Ingrian Networks DataSecure Appliance

i430, i426, and i116

Security Policy

April 30, 2008

Version: 1.0

Prepared by:

Ingrian Networks

350 Convention Way

Redwood City, CA 94063-1405

TABLE OF CONTENTS

1. Module Overview

The Ingrian DataSecure Appliance i430, i426, i116 is a multi-chip standalone cryptographic module that is encased in a hard, opaque, commercial grade metal case and is a hardware/software solution for providing security and cryptographic processing. The cryptographic module also utilizes an internal server called the Network-Attached Encryption Server, which executes a range of security-related tasks, including processing all cryptographic requests generated by NAE connectors residing on application servers and databases.

The module configurations under validation are as follows:

DataSecure Appliance i430: HW P/N DS-0430-0100-00; FW Version 4.6.5
DataSecure Appliance i430: HW P/N DS-0430-01NP-00; FW Version 4.6.5[1]
DataSecure Appliance i426: HW P/N DS-0426-0100-00; FW Version 4.6.5
DataSecure Appliance i116: HW P/N DS-0116-0100-00; FW Version 4.6.5

The cryptographic module provides several interfaces for data input, data output, status output, and command input. The following images show the module's cryptographic boundary, which is the surrounding hard, opaque, commercial grade metal case, and the module's interfaces:

Figure 1 – Image of the i430

[1] Note that both hardware platforms listed for the i430 are the exact same hardware but are referenced differently depending on usage (i.e. production versus non-production).

Figure 2 – Image of the i426

Figure 3 – Image of the i116

The following outlines the different hardware configurations of the Ingrian DataSecure Appliance:

Ingrian DataSecure Appliance i116 Hardware

VIA C3 800 MHz CPU, 1GB RAM, 80GB SATA drive

This hardware platform is intended for smaller deployments. It features a single processor architecture and single hard drive resource and can process more than 11000 secure cryptographic operations per second.

Ingrian DataSecure Appliance i430 Hardware

Single Quad Core CPU, 1U Rack Mountable Chassis, 1GB RAM, Dual 80 GB SATA drives

This hardware platform is intended for larger deployments. It features a single processor architecture and single hard drive resource and can process more than 100000 secure cryptographic operations per second. The hard drive is hot swappable.

Ingrian DataSecure Appliance i426 Hardware

Two Dual Core CPUs, 2U Rack Mountable Chassis, 1GB RAM, 2 80GB SATA in RAID configuration.

This hardware platform is intended for larger deployments. It features a dual processor architecture and dual hard drives in a RAID-1 mirroring configuration. These drives are hot swappable. This appliance can process more than 45000 secure cryptographic operations per second.

NOTE: The hot swappable hard drives in the i430 and i426 are not allowed to be removed while the module is in FIPS mode (see Section 3 below).

2. Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved mode of operation

The cryptographic module supports the following FIPS Approved algorithms:

- DSA with 1024-bit keys for digital signature generation and verification
- RSA with 1024/2048-bit keys for digital signature generation and verification
- Triple-DES (three key) for encryption and decryption
- Triple-DES (two key) for encryption and decryption
- AES for encryption and decryption
- SHA-1 for hashing
- HMAC-SHA-1
- ANSI X9.31 DRNG for key generation
- Diffie-Hellman for key agreement within SSH V2 protocol (SP 800-56A, vendor affirmed, key establishment provides 80 bits of encryption strength)

The cryptographic module relies on the implemented deterministic random number generator (DRNG) that is compliant with ANSI X9.31 for generation of all cryptographic keys.

The cryptographic module supports the following commercially available protocols:

- TLS/SSL V3.1 protocol for key establishment (RSA for key transport provides 80 or 112 bits of encryption strength)
- SSH V2 protocol for key establishment (Diffie-Hellman for key agreement - see FIPS Approved algorithms listed above)

The module also supports the following algorithms, which are allowed for use in FIPS mode:

- NDRNG to generate the seed value and seed key for the ANSI X9.31 DRNG
- MD5 (as part of TLS/SSL)

The cryptographic module may be configured for FIPS mode via establishing the following configuration settings. Any deviation from the following configuration settings will put the module in non-FIPS mode.

