Sentry ONE CSPN Security Target

1. Product identification

Publishing organization	DataLocker Inc.
Link to the organization	www.datalocker.com
Trade name of the product	Sentry ONE
Article (SKU)	SONEXXX
Version number evaluated	Device software 6.3, chipset firmware 3.05
Category of product	Secure storage

2. Description of product

2A.General description

The main use of the secure USB flash drive Sentry ONE is to automatically hardware encrypt and mandatory password protect any stored user data on the USB storage device to allow storage and/or transport.

Concerning the product reference (SONEXXX), XXX denotes storage capacity option.

As a matter of further user assurance the product is certified to FIPS 140-2 level 3, see the Security Policy #2753 for details.[1]

[1] https://csrc.nist.rip/groups/STM/cmvp/documents/140-1/140sp/140sp2753.pdf

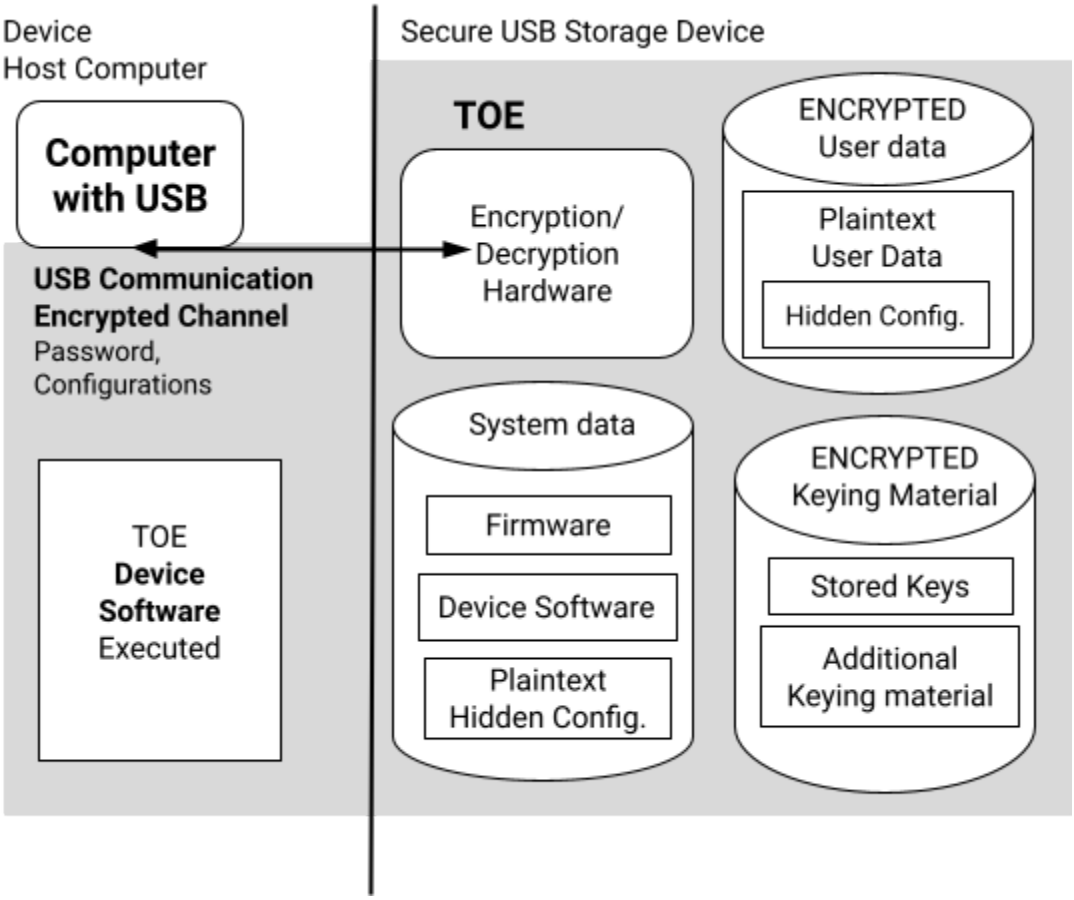

Figure 1. Description scheme of the TOE, marked in gray.

