Bodacion Technologies
A Virtual Media Company

HYDRA Server Cryptographic Module

Version 1.4

HYDRA

FIPS 140-1 Non-Proprietary
Security Policy
Level 1 Validation

June 2003

1. Introduction

1.1. Purpose

This is the non-proprietary FIPS 140-1 security policy for the Bodacion Technologies HYDRA Server 1.4 cryptographic module. This Security Policy details the secure operation of HYDRA Server as required in FIPS 140-1 as published by the National Institute of Standards and Technology (NIST) of the United States Department of Commerce.

1.2. References

For more information on HYDRA Server, see Bodacion Technologies' website at www.bodacion.com. The site features several white papers on the technology.

1.3. About This Document

This Security Policy document is one part of the complete FIPS 140-1 submission package. It outlines the functionality provided by the cryptographic module and gives high-level details on the means by which the module satisfies FIPS 140-1 requirements. With the exception of this non-proprietary Security Policy, the FIPS 140-1 Validation Submission Documentation is Bodacion-proprietary and may otherwise be government-controlled and releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Bodacion Technologies.

2. The Bodacion HYDRA Server Crypto Module

2.1. FIPS compliant mode

For the module to be used in FIPS compliant mode, the user must configure a browser to use TDES and SHA-1 for the Transport Layer Security (TLS) process. In non-FIPS mode a browser could use RC4, MD5, and Secure Session Layer (SSL).

2.2. Overview

The cryptographic module is the HYDRA Server 1.4. The HYDRA Server is a Hardware/Firmware (both version 1.4) module. It operates as a Secure Internet Server implemented in a single hardware board with a kernel that holds all of the Server's functionality, including cryptographic functionality. The kernel resides in Flash memory that is installed on the HYDRA Server's hardware. The server offers a web server service (HTTP and HTTPS), along with FTP and other services. The module contains SSL, TLS, and TDES, RC4, RSA, MD5 and SHA-1 algorithms. As described in Section 2.1, in FIPS compliant mode the HYDRA Server must use TDES and SHA-1 for HTTPS using TLS.

- **Physical Boundary**: The physical boundary of the module includes a single hardware board and all of the firmware included. The single board is a PowerPC based board that contains Flash memory that houses the HYDRA's firmware. The entire board and firmware is in the module. The cryptographic functions of the HYDRA form a library in the HYDRA's firmware. This library is completely internal to the firmware and not accessible from outside of the module. All cryptographic functions are contained in this library and included in the modules boundary.
- **FIPS-approved algorithms**: HYDRA Server supports the FIPS approved 3DES, and SHA-1. The HYDRA Server supports the non-FIPS approved RSA (under TLS protocol), RC4, MD5 and AES. HYDRA Server performs FIPS approved pseudo-random number generation for key generation when used in FIPS mode.

2.3. Module Interfaces

HYDRA Server combines hardware and firmware to provide web services in a secure environment. The crypto module utilizes only three interfaces—one of which is a LED interface for show-status, the others being an Ethernet interface and Serial interface. No external interface can be used to add to or subtract from HYDRA Server's kernel; no command line exists.

The crypto module within HYDRA Server coexists with the kernel and tasks (e.g. FTP, HTTP) that comprise a single-entity solution. No APIs are necessary; tasks share memory and are part of the kernel itself; therefore no internal programming interfaces are required. No general purpose Operating System or User Interface exists.

Data input, data output, and control input are accomplished via a standard Ethernet interface. Status output is accomplished via a standard LED interface (system status is shown via a flashing light on the front of the base board). Some initial configuration is allowed via a Serial Interface.

2.4. Roles and Services

HYDRA Server meets level-1 requirements for Roles and Services. The module supports a crypto-officer and users. The Crypto-Officer is authenticated with a password (role-based), but no FIPS approved user authentication is performed.

The Crypto-Officer is authenticated with the crypto module via a password. Once authenticated, the crypto-officer can assume his role. Crypto-officers can manage and configure the cryptographic module.

Users of the module are HTTPS clients (Web Browsers) and are identified by their respective IP-address as part of the Internet Protocol. Users start the initiation by obtaining a certificate/signature for the module that contains the modules public RSA key. A request to the module in encrypted form is made and a session is initiated. Users are not authenticated. Any web browsers capable of TLS can obtain the modules RSA certificate and can establish a session with the module. A Web page being served by the HYDRA server could potentially require authentication of users, however this is not required by the module and not performed by the module. Any web page authentication would be outside of the module boundary.

The following table outlines the authentication for each operator, the crypto-officer and user.

Role	Type of Authentication	Authentication Data
User	None	Not authenticated
Crypto-Officer	Role	Password

Table 1 - Authentication Data

The following table outlines the approved services to each operator.