Authorized users can set the module in FIPS mode by setting the 'Set FIPS compliant' button under the high security configuration tab. The module is in FIPS mode when the ‘Set FIPS Mode’ button is enabled and is not in FIPS Mode if otherwise.

NOTES:

1. *The hot swappable hard drives in the i430 and i426 are not allowed to be removed while the module is in FIPS mode.*
2. *For the i430 and i426, the removable power supplies are excluded from FIPS 140-2 requirements. (For the i116, no components are excluded from FIPS 140-2 requirements.)*

Non-FIPS mode of operation

In non-FIPS mode, the cryptographic module provides non-FIPS Approved algorithms as follows:

- RSA 512, 768
- Single DES
- SEED
- RC4

4. Ports and Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

1) Serial Port (RS232 DB9): data input, data output, status output, command input
2) Ethernet 10/100/1000 (Qty. 1 or 2): data input, data output, status output, command input
3) PS2: control input (BIOS) (Qty. 2)
4) VGA: data output, status output (BIOS)
5) Power Interface: power

5. Identification and Authentication Policy

Assumption of roles

The cryptographic module shall support five distinct operator roles (User, Cryptographic Officer/Administrator, Ingrian User, Cluster Member and File Encryption User). The cryptographic module shall enforce the separation of roles using identity-based operator authentication. An operator must enter a username and its password and/or provide a certificate to log in. The username is an alphanumeric string of one or more characters. The password is a string of eight or more characters chosen by the operator from the 90 printable and human-readable characters. Upon correct authentication, the role is selected based on the username of the operator and the logical interface that the operator is connected to. At the end of a session, the operator must log-out.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	Username/Password and/or Public Certificate

Role	Type of Authentication	Authentication Data
Cryptographic-Officer[2]	Identity-based operator authentication	Username/Password with the option of a Public Certificate
Ingrian User	Identity-based operator authentication	Public Certificate
Cluster Member	Identity-based operator authentication	Public Certificate
File Encryption User	Identity-based operator authentication	Public Certificate

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username/Password	The probability that a random attempt will succeed or a false acceptance will occur is 1/4,304,672,100,000,000 which is less than 1/1,000,000. The number of authentication attempts that can be made is 6 per minute (i.e. after 6 unsuccessful authentication attempts the account is locked for one minute). Therefore the probability of successfully authenticating to the module within one minute is 6/4,304,672,100,000,000 which is less than 1/100,000.
Username/Password and Public Certificate	The probability that a random attempt will succeed or a false acceptance will occur is less than $\frac{1}{2^{80}}$ which is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute is also less

[2] It should be noted that the terms 'Administrators' and 'Cryptographic Officer' are used interchangeably throughout this document.

	than $\frac{1}{2^{80}}$ which is less than 1/100,000.
Public Certificate	The probability that a random attempt will succeed or a false acceptance will occur is less than $\frac{1}{2^{80}}$ which is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute is also less than $\frac{1}{2^{80}}$ which is less than 1/100,000.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
User: This role is associated with external applications that connect via the module's XML interface. This user is allocated all cryptographic services for keys that they have permission to access, such as encrypt data, decrypt data, sign data, and verify data.	• Encrypt Data: This service TDES or AES encrypts plaintext data passed into the cryptographic module. • Decrypt Data: This service TDES or AES decrypts ciphertext data passed into the cryptographic module. • Sign Data: This service digitally signs data with RSA or DSA. • Verify Data: This service verifies the digital signature with RSA or DSA. • MAC Verify Data: The module enters this state when a user wants to MAC verify a block of data. • MAC Data: The module will enter this state when a user wants to MAC a block of data. • Export Key: This service allows a User to export encrypted cryptographic keys. • Query Key Names: This service allows a User to output the list of key names and meta data that he/she is allowed to access. • Download Certificate: This service allows a User to