2B.How to use the product

The product is plugged into an available powered USB (1.1/2/3/3.1) port whereby it powers up and presents to the device host computer (Windows 7/8/10 / Mac OS) as a virtual DVD-RW and unmounted storage partition.

Upon the initial setup cycle the device software requires a device hardware password to be configured. The password is entered, confirmed and checked by the device software to adhere to the default password policy.

On the consecutive use, after the initial setup cycle of the password, the device user will launch the device software off the virtual DVD-RW and enter their set password. The password is then sent over an encrypted channel to the embedded system on the actual secure USB storage device where it is then evaluated and any password attempts are counted towards a tamper-proof brute force counter.

Upon entering the correct password the secure storage partition will mount and this partition will function like a flat storage partition and support read, write and delete from any device host computer software. All user data that is stored on the product passes through the embedded system where it is hardware encrypted with 256-bit AES XTS mode encryption utilizing a data encryption key that is safeguarded on the product by the user password.

When the product is locked through the device host computer executed device software or when it is unplugged (powered down) the product automatically locks and a new usage cycle can take place, requiring the correct password to be entered on each following cycle.

2C.Intended product environment

The product is used to store and transport data securely and is accessed using a computer.

The device has no restrictions on the intended product environment, it can be used anywhere that the technical environment criteria is met.

The device is, as most USB flash drives, small and portable and could be misplaced and/or stolen in the intended product environment. The security functions of the product are aimed at protecting the stored data from disclosure.

2D.Operating environment and general assumptions

OE.TRUSTED_CLIENT_HOST

The device host computer is trusted, meaning that it has an updated operating system and has an updated anti-malware software to protect the correct operation of the device software and does not exhibit generally suspicious behaviour.

Notice: once the secure USB storage device is unlocked with the user password the device host computer has plaintext access to the users stored protected data. Therefore the user needs to exercise reasonable judgement where the secure USB storage device is unlocked.

GA.USER_GUIDANCE

Users will be instructed to not disclose the device password.

GA.INTACT Lost device and user self test

If a secure USB storage device has been lost or unattended and there is a warranted supspicion it should be verified.

Note that the product performs a security function in the form of a self test on power up and enters an irreversible mute state if this fails.

The secure USB storage device shall be discarded if it may be suspected that an attacker has tampered with the device or if any step of the user self test fails. The user self test should be performed in the order listed.

1. Verify the secure USB storage device visually, that it doesn't have marks or new scratches that might indicate tampering.
2. Verify that the secure USB storage device is physically intact by slightly twisting it.
3. The secure USB storage device weighs about 30 gram/ounces.
4. Verify when plugged into a computer that the blue indicator light on the secure USB storage device blinks (the correct frequency is 3 times per second during the unlock and during read/write operations).
5. Verify that the secure USB storage device is showing as a DVD-RW and a storage partition (only mounted when the secure USB storage device is unlocked)
6. Verify that the device software (to be executed) on the virtual DVD-RW is issued by DataLocker Inc before executing it.
7. Verify that the correct device software (to be executed on the host) and firmware is still present on the secure USB storage device by verifying the version under About in the user interface.

GA.VENDOR_SECRETS Signing certificates

The private keys and passwords held by the vendor that are required to sign and update secure USB storage device controller firmware and device software and device software updates are kept safe and are properly protected from disclosure.

2E. Dependencies not included with the product

A computer, with one available, sufficiently powered USB Type A port (1.1/2/3/3.1).

2F. Typical product users and roles

The organizational and personnel employment context for the product is as follows:

- One user per item of the secure USB storage device that stores their user data on the product.

3.Technical environment

The system requirements are Windows® 10, 8.1, 8, 7 (SP1), Mac OS X v.10.9.x -10.13.x, Linux v2.6+ , Citrix Ready (XenApp, XenDesktop compatible).

No installations are required on the device host computer for the secure USB storage device to operate.

Note that a record must be added to the device host computer registry for the secure USB storage device to properly mount and operate (sometimes referred to as enumeration). The registry record identifies the secure USB storage device with vendor name, product name, serial number and other general descriptors, these will remain on the device host computer after usage is completed - this is a mandatory behaviour enforced by the operating system for all USB connected devices.

