|  |
| --- |
| Diamond Key Security, NFP  Copyright © 2018, 2019 Diamond Key Security, NFP |
| Security Features within the  Diamond-HSMTM |



Contents

[1. Overview 1](#_Toc955175)

[1.1. Definitions 1](#_Toc955176)

[1.2. Layers of Security 2](#_Toc955177)

[2. Physical Protection 3](#_Toc955178)

[2.1.1. Tamper Detecting Case 3](#_Toc955179)

[2.1.2. Sensor Cards 3](#_Toc955180)

[3. Logical Protection 3](#_Toc955181)

[3.1. Firewall 3](#_Toc955182)

[3.2. Single-board Computer 3](#_Toc955183)

[3.2.1. Logical Separation of components 3](#_Toc955184)

[3.2.2. Console Interface 4](#_Toc955185)

[3.2.3. Load Balancer 5](#_Toc955186)

[3.2.4. Passwords 5](#_Toc955187)

[4. Security Concerns and Mitigations for Specific Operations 5](#_Toc955188)

[4.1. HSM Upgrades 5](#_Toc955189)

[4.2. Key Backup 5](#_Toc955190)

1. Overview

This document outlines the built-in security features of the Diamond-HSMTM and shows how these features are used to protect the information stored in its internal CrypTech devices.

* 1. Definitions

BIND – Berkeley Internet Name Domain. BIND is open source software for publishing DNS information on the Internet, and to resolve DNS queries from users. The software originated in the early 1980s at the University of California at Berkeley.[[1]](#endnote-2)

CrypTech – CrypTech is a loose international collective of engineers trying to improve assurance and privacy on the Internet. [[2]](#endnote-3)

DNS – Domain Name System. DNS is a decentralized system for naming computers and other resources on the Internet. It maps domain names to numerical IP address which are used to identify computer services and devices on the Internet.[[3]](#endnote-4)

DNSSEC – Domain Name System Security Extensions. DNSSEC is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System as used on IP networks. It is an extension to DNS which provides DNS clients(resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality.[[4]](#endnote-5)

HSM – A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing[[5]](#endnote-6).

OpenDNSSEC – OpenDNSSEC is a policy-based zone signer that automates the process of keeping track of DNSSEC keys and the signing of zones.[[6]](#endnote-7)

PKCS 11 – Public-Key Cryptography Standards #11. The PKCS #11 standard defines a platform-independent API to cryptographic tokens, such as HSMs and smart cards.

* 1. Layers of Security

The Diamond-HSM’s approach to security is to assume that environment that the HSM has been placed in is not secure. To the Diamond-HSM, an internal private ethernet can be just as insecure as the Internet. To secure its data, the Diamond-HSM relies on layers of security. The following diagram shows the HSM’s key components.

A screenshot of a cell phone

Description automatically generated

Diagram 1.3 – Key HSM Components

Each layer has been designed to block unauthorized usage if the HSM.

1. Physical Protection

The sensor cards and tamper detecting case are used to protect the HSM from physical attacks.

* + - 1. Tamper Detecting Case

The case has switches to detect removal of the top plate and front panel which connect to the sensor cards. The case also provides power to all of the HSM’s internal components and uses a battery to power the sensors and to preserve the master key in the event of a power failure.

* + - 1. Sensor Cards

There is a sensor card attached to each CrypTech device. The sensor cards respond to a variety of events and will clear the master key if any of the events have been triggered. Tamper events include the following:

* Ambient light monitoring
* Temperature sensors
* Case open
* Motion

1. Logical Protection
   1. Firewall

The firewall is used to block all connections to the HSM except on three ports. The ports are as follows:

* Port 8080 – Management port. Provides a console interface for configuring the HSM.
* Port 8081 – Data port. This interface is used by PKCS #11.
* Port 80 – Web port. This is a simple web interface for checking the status of the HSM.

The firewall can be configured to allow all connections, a range of IP addresses, a list of IP address, and it can also be used to block all connections. Changes can be made per port and no other ports can be opened.

* 1. Single-board Computer

The single board computer has three parts for connecting to the outside computers. Each part corresponds to one of the HSM’s open ports. The single-board computer doesn’t allow any other communication outside of those ports. For example, a user cannot SSH into the single-board computer.

* + - 1. Logical Separation of components

Even though the three major components all reside on one single-board computer and share some data, the components can’t be used as an attack vector for another component. For instance, an attack on port 8081 can’t be used to gain access to the management port on a CrypTech device. This is because all parts have been logically separated as shown in the following diagram.

A screenshot of a cell phone

Description automatically generated

Diagram 2.3.1 – Key HSM Components

As shown in Diagram 2.3.1, the three main components are the load balancer, the consoler interface, and the web interface. The load balancer listens to connections on port 8081 and connects to only the DATA port on a CrypTech device. The console interface cannot directly communicate with the load balancer; however, there are background processes such as the key synchronizer that connects to the load balancer and can receive commands from the console interface.

* + - 1. Console Interface

The console interface doesn’t serve as a passthrough for the CTY interface on a CrypTech device. The Diamond-HSM has its own interface that it checks for errors and will require the user to reenter their password to perform certain operations. The Diamond-HSM’s interface will generate new CTY commands and forward those commands to the CrypTech devices.

* + - 1. Load Balancer

CrypTech devices accept remote procedure calls (RPCs) over its DATA port. The load balancer processes all RPCs before sending them to a CrypTech device. It can also be used to block certain operations. For example, the is a ‘pkey export’ procedure that the load balancer can be set up to block if that feature has been disabled.

* + - 1. Passwords

The CrypTech devices support three passwords: the ‘wheel’ password, the ‘so’ password, and the ‘user’ password. Only the ‘wheel’ password can be used to enter the console interface. The ‘user’ and ‘so’ passwords are used by PKCS#11. In future versions of the Diamond-HSM, the ‘wheel’ password can be restricted to only the console interface. Attempts to use it for the data interface will be banned. This will prevent attacks to gain the ‘wheel’ password from the ‘data’ interface.

1. Security Concerns and Mitigations for Specific Operations
   1. HSM Upgrades
   2. Key Backup

1. <https://www.isc.org/downloads/bind/> [↑](#endnote-ref-2)
2. <https://trac.cryptech.is/> [↑](#endnote-ref-3)
3. <https://en.wikipedia.org/wiki/Domain_Name_System> [↑](#endnote-ref-4)
4. <https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions> [↑](#endnote-ref-5)
5. <https://en.wikipedia.org/wiki/Hardware_security_module> [↑](#endnote-ref-6)
6. <https://www.opendnssec.org/> [↑](#endnote-ref-7)