	download a certificate into the module. • Query Key Meta Data: This service allows a User to output the following key information that he/she is allowed to access: key length, whether a key is exportable, whether a key can be deleted by current user, key permissions, and supported algorithms and modes for a key. • Generate Random Bytes: This service allows a User to generate and return random data up to 2^{17} bytes. • Authenticate User: This service allows an operator to authenticate into the User role with a username and password. Authentication into the User role may also require an SSL tunnel to be created. None of the above services can be accessed until an operator successfully authenticates into a User role.
Cryptographic-Officer: This role is associated with human administrators who can access the module via the Web Management Console and/or the CLI. This role provides all services that are necessary for the secure management of the module.	• Key Management: This service allows a CO to manage all cryptographic keys that are stored with in the module. This includes, the generation, storage, export (only public keys can be export directly), import, and zeroization of keys. • Update Firmware: This service allows a CO to upgrade the module's firmware. • Cluster Management: This service allows a CO to manage clusters. This includes the creation, joining, and removal of a cluster from the module. • Certificate Management: This service allows a CO to create/import/revoke certificates within the module. • Service Management: This service allows a CO to manage all services that the module supports. This includes the starting and stopping of all services. • Enable/Disable FIPS Mode: This service allows the CO configure the module into its FIPS validated configuration. • Operator Management: This service allows a CO to create, modify, or delete module operators. The operators include Cryptographic Officers and Users. • Reset Factory Settings: This service allows a CO to rollback to the default image that was shipped with the module.

	• Restore Default Configuration: This service allows a CO to delete the current configuration file and restore the default configuration settings. • Restore Configuration File: This service allows a CO to restore a previously backed up configuration file. • Backup Configuration File: This service allows a CO to back up a configuration file • Migrate DB: This service allows a CO to encrypt and decrypt columns from a specific database. • Authenticate Administrator: This service allows an operator to authenticate into the Administrator role with a username and password. • Zeroize Key(s): This service allows a CO to delete a specific key.
Cluster Member: This role is associated to other DataSecure Servers that can connect to this module to create a cluster.	• Receive Configuration File: This service allows a Cluster Member to update the module's configuration settings. • Zeroize Key(s): This service allows a Cluster Member to delete a specific key. • Backup Configuration File: This service allows a Cluster Member to back up a configuration file. • Authenticate Cluster Member: This service allows another module to authenticate into the module as a Cluster Member via an SSL tunnel. None of the above services can be accessed until another module is authenticated into the Cluster Member role.
Ingrian User: This role is associated with an Ingrian employee who can bring the module back into an "uninitialized state" in the event that the all CO passwords are lost.	• Authenticate Ingrian User: This service allows an operator to authenticate into the Ingrian User role with a signed token. None of the below services can be accessed until an operator has successfully authenticated as an Ingrian User. • Restore Default Configuration: This service allows an Ingrian User to delete the current configuration file and restore the default configuration settings. • Reset Factory Settings: This service allows an Ingrian User to rollback to the default image that was shipped with the

	module. • Zeroize Key(s): This service will automatically zeroize all keys when Restore Default Configuration and Reset Factory Settings are activated
File Encryption User: This role is associated with the File Encryption Connector.	• Authenticate File Encryption User: This service allows the File Encryption Connector to authenticate into the module as a File Encryption User via a TLS tunnel. None of the below services can be accessed until the File Encryption Connector is authenticated into the File Encryption User role. • Request/Export Encrypted Key and Metadata: This Service allows a File Encryption User to request encrypted AES keys and metadata associated with the key. • Push Log Information: This service allows a File Encryption User to push log files to the module regarding key usage by the File Encryption Connector.

Unauthenticated Services:

The cryptographic module supports the following unauthenticated services:

- Health Status: This service provides the current statistics of the cryptographic module;
- Self-tests: This service executes the suite of self-tests required by FIPS 140-2.
- SNMP statistics;
- Initiation of authentication mechanisms (e.g. TLS, SSH);
- Version negotiation of XML protocol.