Role	Authorized Services
User	Symmetric Key Encryption - TDES - RC4 Asymmetric Key Encryption - RSA Message Digest Algorithms - SHA-1 - MD5 Random Number Generation - FIPS 186-2, Appendix 3.3
Cryptographic Officer	Initialization of Cryptographic Module Administration of the module Module Status Self-test (power-on) Zeroization (power-off)

Table 2 – Authorized Services

An operator performing a service for either crypto-officer of user role, access the service through the use of the logical cryptographic API and physically through the Ethernet port.

Service	Cryptographic Keys/CSPs	Access
Symmetric Encryption/Decryption	Symmetric Key	Read/Write
Key Exchange	Asymmetric Key Pair	Read/Write
Hash Generation	None	N/A
Random Number Generation	Seed	N/A
Module Initialization	None	N/A
Administration of Module	C-O password	Read/Write
Module Status	None	N/A
Self-Test	None	N/A
Zeroization	Keys/CSP	Read/Write

Table 3 – Access Rights

2.5. Finite State Machine Model

The Bodacion HYDRA Sever Cryptographic Module v1.4 is designed around a finite state machine model (FSM) that conforms to FIPS 140-1 requirements.

2.6. Physical Security

The crypto module of HYDRA Server is part of the complete hardware/firmware solution for web service. It does not run on an operating system, but instead is part of a kernel/task system that is HYDRA Server's firmware.

The firmware portion of HYDRA Server is designed to run on a CompactPCI machine that utilizes a PowerPC CPU. The hardware meets FCC Class A EMI/EMC certification.

No keyboard, mouse, or video may be connected to HYDRA Server. Management is accomplished via browser into HYDRA Server's Ethernet port. Initial configuration is accomplished via HYDRA Server's serial port interface. While a USB port is included on the base board, it is non-functional. HYDRA Server has no floppy drive, and has no CD-ROM drive.

The server uses industry-standard, production-grade integrated circuits. It is encased in an opaque metal container.

2.7. Software Security

The firmware portion of HYDRA Server is written in C++ and assembly language. It is a kernel/task environment that embodies all functionalities of the product, including cryptography, FTP server, HTTP server, etc. Other than standard security functions such as 3DES, RSA, etc., the entire environment was developed by Bodacion Technologies.

The firmware portion of HYDRA Server cannot be accessed from the outside unless it is done via browser by an authenticated crypto-officer operator. There is no command prompt and no traditional file structure as in other firmware environments.

The firmware performs a health check when HYDRA Server is booted. The health check is based on known answer tests, covered in section 2.12.

2.8. Operating System Security

The HYDRA Server Cryptographic Module contains a firmware kernel that operates as a resource manager. No general-purpose operating system exists that allows for outside software/firmware to be installed or executed in the module.

2.9. Cryptographic Key Management

The module's cryptographic functionality is utilized in the HTTPS server in the module. To be operated in FIPS mode, a user must configure their web browser to use the TLS protocol. A user can then obtain secure (encrypted) HTTPS web pages from the module.

A user (web browser) that requests a page on the HYDRA's HTTPS Web Server through TLS first obtains the module's certificate. Using the certificate, the user makes a request to the module to start a session. Once the module has validated the request, a secret session TDES key is generated using the FIPS PRNG. The secret session key is then distributed using RSA under the TLS protocol. These secret session keys are then used for secure communication between the module and user. Upon termination of the session, the session key is destroyed by zeroization.

Before user session encryption services can be provided, the crypto-officer must generate the modules RSA public and private key. After choosing an option from a menu to request the certificate, the module generates the modules public and private key based on random data gathered by monitoring the crypto-officers actions and seeding it into the PRNG. A certificate is then created that contains the modules public key.

All keys used in the module are stored in AES encrypted (plaintext because AES is not FIPS approved) form.

2.10. Cryptographic Algorithms

HYDRA Server employs several methods to ensure security in the system. A biomorphic sequence generator based on the Raki series is used to generate streams of characters called bodacions. These bodacions are used to create session ids to manage session with users. In addition, the bodacion is the technology that drives the pseudo-random number generator inherent in HYDRA Server. The HYDRA PRNG is then used to seed an FIPS 186-2 PRNG for key generation.

In addition to the patent-pending bodacion technology, HYDRA Server employs FIPS-approved (and industry standard) cryptographic algorithms such as 3DES and SHA-1. The non-FIPS approved RSA (under TLS protocol), RC4 and MD5 are included as well. The module includes a non-FIPS approved implementation of AES for the storage of keys.

2.11. EMI/EMC

The HYDRA Server Cryptographic Module conforms to FCC Part 15, Subpart J, Class A requirements.

2.12. Self-Tests

HYDRA Server utilizes self-tests on startup to insure the health of the system and the cryptographic module. The module performs known-answer tests of the FIPS algorithms, a CRC for integrity of the module and a continuous random number test for the PRNG. The complete list of test is included below.

Power Up Self-Test

- TDES KAT
- SHA-1 KAT
- CRC Integrity Check

Conditional Test

- Continuous Random Number Test