4.Assets

The sensitive assets of the TOE that require all or any protections of the products security functions in regards to confidentiality, integrity, availability, and authenticity are as follows.

4A.Primary assets

A1.PLAINTXT Plaintext user data

The plaintext user data is the primary asset. For clarification, the data is stored encrypted and is decrypted on-the-fly when passing through the controller on its way to the device host computer process upon correct authorization with the user password.

Requires: Confidentiality and integrity.

```
Security functions protecting the asset
SF_HWENC Hardware encryption
SF_PASSWORD Password policy enforcement
```

4B.Secondary assets

A2.PWD User password

The user password must be remembered and must be protected by the user and the device host computer unto which the secure USB storage device connects. Upon authorization of the password, the secure USB storage device mounts the secure storage partition with the user data that is then available to the device host computer for read and/or write operations.

Requires: Availability. Integrity and confidentiality

```
Security functions protecting the asset
SF_PASSWORD Password policy enforcement
```

A2.SYSTEM System data

The system data on the USB storage device which includes controller firmware and device software.
The controller firmware is closed source and requires authentication embedded within the firmware image to be updated. The firmware requires confidentiality and authenticity.

The device software that is also closed source is able to configure policies of the device and communicate the password to the with the controller firmware. The device software requires integrity.

Requires: Integrity, confidentiality, and authenticity.

```
Security functions protecting the asset
SF_SYSTEM System data on device
SF_PHYSICAL Physical Security
SF_SELF Security self tests
```

A2.HW Hardware cryptography components

The USB storage device enforces hardware encryption of the stored plaintext data and the components of this cryptography are critical for the security of the device.

Component	Description / Use
AES Session Key (secure channel)	AES-256 key used to encrypt secure channel data between host application and module
MAC Key (secure channel)	HMAC-SHA-256 key used to authenticate messages sent via secure channel between host application and module.
Data Encryption Key	XTS-AES 256-bit key for encryption / decryption of all files on the drive
DEK Encryption Key	256-bit AES key for obfuscating the Data Encryption Key
DRBG Entropy Input	HWRNG providing 512- bit entropy to seed DRBG
DRBG Nonce	HWRNG providing 512- bit Nonce to seed the DRBG
DRBG V Value	Secret value of the internal state
DRBG Key Value	Secret value of the internal state

Requires: Confidentiality, Integrity

```
Security functions protecting the asset
SF_SELF Security self tests
SF_HWENC Hardware encryption
```

5. Threats

The different threatening agents are:

- internal attackers: any user on device host computers in the protected network;
- external attackers: anyone outside the organization.

T.UNAUTHORISED_USER_DATA_ACCESS

The primary threat to be addressed is the unauthorized disclosure of user data stored on a secure USB storage device.

Attackers may attempt to use the logical interface to access plaintext data or may connect the secure USB storage device to a host that provides raw access to the device content (e.g. to specified disk sectors or blocks).

Attackers may gain physical access to the secure USB storage device, and thus try to bypass the logical interface to obtain access to user data (perhaps by making physical modifications to the device to access its memory via their own physical connections, or the attacker might use equipment appropriate for the attack potential to read the contents of memory locations from their physical state).

Attackers may try to access user data that remains unprotected due to a failure that interrupts the correct operation of the secure USB storage device.

Attackers may try to look for unencrypted keying material giving them unauthorized access to user data.

```
Security functions countering the threat
SF_HWENC Hardware encryption
SF_PASSWORD Password policy enforcement
SF_PHYSICAL Physical Security
SF_SYSTEM System data on device
```

T.UNAUTHORISED_SYSTEM_DATA_MODIFICATION

Attackers may try to modify system data stored on a secure USB storage device. Attackers may attempt to use the logical interface to modify system data or may connect the device to a device host computer that provides raw access to the device content (e.g. to specified disk sectors or blocks).

Note that since system data may include software that runs on the device host computer, the threat of unauthorized modification of this software could also make the secure USB storage device a delivery mechanism for malicious intents.

```
Security functions countering the threat
SF_SYSTEM System data on device
SF_PHYSICAL Physical security
```

```
SF_SELF Security self tests
```

T.KEYING_MATERIAL_COMPROMISE

Possession of any of the keys, authorization data, random numbers or any other values that contribute to the creation of keys or authorization data could allow an attacker to defeat the encryption. As part of a conservative approach to security, gaining access to keying material is considered to be of equal importance to gaining access to plaintext user data or system data itself.