Table 5 - Specification of Service Inputs & Outputs

Service	Control Input	Data Input	Data Output	Status Output
Encrypt Data	Encrypt Command	Plaintext data Key name Algorithm Parameters	Ciphertext data	Success/fail
Decrypt Data	Decrypt Command	Ciphertext data Key name Algorithm Parameters	Plaintext data	Success/fail
Sign Data	Sign Command	Data to be signed Key name Algorithm Parameters	Signed data	Success/fail
Verify Data	Verify Command	Data with signature Key name Algorithm Parameters	None	Success/fail
MAC Verify Data	MAC Verify Command	Data to be verified with MAC Key name Algorithm Parameters	None	Success/fail
MAC Data	MAC Data Command	Data to be MAC-ed Key name Algorithm Parameters	MAC-ed data	Success/fail

Service	Control Input	Data Input	Data Output	Status Output
Export Key	Export Key Command	Key name	Exported key	Success/fail
Query Key Names	Query Key Names Command	None	Key meta data for all keys accessible by user	Success/fail
Download Certificate	Download Certificate Command	Certificate name	Certificate	Success/fail
Query Key Meta Data	Query Key Meta Data Command	Key name	Key meta data if accessible by user	Success/fail
Generate Random Bytes	Generate Random Bytes Command	Number of random bytes	Random bytes	Success/fail
Authenticate User	Authenticate User Command	Username/Password and/or Certificate	None	Success/fail
Key Management	Key Management Command	Key name Algorithm parameters Key permissions Key to be imported	Key Permissions Public Key	Success/fail
Update Firmware	Update Firmware Command	New image	None	Success/fail
Cluster Management	Cluster Management Command	Cluster keys Configuration file	Cluster keys Configuration file Cluster commands	Success/fail

Service	Control Input	Data Input	Data Output	Status Output
Certificate Management	Certificate Management Command	Certificate Name Common Name Key Size Certificate Duration	Certificate	Success/fail
Service Management	Service Management Command	Service name	None	Success/fail
Enable/Disable FIPS mode	Enable/Disable FIPS mode Command	Configuration settings	None	Success/fail
Operator Management	Operator Management Command	Operator password Operator permissions Operator name	Operator permissions	Success/fail
Reset Factory Settings	Reset Factory Settings Command	None	None	Success/fail
Restore Default Configuration	Restore Default Configuration Command	None	None	Success/fail
Restore Configuration File	Restore Configuration File Command	Configuration file	None	Success/fail
Backup Configuration File	Backup Configuration File Command	Configuration settings	Configuration file	Success/fail

Service	Control Input	Data Input	Data Output	Status Output
Migrate DB	Migrate DB Command	Database Table Name Column Name Encrypted Column or Plaintext Column	Encrypted Column or Decrypted Column	Success/fail
Authenticate Administrator	Authenticate Administrator command	Username/password	None	Success/fail
Receive Configuration File	Receive Configuration File Command	New configuration file	None	Success/fail
Zeroize Key(s)	Zeroize Key Command	Key name	None	Success/fail
Authenticate Cluster Member	Authenticate Cluster Member Command	Cluster certificate	None	Success/fail
Authenticate Ingrian User	Authenticate Ingrian User Command	Ingrian user certificate	None	Success/fail
Authenticate File Encryption User	Authenticate File Encryption User Command	File Encryption User certificate	None	Success/fail
Request/Export Encrypted Key and Metadata	Request/Export Encrypted Key and Metadata Command	Configuration request[3]	Encrypted Key and Metadata	Success/fail
Push Log Information	Push Log Information command	Log File	None	Success/fail

[3] Note that as the File Encryption User has already authenticated the only configuration that can be passed is the one associated with the authenticated user.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

Table 6 - Specification of Critical Security Parameters

Key	Description/Usage
AES Key	AES 128, 192, 256 key used to encrypt/decrypt input data.
TDES-EDE Key	TDES 168, 112 key used to encrypt/decrypt input data.
HMACSHA1 Key	HMAC key used to hash/verify input data.
RSA 2048 Key	Private part of a 2048 bit RSA key pair used for signing input data.
RSA 1024 Key	Private part of a 1024 bit RSA key pair used for signing input data.
TLS RSA Key 1024/2048	Private part of 1024/2048 bit RSA key pair used for TLS server authentication and key transport. These certificates are used for the Web Administration, User Cryptographic and Cluster services.
TLS session keys	128 or 256 bit AES or 168 bit TDES keys; HMAC SHA-1 key
CA RSA Key 1024/2048	The private part of the RSA key pair used for signing X509 CSR and/or CRL
CO Password	Used to authenticate COs.
User Password	Used to authenticate Users.
DSA key	160-bit DSA private key
SSHv2 Diffie-Hellman key	1024-bit Diffie-Hellman private key
SSH session keys	168-bit TDES keys, 128-bit AES keys, 192-bit AES keys, or 256-bit AES keys ; HMAC SHA-1 keys
SSH RSA key	1024-bit RSA private key

