FIPS 140-2 Non-Proprietary Security Policy

NRevenector 2018

Document Version 1.0

Hardware P/N: 58.0036.0301.00 or 58.0036.0302.00

Firmware Version:

Bootloader: *90.0036.0401.00/**2019141001***

FP InovoLabs GmbH
Prenzlauer Promenade 28
13089 Berlin
Germany

fp-francotyp.com

Contents

Figures

Tables

1 Introduction

1.1 Overview

Figure: 1 *NRevenector 2018*

FP InovoLabs GmbH is a wholly-owned subsidiary of Francotyp-Postalia Holding AG (FP), one of the leading global suppliers of mail center solutions and increasingly a provider of Industrial IoT (IIoT) solutions. A major component of FP's business is the production and support of equipment incorporating a hardware security module (HSM) that securely connects to network infrastructures.

The HSM performs cryptographic functions and physically protects both Critical Security Parameters (CSPs) and Application Relevant Data Items (ARDIs) from unauthorized access and substitution. The NRevenector 2018 provides strong protection for running and updating application-specific firmware inside the HSM.

This document forms a Cryptographic Module Security Policy for the cryptographic module of the device under the terms of the NIST FIPS 140-2 validation. This Security Policy specifies the security rules under which this device operates.

1.2 Purpose of Module

The main purpose of the Cryptographic Module is the running of the Start Firmware service. The selected firmware is authenticated and prepared for secure execution. To do this, the device must be in an authenticated role. Once the firmware has been loaded, control is passed to it.

1.3 Implementation

The *NRevenector 2018* is a multiple-chip embedded cryptographic module, based around a cryptographic integrated circuit, together with a small number of support components. The components, mounted on a PCB, are covered by hard opaque potting material. The extent of the potting forms the cryptographic boundary of the module. The module has a proprietary electrical connector forming the interface to it. The module does not contain a modifiable operational environment.

2 Cryptographic Module Specification

2.1 FIPS Security Level Compliance

The cryptographic module is designed to meet FIPS 140-2 as shown in the table below:

Overall Module Security Level		**3**
Section	**Security Requirement**	**Level**
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	3
3	Roles, Services and Authentication	3
4	Finite State Model	3
5	Physical Security	3 + EFP
6	Operational Environment	N/A
7	Cryptographic Key Management	3
8	Electromagnetic Interference/ Electromagnetic Compatibility (EMI/EMC)	3
9	Self-Tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	3

Table 1: FIPS 140-2 Security Levels

3 Cryptographic Ports and Interfaces

The cryptographic module ports and interfaces are as indicated in Table 2.

External Port	Interface Type	Description
36-pin Serial IO card edge connector	Data input Data output Control input Status output Power input	Interface for communicating with module
USB Port (disabled for version 58.0036.0302.00)	Data input Data output Control input Status output Power input	Alternate interface for communicating with module
Status LEDs (ERR, BL, PWR, APP)	Status output	• ERR: error • BL: Bootloader running • PWR: internal power supply on • APP: Application running
Battery	Power input	Additional power supply for module.

Table 2: Cryptographic Ports & Interfaces

3.1 Cryptographic boundary

The cryptographic boundary is defined to be the outer edge of the epoxy that covers most of the printed circuit board, as shown below.

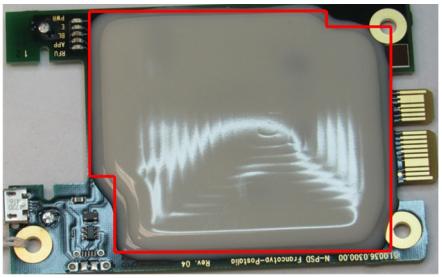

Figure: 2 Module Boundary (Outer Edge of Epoxy)

There are a small number of components on the printed circuit board that lie outside the cryptographic boundary, which may or may not be present depending on the build version of the device. These components have no impact on security-related aspects of the module.

4 Rules of Operation

The *NRevenector 2018* shall:

1. Support only an Approved mode of operation. The Approved mode indicator is returned via the Get Device Status service.
2. Not allow unauthenticated operators to have any access to the module's cryptographic services.
3. Inhibit data output during self-tests and error states.
4. Logically disconnect data output from the processes performing zeroization and key generation.
5. Enforce identity-based authentication.
6. Not retain the authentication of an operator following power-off or reboot.
7. Support the following roles: Default User and Cryptographic Officer/User.
8. Not permit the output of plaintext cryptographic keys or other CSPs.
9. Not support a bypass mode or maintenance mode.
10. Perform the self-tests as described in section 9 of this document.
11. Support the following logically distinct interfaces:
    - Data input interface
    - Data output interface
    - Control input interface
    - Status output interface
    - Power interface.
12. Support a FIPS approved deterministic random bit generator (DRBG) as specified in NIST SP 800-90a section 10.2.1
13. Store an error indication whenever an error state is entered. As a result the error indication can be read by the Get Device Status Service.
14. Not perform any cryptographic functions while in an error state.
15. Not support multiple concurrent operators.

