yubico
the key to the cloud

Security Policy
FIPS 140-2 Level 1

Yubico YubiKey Standard and YubiKey Nano Hardware Version 1.6 / Firmware Version 2.5.1

Document Version 1.4

September 16, 2014

Introduction

Yubico is the leading provider of simple, open online identity protection. The company's flagship product, the YubiKey®, uniquely combines driverless USB hardware with open source software. More than a million users in 100 countries rely on YubiKey strong two-factor authentication for securing access to computers, mobile devices, networks and online services. Customers range from individual Internet users to e-governments and Fortune 500 companies. Founded in 2007, Yubico is privately held with offices in California, Sweden and UK.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. Yubico shall have no liability for any error or damages of any kind resulting from the use of this document.

The Yubico Software referenced in this document is licensed to you under the terms and conditions accompanying the software or as otherwise agreed between you or the company that you are representing.

Trademarks

Yubico and YubiKey are trademarks of Yubico Inc.

Notices

This document may be freely reproduced and distributed in its entirety without modification.

Contact Information

Yubico Inc
228 Hamilton Avenue, 3rd Floor
Palo Alto, CA 94301
USA
info@yubico.com

Table of Contents

1 Introduction

1.1 Scope

This document describes the cryptographic module security policy for the Yubico YubiKey Standard and YubiKey Nano USB token with firmware 2.5.1 (also referred to as the “module” hereafter). It contains specification of the security rules, under which the cryptographic module operates, including the security rules derived from the requirements of the FIPS 140-2 standard.

1.2 Overview

The cryptographic module is a USB 1.1/2.0 compliant OTP (One Time Password) token where the OTP output comes as typed string of characters through keyboard emulation. The chip based platform runs the Yubico OTP Operating System which manages all low level resources, cryptographic algorithms, access control and the life cycle of all keys.

1.3 Glossary

Term	Description
OTP	One Time Password
OATH	OTP based on the Initiative for Open Authentication industry standard

Table 1 - Glossary

2 Security Levels

The following table lists the level of validation for each area in FIPS 140-2:

Security Requirements	Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)	1
Self-Tests	1
Design Assurance	2
Mitigation of Other Attacks	N/A

Table 2 - FIPS 140-2 Security Requirement Levels

3 Cryptographic Module Specification

3.1 Cryptographic Boundary

The cryptographic boundary for is the physical boundary of the USB device. The USB device is a standalone cryptographic module designed as a single monolithic entity to provide tamper evidence and prevention.

The physical boundary is depicted below:

Figure 1 – Yubikey Standard

Figure 2 – Yubikey Nano

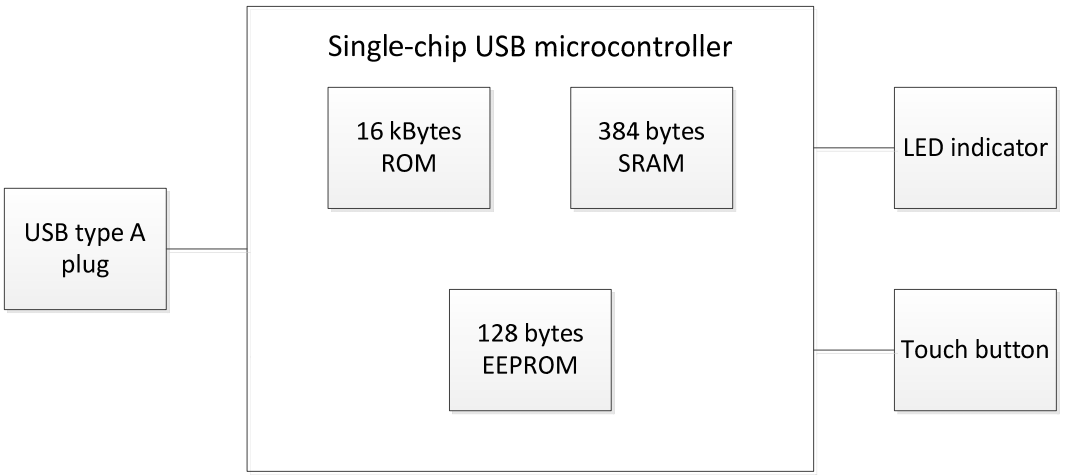

Figure 3 - Cryptographic Boundary

The embedded chip contains the following hardware components:

- USB controller
- General purpose Microcontroller for operations
- Low-speed (1.5 Mbps) USB 1.1 type A plug
- Non-volatile (EEPROM) memory embedded on-chip for storing configurations and non-volatile counter values
- ROM storage for firmware and RAM for operations
- LED indicator light
- Capacitive touch button

3.2 Fabrication

The device is completely monolithic and sealed using an innovative injection molding process. The USB microcontroller is chip-on-board mounted and embedded into epoxy resin. The device PCB is then injection molded using a glass-fiber reinforced thermoplastic. All supporting components, such as resistors and capacitors are contained within the resin except for the LED component for light indication and the capacitive touch button leads and the USB connector contacts.