Definition of Public Keys:

The following are the public keys contained in the module:

Table 7 - Specification of Public Keys

Key	Description/Usage
RSA 1024 Public Key	Public part used for verifying signatures.
RSA 2048 Public Key	Public part used for verifying signatures.
TLS RSA Public Key 1024/2048	Public part of 1024/2048 bit RSA key pair used for TLS server authentication and key transport. These certs are used for the Web Administration, User Cryptographic and Cluster services.
CA RSA Public Key 1024/2048	The public part of the RSA key pair used for verifying signatures on X509 certificates.
Software Upgrade RSA Public key	1024 bit RSA public key used for verifying signatures on Software Upgrades.
SSH Diffie-Hellman Public Key	1024-bit public key
SSH DSA Public Key	1024-bit DSA public key
SSH RSA Public Key	1024-bit RSA public key
Ingrian User Verification Public Key	1024-bit RSA public key
CO Verification Public Key	Optional 1024-bit RSA public key
User Verification Public Key	Optional 1024-bit RSA public key
Cluster Member Public Key	1024-bit RSA public key
File Encryption User Public Key	1024-bit RSA public key

Definition of CSPs Modes of Access

Table 6 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

Table 8 – CSP Access Rights within Roles & Services

Authorized Role(s)	Service	Cryptographic Keys and CSPs Access Operation
User	Encrypt Data	Select AES or TDES-EDE Key
User	Decrypt Data	Select AES or TDES-EDE Key
User	Sign Data	Select RSA 1024 or 2048, or DSA 1024
User	Verify Data	Select RSA 1024 or 2048, or DSA 1024
User	MAC Verify Data	Select HMACSHA1
User	MAC Data	Select HMACSHA1
User	Export Key	Select any of the following keys: - AES or TDES-EDE - HMACSHA1 - RSA 2048 - RSA 1024 - CA RSA Key Pair 1024/2048 Wrap the above key with SSH session keys or TLS session keys.
User	Query Key Names	Select any of the keys in Table 6.
User	Download Certificate	Select any of the public keys in Table 7. Export public key.
User	Query Key Meta Data	Select any of the keys in Table 6.
User	Generate Random Bytes	None.
User	Authenticate User	Select User Password Generate TLS or SSH session

Authorized Role(s)	Service	Cryptographic Keys and CSPs Access Operation
		keys
Cryptographic Officer	Key Management	Select any of the keys in Table 6 an perform the following: - Generate selected key - Zeroize selected key
Cryptographic Officer	Update Firmware	Select CA RSA Public Key 1024/2048
Cryptographic Officer	Cluster Management	None
Cryptographic Officer	Certificate Management	Select RSA 1024 or 2048
Cryptographic Officer	Service Management	None.
Cryptographic Officer	Enable/Disable FIPS mode	None
Cryptographic Officer	Operator Management	None
Cryptographic Officer, Ingrian User	Reset Factory Settings	Zeroizes all secret and private keys.
Cryptographic Officer, Ingrian User	Restore Default Configuration	Zeroizes all secret and private keys.
Cryptographic Officer	Restore Configuration File	None
Cryptographic Officer, Cluster Member	Backup Configuration File	None
Cryptographic Officer	Migrate DB	Select AES or TDES-EDE Key Encrypt with selected key Decrypt with selected key
Cryptographic Officer	Authenticate Administrator	Generate TLS or SSH session keys Select CO Password
Cluster Member	Receive Configuration File	Select AES or TDES-EDE Key
Cryptographic Officer, Cluster Member, Ingrian User	Zeroize Key(s)	Zeroizes selected key
Cluster Member	Authenticate Cluster Member	Select TLS RSA Public Key 1024/2048

Authorized Role(s)	Service	Cryptographic Keys and CSPs Access Operation
Ingrian User	Authenticate Ingrian User	Ingrian User Verification Public Key
File Encryption User	Authenticate File Encryption User	File Encryption User Public Key
File Encryption User	Request/Export Encrypted Key and Metadata	AES key
File Encryption User	Push Log Information	None

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the device does not contain a modifiable operational environment.

