24.1. Glossary of Abbreviations

Glossary of Abbreviations

24.1.1.

Abbreviation	Meaning
3DES	Triple Data Encryption Standard
ABAC	Attribute Based Access Control
AES	Advanced Encryption Standard
AH	Authentication Header
AISEP	Australasian Information Security Evaluation Program
AoG	All-of-Government
AS	Australian Standard
ASD	Australian Signals Directorate
BYOD	Bring Your Own Device
BYOK	Bring Your Own Keys
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria
CCI	Controlled Cryptographic Item
CCRA	Common Criteria Recognition Arrangement
CDS	Cross-Domain Solution
CEO	Chief Executive Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COMSEC	Communications Security
CSfC	Commercial Solutions for Classified
CSO	Chief Security Officer
CSP	Cloud Service Provider
DdoS	Distributed Denial-Of-Service
DH	Diffie-Hellman
DIS	Draft International Standard
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting and Conformance
DMZ	Demilitarized zone
DoS	Denial-Of-Service
DSA	Digital Signature Algorithm

EAL	Evaluation Assurance Level
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
ECB	Electronic Code Book mode
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read-Only Memory
EPL	Evaluated Products List
EPLD	Evaluated Products List – Degausser
EPROM	Erasable Programmable Read-Only Memory
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
FTL	Flash Transition Layer
GCDO	NZ Government Chief Digital Officer
GCSB	Government Communications Security Bureau
GPU	Graphics Processing Unit
HA	High Availability
HACE	High Assurance Cryptographic Equipment
HB	Handbook
HGCE	High Grade Cryptographic Equipment. Terminology superseded by HACE.
HGCP	High Grade Cryptographic Products. Terminology superseded by HACE.
HMAC	Hashed Message Authentication Code
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HYOK	Hold Your Own Keys
IaaS	Infrastructure-as-a-Service
ICT	Information And Communications Technology
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute Of Electrical And Electronics Engineers
IETF	International Engineering Task Force

IKE	Internet Key Exchange
IM	Instant Messaging
IMS	IP Multimedia Subsystem
IODEF	Incident Object Description Exchange Format
IP	Internet Protocol
IPSec	Internet Protocol Security
IR	Infrared
IRC	Internet Relay Chat
IPT	Internet Protocol Telephony
IRP	Incident Response Plan
ISAKMP	Internet Security Association Key Management Protocol
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria
ITSM	Information Technology Security Manager
IWF	Inter-Working Function
KMP	Key Management Plan
KMS	Key management system
MDM	Mobile Device Manager
MFA	Multi-Factor Authentication
MFD	Multifunction Device
MMS	Multimedia Message Service
MSL	(New Zealand) Measurement Standards Laboratory
NAND	Flash Memory Named After The NAND Logic Gate
NAND	NOT AND – A Binary Logic Operation
NDPP	Network Device Protection Profile
NIST	National Institute Of Standards And Technology
NOR	Flash Memory Named After The NOR Logic Gate
NOR	NOT OR – A Binary Logic Operation
NTP	Network Time Protocol
NZCSI	New Zealand Communications Security Instruction
NZCSP	New Zealand Communications Security Policy
NZ e-GIF	New Zealand E-Government Interoperability Framework

NZEO	New Zealand Eyes Only
NZISM	New Zealand Information Security Manual
NZS	New Zealand Standard
OTP	One-Time Password
PaaS	Platform-as-a-Service
PAM	Privileged Access Management
PBX	Private Branch Exchange
PED	Portable Electronic Device
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PP	Protection Profile
PSR	Protective Security Requirements
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAM	Random Access Memory
RBAC	Role-Based Access Control
RF	Radio Frequency
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman
RTP	Real-Time Transport Protocol
SaaS	Software-as-a-Service
SBC	Session Border Controller
SCEC	Security Construction And Equipment Committee
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SCIM	System for Cross-domain Identity Management
SDN	Software Defined Networking
SecPlan	System Security Plan
SecPol	System Security Policy
SitePlan	System Site Plan
SHA	Secure Hashing Algorithm
SIM	Subscriber Identity Module

SIP	Session Initiation Protocol
SLA	Service Level Agreement
S/MIME	Secure Multipurpose Internet Mail Extension
SMS	Short Message Service
SOE	Standard Operating Environment
SOP	Standard Operating Procedure
SP	Special Publication
SPF	Sender Policy Framework
SRMP	Security Risk Management Plan
SSD	Solid State Drive
SSH	Secure Shell
SSL	Secure Sockets Layer
SSP	System Security Plan
TLS	Transport Layer Security
TOE	Target of Evaluation (in Common Criteria)
TOE	Trusted Operating Environment
UC	Unified Communication
UTC	Co-ordinated Universal Time
VDP	Vulnerability Disclosure Policy
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WEEE	Waste Electrical and Electronic Equipment
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access 2
XAUTH	Ike Extended Authentication