5 Roles, Services, Authentication & Identification

5.1 Roles

In the *NRevenector 2018*, the User and the Cryptographic Officer are a combined role and share the same services. This role (*Cryptographic Officer/User*) requires identity-based authentication.

The Default User role performs all services which do not read, update, modify or generate critical security parameters (CSPs) and does not require authentication.

5.2 Identity Based Authentication

The operator is authenticated using an identity-based authentication method. This method is based on a challenge-response protocol using a User ID (UID) and secret passphrase known to both parties (pre-loaded into the module). After successful authentication the operator (Host System/PES) implicitly assumes the *Cryptographic Officer/User role.*

5.3 Services

The following services are offered by the cryptographic module. The only one that requires authentication is the Program FLASH service.

Service	Approved Security Functions Used	Associated CSPs	Access Rights	Roles	Notes
(All services that access CSPs)	AES 128 CTR AES 128 CBC HMAC-SHA-256	MKEK NVDEK NVDAK	Read Read Read	CO/User, Default User	The module automatically encrypts, decrypts, and authenticates stored critical security parameters. Operators do not have read access to these CSPs.
Get Device Status	None	None	None	Default User	
Local Login	DRBG	Passphrase DRBG State[1]	Read Read/Write/Generate	Default User	Required to enter the CO/User role.
Logoff	None	None	None	CO/User	Leaves the CO/User role.
Program FLASH with Firmware	RSA 2048 Verify using SHA-256	None	None	CO/User	Receives firmware from an external source and programs it into the cryptographic module's FLASH memory.
Reboot Device	None	None	None	Default User	Service to cause the device to reboot.
Scrap	None	MKEK NVDEK NVDAK DRBG State	Zeroize Zeroize Zeroize Zeroize	Default User	Zeroizes all plaintext CSPs.

[1] DRBG State may include the following CSPs: Entropy string, DRBG seed, DRBG state: Key, and DRBG State: V

Select Programmed Firmware	None	None	None	Default User	Configures the bootloader.
Self-Test	All listed in section 9	None	None	Default User	Performed by power-cycling the device.

Table 3: Services and Roles

5.4 Authentication Strength

The passphrase contains at least 6 randomly chosen characters for the *Cryptographic Officer* | *User* role, resulting in a total of more than 62^6 combinations (here, 62 represents the complete set of 26 upper- and 26 lower-case ASCII letters, together with 10 digits). The probability that a random attempt will succeed is therefore $1/(62^6)$, which is less than 1/1,000,000.

Should multiple attempts be made to authenticate during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur. This is achieved by inserting a delay of 1 second after any failed attempt resulting in a maximum of 60 attempts per minute. The probability is therefore $60/(62^6)$, which is less than 1/100,000.

6 Physical Security

All the components of the device are covered with a hard, tamper-evident potting material, which is tamper evident and opaque within the visible spectrum. The module is inspected for tamper evidence each time it is retrieved from the field. Because of the potting material it is not possible to physically access any internal components without seriously damaging the module or causing zeroization. Hardness testing was performed at ambient temperature and at the extremes of the module's documented operating temperature range (-12 ˚C to 72 ˚C).

7 Cryptographic Functions

7.1 Modes of Operation

The module only has one mode of operation, its FIPS Approved mode of operation. Once the module has completed its self-test and entered its FIPS mode of operation, the LED marked "BL" will light on the printed circuit board. This LED will extinguish when the module is re-booted, for example to start the chosen firmware application. Additionally, the Approved mode indicator is returned via the Get Device Status service.

7.2 Approved Algorithms

The module implements the following FIPS-Approved security functions:

Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	CAVP Cert.	Use
AES	FIPS 197, SP 800-38A	ECB, CBC, CTR	128	#5662	Data encryption / decryption
CKG	SP 800-133			Vendor affirmed	The unmodified output of the DRBG is used for symmetric key generation
DRBG	SP 800-90A & SP 800-90B	CTR DRBG: Block Cipher DF	128	#2497	Deterministic random bit generation
HMAC	FIPS 198-1	HMAC-SHA-256	128	#3769[2]	Message authentication
RSA	FIPS 186-4	PKCS 1.5 SigVer PKCSPSS SigVer	(2048, SHA-256) (2048, SHA-256)	#3046[3]	Digital signature verification
SHS	FIPS 180-4	SHA-256		#4538[4]	Message digest

Table 4: FIPS 140-2 Approved Security Functions

7.3 Allowed Algorithms

The module uses a single hardware implemented NDRNG for seeding the DRBG. The NDRNG is allowed, but not FIPS approved. The NDRNG is used as the entropy source for the module's DRBG, which is seeded with full entropy (security strength of 128 bits).