8. Security Rules

The example cryptographic module's design corresponds to the example cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The cryptographic module shall provide five distinct operator roles. These are the User role, Ingrian User role, Cluster Member role, Cryptographic-Officer/Administrator role, and the File Encryption User role.
2. The cryptographic module shall provide identity-based authentication.
3. When the module has no valid roles logged in, the operator shall not have access to any cryptographic services.
4. The cryptographic module shall perform the following tests:

   A. Power up Self-Tests:

   1. Cryptographic algorithm tests:

      a. TDES Known Answer Test
      b. AES Known Answer Test
      c. DRNG Known Answer Test
      d. SHA-1 Known Answer Test
      e. HMAC-SHA-1 Known Answer Test
      f. RSA Sign/Verify Known Answer Test
      g. DSA Sign/Verify Known Answer Test
      h. Diffie-Hellman Known Answer Test

i. SSH Key Derivation Function Know Answer Test

2. Software/Firmware Integrity Test (CRC-16 and RSA signature verification)

B. Conditional Self-Tests:

1. Continuous Random Number Generator (RNG) test – performed on NDRNG and DRNG
2. DSA Pairwise Consistency Test
3. RSA Pairwise Consistency Test
4. Software/Firmware Load Test
5. Diffie-Hellman Primitive Test

5. At any time the cryptographic module is in an idle state, the operator shall be capable of commanding the module to perform the power-up self-test by power cycling the module.
6. Prior to each use, the internal RNG shall be tested using the conditional test specified in FIPS 140-2.
7. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
8. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. The module shall support concurrent operators.
10. The hot swappable hard drives in the i430 and i426 shall not be removed or replaced.

9. Physical Security Policy

Physical Security Mechanisms

The multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure with tamper evident seals (for all module configurations) and locks on the front bezel (for the i430 and i426 configurations).

Table 9 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seals and locks on the front bezel	6 months	Inspect the seals and or locks on the front bezel, and the seals on the removable doors

10. Mitigation of Other Attacks Policy

The FIPS 140-2 Area 11 Mitigation of Other Attacks requirements are not applicable because the DataSecure Appliance is not designed to mitigate any specific attacks outside the scope of FIPS 140-2.

11. References

National Institute of Standards and Technology (NIST), FIPS Pub 140-2, Security Requirements for Cryptographic Modules, May 25, 2001.

12. Definitions and Acronyms

AES – Advanced Encryption Standard

ANSI – American National Standards Institute

BIOS – Basic Input/Output System

CA – Certificate Authority

CBC – Cipher-Block Chaining

CLI – Command Line Interface

CO – Cryptographic Officer

CPU – Central Processing Unit

CRC – Cyclic Redundancy Check

CRL – Certificate Revocation List

CSP – Critical Security Parameter

CSR – Certificate Signing Request

DB – Database

DES – Data Encryption Standard

DRNG – Deterministic Random Number Generator

DSA – Digital Signature Algorithm

EDE – Encrypt-Decrypt-Encrypt

HMAC – Keyed-Hash Message Authentication Code

MD5 – Message Digest Algorithm 5

NAE – Network Attached Encryption

NDRNG – Non-Deterministic Random Number Generator

RAID – Redundant Array of Independent Drives

RAM – Random Access Memory

RC4 – Rivest Cipher 4

RSA – Rivest, Shamir, Adelman

SATA – Serial Advanced Technology Attachment

SHA – Secure Hash Algorithm

SNMP – Simple Network Management Protocol

SSH – Secure Shell

KDF – Key Derivation Function

D-H – Diffie-Hellman Protocol

SSL – Secure Sockets Layer

TDES – Triple-Data Encryption Standard

TLS – Transport Layer Security

VGA – Video Graphics Array

XML – Extensible Markup Language