

ACRONYMS

3DES	Triple Data Encryption Standard	IV	Initialization Vector
AES	Advanced Encryption Standard	KDC	Key Distribution Center
AH	Authentication Header	MAC	Mandatory Access Control
ANSI	American National Standards Institute	MAC	Message Authentication Code
ATM	Automatic Teller Machine	MIC	Message Integrity Code
CBC	Cipher Block Chaining	MIME	Multipurpose Internet Mail Extension
CC	Common Criteria	MLS	Multilevel Security
CFB	Cipher Feedback	MTU	Maximum Transmission Unit
CMAC	Cipher-Based Message Authentication Code	NIDA	Network-Based IDS
DAC	Discretionary Access Control	NIST	National Institute of Standards and Technology
DBMS	Database Management System	NSA	National Security Agency
DDoS	Distributed Denial of Service	OFB	Output Feedback
DES	Data Encryption Standard	PIN	Personal Identification Number
DMZ	Demilitarized Zone	PIV	Personal Identity Verification
DoS	Denial of Service	PKI	Public Key Infrastructure
DSA	Digital Signature Algorithm	PRNG	Pseudorandom Number Generator
DSS	Digital Signature Standard	RDBMS	Relational Database Management System
ECB	Electronic Codebook	RBAC	Role-Based Access Control
ESP	Encapsulating Security Payload	RFC	Request for Comments
FIPS	Federal Information Processing Standard	RNG	Random Number Generator
IAB	Internet Architecture Board	RSA	Rivest-Shamir-Adelman
ICMP	Internet Control Message Protocol	SHA	Secure Hash Algorithm
IDS	Intrusion Detection System	SHS	Secure Hash Standard
IETF	Internet Engineering Task Force	S/MIME	Secure MIME
IP	Internet Protocol	SQL	Structured Query Language
IPSec	IP Security	SSL	Secure Sockets Layer
ISO	International Organization for Standardization	TCP	Transmission Control Protocol
ITU	International Telecommunication Union	TLS	Transport Layer Security
ITU-T	ITU Telecommunication Standardization Sector	TPM	Trusted Platform Module
		UDP	User Datagram Protocol
		VPN	Virtual Private Network