4 Cryptographic Module Ports and Interfaces

4.1 Physical Interfaces

4.1.1 USB Interface

Four electrical connections are made between the microcontroller and the USB connector:

- VSS, Ground (reference voltage).
- VDD, Power supply voltage input.
- DP, USB D+ connection.
- DM, USB D- connection.

The above four electronic signals are in full compliance with the USB interface specification. Communications between the host applications and the device is accomplished using an HID device (keyboard) driver that converts back and forth between USB and commands from the microcontroller.

4.1.2 Capacitive Touch Button

A capacitive touch button is located on the top of the module. This button detects physical contact as a means to trigger a specified action within the microcontroller.

4.1.3 LED Indicator Light

Surrounding the capacitive touch button is an LED light. This light is used to indicate the current state of the module to the user visually.

4.2 Logical Interfaces

The module provides a logical interface via an API. There is only one API, exposed during the configuration of the module. The API provided by the module is mapped to the FIPS 140-2 logical interfaces: data input, data output, control input, and status output. All of these physical interfaces are separated into the logical interfaces from FIPS as described in the following table:

FIPS 140-2 Logical Interface	Module Mapping
Data Input Interface	Parameters passed to the module via API calls
Data Output Interface	Depending on operating mode data is returned from the module by means of standard keyboard entry codes (scan codes) sent to the host operating system/application or through API calls
Control Input Interface	Control input passed to the module via API calls
Status Output Interface	Information returned to the user via the status LED
Power Interface	Does not provide a separate power or maintenance access interface beyond the power interface provided by the computer itself

Table 3 - Logical Interfaces

5 Roles, Services and Authentication

5.1 Roles

The module does not provide any identification or authentication for any user that is accessing the device. The module provides a Crypto Officer and a User role (there is no Maintenance role). Since the device does not provide any identification or authentication services, the level of access granted to any functionality of the module is implicitly determined by the service calling the module; the device itself makes no determination about the role itself. The Crypto Officer is expected to configure the device by loading the keys.

The module supports two independent roles: the Crypto Officer and the User.

Service/Algorithm	User	Crypto Officer
AES	X	
HMAC-SHA1	X	
Key zeroization		X
Key Loading		X
Show Status	X	
Self-Test	X	

Table 4 - Roles & Services

5.1.1 Crypto Officer Role

The Crypto Officer Role is only used during the configuration of the module to set the AES and HMAC-SHA1 keys. The loading of these keys can only be done using the YubiKey Configuration Utility. This utility is run from a Microsoft Windows system such as Windows 7, and provides the ability to load/provision keys into one or many modules, and by extension, the implicit assumption of the Crypto Officer Role. The utility can also be used to zeroize existing keys and load new keys into the token, but it is not possible to export an existing configuration. Loading of new Keys overwrites the exact position of the old keys for effective key zeroization.

The Crypto Officer ensures that the module is configured and locked with a configuration access code. In this mode it is not possible for a user to add, change or in any way update the configuration of the device.

The Crypto Officer can maintain the module via a host-based application. The Crypto Officer cannot export the configuration currently stored in a key, but can only overwrite it with a new configuration after authenticating to the key using the configuration password.

5.1.2 User Role

The User Role is the main operating role of the module. The module is designed as the second factor for authentication with only a single button for activating its functionality, not as a complete two-factor authentication device. As such, it does not require the User Role to authenticate to the module itself when using the token.

The applications using a module as a second authentication factor are expected to utilize extra input from the user directly into the application authentication dialog in addition to the OTP generated by the module as a function of the User Role. An individual module (and hence it's User Role) is tied to the user account by the unique identifier embedded into the firmware and output as part of the OTP string.

As long as the token remains connected and powered on, the User Role is active. This does not mean that the User Role remains indefinitely logged into an application. Normally an application will timeout without activity or the user will close the session, requiring the user to activate the OTP function of the module again to access the application.