Alternatively, an attacker might try to determine a key because of insufficient entropy used in its generation.

```
Security functions countering the threat
SF_HWENC Hardware encryption
```

T.AUTHORISATION_GUESSING

Attackers may try to mount an exhaustive search (brute force) attack against the secure USB storage device to determine authorization factors to gain unauthorized access to the user data stored on the device.

```
Security functions countering the threat
SF_PASSWORD Password policy enforcement
```

6. Security functions

6A.Overview

DataLocker's Sentry ONE USB Flash Drive is for organizations that require a secure way to store and transfer portable data.

- The stored data is secured by hardware-based 256-bit AES encryption to guard sensitive information in case the drive is lost or stolen.
  ```
  SF_HWENC Hardware encryption
  SF_SYSTEM System data on device
  SF_SELF Security self tests
  ```

- Its strong password rules and lock-down control protect against brute force attacks.
  ```
  SF_PASSWORD Password policy enforcement
  SF_SYSTEM System data on device
  ```

- Its durable, metal cladded casing provides added protection to the epoxy potted interior which makes the secure USB storage device tamper-evident and tamper-resistant.
  `SF_PHYSICAL Physical security`

Such advanced security functions make the Sentry ONE USB Flash Drive ideal for organizations that require employees to transport and store confidential and sensitive computer files.

6B.Security functions being assessed

The security functions included in the scope of the evaluation are as follows:

SF_HWENC Hardware encryption

The secure USB storage device hardware encrypts the user plaintext data, with a DEK derived from the user password and with supporting keys that are internally generated, and decrypts the ciphertext upon the user password authorization via a secure channel over USB.

If the brute-force counter limit is reached OR if a reset is initiated either by the user in the device software all cryptographic keys will be destroyed . This will mean that any remaining stored ciphertext on the hardware device can be regarded as erased as it is unrecoverable without the key that no longer exists.

```
Asset protected A1.PLAINTXT Plaintext user data,  A2.HW Hardware cryptography
components in terms of confidentiality and integrity.
Threat countered T.KEYING_MATERIAL_COMPROMISE,T.UNAUTHORISED_USER_DATA_ACCESS
```

SF_PASSWORD Password policy enforcement

1. User data is automatically protected by the secure USB storage device once the user has been authorized. Before authorization, no user data can be written to the secure USB storage device.
2. The secure USB storage device requires that a valid passphrase is supplied before starting a session that allows any access to user data.
3. The secure USB storage device enforces a long ≥ 8 character password policy.
4. A faulty password attempt increases the brute force counter in the controller of the secure USB storage device. The amount of attempts are limited to the brute-force counter limit, the limit is a closed configuration and cannot be updated after factory production.
5. The product authorizes the user under the following conditions:
    a. connection of the secure USB storage device to a device host computer.
    b. recovery of a device host computer from a power-down or sleep state while the secure USB storage device is connected to it
    c. recovery of the secure USB storage device from its own power-down state.
    d. changing the value of authorization data of the secure USB storage device.
6. The secure USB storage device allows device host computer-initiated termination of the current session.

```
Asset protected A2.PWD User password and A1.PLAINTXT Plaintext user data in
terms of integrity and confidentiality.
Threat countered T.UNAUTHORISED_USER_DATA_ACCESS,T.AUTHORISATION_GUESSING
```

SF_PHYSICAL Physical security

With the purpose to physically protect the assets the device is composed of production-grade components and is completely covered with a hard, opaque potting material making it tamper evident and tamper resistant. Any attempts to remove the potting at ambient temperatures will result in permanent damage to the device. Compromise of just the exterior metallic casing does not compromise the security of the secure USB storage device.

```
Asset protected A2.SYSTEM System data and A2.HW Hardware cryptography
components in terms of integrity.
Threat countered T.UNAUTHORISED_SYSTEM_DATA_MODIFICATION
```

