Authentication Modules
PAP	Password Authentication Protocol
PAT	Port Address Translation
PBKDF2	Password-based Key Derivation Function 2
PBX	Private Branch Exchange
PCAP	Packet Capture
PEAP	Protected Extensible Authentication Protocol
PED	Personal Electronic Device
PEM	Privacy-enhanced Electronic Mail
PFS	Perfect Forward Secrecy
PFX	Personal Exchange Format
PGP	Pretty Good Privacy
PHI	Personal Health Information
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
POODLE	Padding Oracle on Downgrade Legacy Encryption
POP	Post Office Protocol
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol

ACRONYM	SPELLED OUT
PSK	Pre-shared Key
PTZ	Pan-Tilt-Zoom
RA	Recovery Agent
RA	Registration Authority
RAD	Rapid Application Development
RADIUS	Remote Authentication Dial-in User Server
RAID	Redundant Array of Inexpensive Disks
RAS	Remote Access Server
RAT	Remote Access Trojan
RBAC	Role-based Access Control
RBAC	Rule-based Access Control
RC4	Rivest Cipher version 4
RDP	Remote Desktop Protocol
RFID	Radio Frequency Identifier
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
ROI	Return on Investment
RMF	Risk Management Framework
RPO	Recovery Point Objective
RSA	Rivest, Shamir, & Adleman
RTBH	Remotely Triggered Black Hole
RTO	Recovery Time Objective
RTOS	Real-time Operating System
RTP	Real-time Transport Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SaaS	Software as a Service
SAML	Security Assertions Markup Language
SAN	Storage Area Network
SAN	Subject Alternative Name
SCADA	System Control and Data Acquisition
SCAP	Security Content Automation Protocol
SCEP	Simple Certificate Enrollment Protocol
SCP	Secure Copy
SCSI	Small Computer System Interface
SDK	Software Development Kit
SDLC	Software Development Life Cycle
SDLM	Software Development Life Cycle Methodology
SDN	Software Defined Network
SED	Self-encrypting Drive
SEH	Structured Exception Handler
SFTP	Secured File Transfer Protocol
SHA	Secure Hashing Algorithm
SHTTP	Secure Hypertext Transfer Protocol
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SLA	Service Level Agreement

ACRONYM	SPELLED OUT
SLE	Single Loss Expectancy
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SMTPS	Simple Mail Transfer Protocol Secure
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SoC	System on Chip
SPF	Sender Policy Framework
SPIM	Spam over Internet Messaging
SPoF	Single Point of Failure
SQL	Structured Query Language
SRTP	Secure Real-Time Protocol
SSD	Solid State Drive
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SSO	Single Sign-on
STP	Shielded Twisted Pair
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TGT	Ticket Granting Ticket
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TOTP	Time-based One-time Password
TPM	Trusted Platform Module
TSIG	Transaction Signature
UAT	User Acceptance Testing
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UPS	Uninterruptable Power Supply
URI	Uniform Resource Identifier
URL	Universal Resource Locator
USB	Universal Serial Bus
USB OTG	USB On The Go
UTM	Unified Threat Management
UTP	Unshielded Twisted Pair
VDE	Virtual Desktop Environment
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Masking
VM	Virtual Machine
VoIP	Voice over IP
VPN	Virtual Private Network

ACRONYM	SPELLED OUT
VTC	Video Teleconferencing
WAF	Web Application Firewall
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WORM	Write Once Read Many
WPA	WiFi Protected Access
WPA2	WiFi Protected Access 2
WPS	WiFi Protected Setup
WTLS	Wireless TLS
XML	Extensible Markup Language
XOR	Exclusive Or
XSRF	Cross-site Request Forgery
XSS	Cross-site Scripting