The User Role has access to the AES and HMAC-SHA1 services for the purpose of generating OTP strings.

Depending on the module configuration set up by the Crypto Officer Role, the User Role has access to one or two module OTP configurations. Each OTP is isolated and separate, and in addition to containing unique identifiers for each configuration, they can be configured to utilize different OTP generation methods.

With only a single button available on the module, the selection of which OTP is presented by the User Role is determined by the length of time the button is pressed. A touch of less than 3 seconds will always generate an OTP string from the first slot, while a 4 to 6 second touch will generate an OTP string from the second slot, if that slot has been configured. If only one slot is configured, it is always the first slot and any touch will generate an OTP from that slot.

The User Role does not have the ability to load, change or export keys to the module.

6 Physical Security

The module is a single-chip standalone cryptographic module made with production grade components and standard passivation.

7 Operational Environment

This set of requirements is not applicable as the microcontroller firmware cannot be upgraded once the token has left production. The module does not provide a general purpose operating system.

8 Cryptographic Key Management & Algorithms

8.1 Cryptographic Algorithms

The module implements the following algorithms in the firmware:

Algorithm	FIPS Approved	Cert Number
AES	Yes	2811
HMAC-SHA1	Yes	1762
SHA-1	Yes	2359

Table 5 - Algorithms & Certifications

.

8.2 Cryptographic Key Management

Keys are not generated in the module, but are loaded during initialization and cannot be changed without zeroizing any keys already loaded into the token. These keys are stored in the module in plain text but cannot be read or exported outside of the token once they have been entered by the Crypto Officer. Only a single set of keys can be loaded in the token for each configuration slot at one time.

The following list of keys and CSPs is used by the module. They are generated or inserted as specified and stored within the module as necessary.

Name	Created	Size in bits	Purpose
AES key	Inserted	128	Generate OTP
HMAC-SHA1 key	Inserted	112	Challenge-Response
Firmware integrity 16bit LRC	Hardcoded	16	Verify firmware integrity

Table 6 - Key Management

Keys are stored in the token's internal data structures, which are not exposed to external access. Keys cannot be explicitly deleted, but when a new configuration is loaded, existing keys are zeroized by being exactly overwritten byte-by-byte by the new key. The Integrity check key is hard coded to the firmware and since the firmware is not upgradable, it is not possible to change this key.

The module implements the following access control policy on keys and CSPs in the module shown in the following table. The Access Policy is noted by R=Read, W=Write and X=Execute.

Services	CSP Access	Rights
AES	AES key	RX
HMAC-SHA1	HMAC-SHA1 key	RX
Integrity Test (16bit LRC)	Yes	RX
RNG	Outside of Module	N/A
Zeroization	AES key, HMAC-SHA1 key	RW
Show Status	None	RX
Self-Test	AES key, HMAC-SHA1 key	RX

Table 7 - Key Services

9 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The module conforms to the EMI/EMC requirements specified in FCC 47 CFR Part 15. In addition it also conforms to CE 89/336/EEC requirements. The module token is a single chip standalone module and is a passive device. The USB host subsystem shall supply operating power and is activated either by a user pressing the button or by API call (if configured to allow API call).

10 Self-Tests

The module runs several self-tests to validate the integrity of the algorithms that are available in the module firmware. In addition to the algorithm self-tests, a firmware integrity test is also run when the token starts to ensure no damage or tampering has occurred.

The random number generator also performs continuous tests each time it is used to generate random data.

If any of the tests fails, the user is alerted via the LED surrounding the capacitive button and the module enters an error state where no functions are allowed to be executed. This state can be reset by removing the module from the USB port and reinserting it to restart the token.

Algorithm	Known Answer Tests
AES	X
HMAC-SHA1	X
Integrity Test (16bit LRC)	X

Table 8 - Algorithm Self-Tests

11 Design Assurance

Yubico uses industry standard tools to design and maintain the eco-system surrounding the module. This includes the design documents for the key hardware, the firmware, server software (not included in this validation), test plans and all user/administrator documentation. Version control is enforced on all documents related to the design and use of the module as is strict access control lists to ensure proper access to those documents.

12 Crypto Offer and User Guidance

The module does not have a non-FIPS mode. The configuration is FIPS-mode As such, no Crypto Offer or User Guidance is required to install or initialize the module in FIPS mode of operation.