SF_SYSTEM System data on device

System data (i.e. device software and controller firmware), is authenticated by signature, and protected by the secure USB storage device to ensure that only authorized changes can be made to it from the device host computer.

```
Asset protected A2.SYSTEM System data for authenticity
Threat countered T.UNAUTHORISED_SYSTEM_DATA_MODIFICATION,
```

SF_SELF Security self tests

Power-On Self-Tests

Power-on self-tests are run upon every initialization of the device and if any of the tests fail, the device will not initialize. The device will enter an error state and no services can be accessed by the users. The device implements the following power-on self-tests:

1. SHA-256 KAT
2. HMAC-SHA-256 KAT
3. RSA-2048/SHA-256 Signature Verification KAT
4. AES-256 ECB Encrypt and Decrypt KATs
5. AES-256 CBC Encrypt and Decrypt KATs
6. AES-256 XTS Encrypt and Decrypt KATs
7. HMAC-SHA-256 DRBG KAT
8. RSA-2048/SHA-256 Signature Verification for Firmware Integrity Check

The device performs all power-on self-tests automatically when the module is initialized. All power-on self-tests must be passed before a user can perform services. The Power-on self-tests can be run on demand by rebooting the device.
A user can discern that all power-on self-tests have passed via normal operation of the module, presentation of the GUI interface, and observing the LED blinking slowly at 3.125 hertz during initialization and read/write activity to the module.

If the device fails a POST, the device will not be connected to the host system and the USB D+/D- pins will be isolated. In this case, the device will not be initialized and no critical security parameters will be available. The LED will blink rapidly at 16 hertz.

Conditional Self-Tests

Conditional self-tests are tests that run continuously during operation of the device. If any of these tests fail, the device will enter an error state. The device can be re-initialized to clear the error and resume operation. No services can be accessed by the operators. The device performs the following conditional self-tests:

1. Continuous RNG test run on output of DRBG
    a. Because there is 16-byte random number output after calling RNG each time, there are two calls to generate the AES 256 key. The test is run with each call.
2. Continuous test on output of DRBG seed mechanism (HW RNG)
3. Firmware Load Test (RSA-2048 Signature Verification)

If the device fails a conditional self-test, the device will not be connected to the host system and the USB D+/D- pins will be isolated.

```
Asset A2.SYSTEM System data, A2.HW Hardware Cryptography Components
protected for integrity.
Threat countered T.UNAUTHORISED_SYSTEM_DATA_MODIFICATION,
```

7. Security Target Matrix

	Assets			
	A1.PLAINTXT	A2.PWD	A2.SYSTEM	A2.HW
Requirements				
Availability (AVAI.)		AVAI.		
Confidentiality (CONF.)	CONF.	CONF.	CONF.	CONF.
Integrity (INTE.)	INTE.	INTE.	INTE.	INTE.
Authenticity (AUTH.)			AUTH.	
Threats				
T.UNAUTHORISED_USER_DATA_ACCESS	X			
T.UNAUTHORISED_SYSTEM_DATA_MODIFICATION			X	X
T.KEYING_MATERIAL_COMPROMISE	X	X		X
T.AUTHORISATION_GUESSING		X		
Security Function				
SF_HWENC	CONF., INTE.			CONF., INTE.
SF_PASSWORD	CONF., INTE.	CONF., INTE.		
SF_PHYSICAL			INTE.	
SF_SYSTEM			AUTH.	
SF_SELF			INTE.	INTE.

8. Acronym list

TOE	Target of Evaluation
USB	Universal Serial Bus interface, computer port
SKU	Stock Keeping Unit, commonly used in commerce to keep track of articles.
FIPS 140-2	The Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules.

9. Document version

Note	Author	Date	Version
Initial version	Anders Kjellander	7 JUL 2019	1.0
Combining and renaming SF, added and updated GA, restructured assets. Acronym list added. Technical environment clarified.	Anders Kjellander	11 JUL 2019	1.1
Updated general description. Terminology clarified. Updated description scheme.	Anders Kjellander	17 JUL 2019	1.2
Minor language corrections	Anders Kjellander	9 SEP 2019	1.3
Minor update to schematic	Anders Kjellander	15 OCT 2019	1.4
Changes implemented	Anders Kjellander	23 JAN 2020	1.5
Changes implemented	Anders Kjellander	21 MAY 2021	1.6