7.4 Non-Approved Algorithms (Not Security Functions)

The following algorithms may be used in the approved mode of operation because they are considered non-approved cryptographic algorithms that are not security functions per IG 1.23. Data secured with these algorithms is considered plaintext.

---

[2] HMAC-SHA-1 is included in the CAVP certificate, but is not used by the module

[3] The following capabilities are included in the CAVP certificate, but are not used by the module: RSA 2048 SHA-256 KeyGen and PKCS 1.5 SigGen

[4] SHA-1 is included in the CAVP certificate, but is not used by the module

Algorithm	Caveat	Use
AES	(no security claimed)	Proprietary implementation used for obfuscation of data that remains within the module.
KDF	(no security claimed)	Proprietary implementation used to derive non-compliant keys used for obfuscation in the Local Login challenge-response protocol. This algorithm is compliant with FIPS 140-2 requirements for authentication strength.
PBKDF	(no security claimed)	Used to derive non-compliant keys used for obfuscation of data in transit during the Local session. This algorithm is compliant with FIPS 140-2 requirements for authentication strength.

Table 5: FIPS 140-2 Non-Approved Algorithms (Not Security Functions)

8 Cryptographic Keys and Critical Security Parameters

The following section lists the critical and public security parameters that are retained by the device. All encrypted critical security parameters in the module are protected by 128-bit AES using the MKEK (which encrypts the NVDEK and NVDAK, which encrypt and authenticate all encrypted CSPs), which is zeroized by the scrap service. Critical security parameters, including private and secret keys, are not output by or input to the module.

8.1 Critical Security Parameters

The table below lists the critical security parameters:

Name	Algorithm	Storage	Generation	Establishment	Destruction	Purpose
Data Encryption Master Key (MKEK) (128-bit key)	AES 128 bits, Counter mode	Plaintext	Internal DRBG (during manufacturing)	N/A	Scrap service or tamper event	Serves to encrypt and decrypt critical security parameters.
Data Encryption Key (NVDEK) (128-bit key)	AES CBC, 128 bits	Encrypted	Internal DRBG (during manufacturing)	N/A	Scrap service, tamper event	Serves to encrypt and decrypt other internally stored critical security parameters.
Data Authentication Key (NVDAK) (128-bit key)	HMAC-SHA256	Encrypted	Internal DRBG (during manufacturing)	N/A	Scrap service, tamper event	Serves to authenticate other internally stored critical security parameters.
Entropy string	NDRNG	Not persistently stored	Internal NDRNG	N/A	Power cycle (volatile)	Required for generation of DRBG state
DRBG seed	CTR_DRBG using AES 128	Not persistently stored	Internal NDRNG	N/A	Power cycle (volatile)	Internal state of the Deterministic Random Bit Generator.
DRBG State: Key	CTR_DRBG using AES 128	Encrypted	Updated during random number generation	N/A	Scrap service, tamper event.	Internal state of the Deterministic Random Bit Generator.
DRBG State: V	CTR_DRBG using AES 128 bits	Encrypted	Updated during random number generation	N/A	Scrap service, tamper event.	Internal state of the Deterministic Random Bit Generator.
Passphrase	N/A	Encrypted	N/A	Pre-loaded (during manufacturing)	N/A (encrypting key zeroized by scrap/tamper)	Identity based authentication

Table 6: Critical Security Parameters

8.2 Public Security Parameters

The following public keys are stored in the device:

Name of certificate or public key	Algorithm	Storage	Generation	Purpose
FPCustomerRootKey	2048-bit RSA key	Plaintext	N/A	Used to verify integrity of Bootloader firmware
Firmware Verification Key	2048-bit RSA key	Plaintext	N/A	Used to verify firmware from Francotyp-Postalia.

Table 7: Public Security Parameters

8.3 Zeroization

Zeroization may occur under the following conditions:

Event	Effect	Resulting State	Speed	Recovery Action
Tamper	All CSPs rendered unreadable.	Chip unbootable until tamper cause has been removed and device is power cycled. If bootable, device permanently enters DEFECT state. No cryptographic functions may be used.	Immediate	Return to FP.
Battery removed	All CSPs rendered unreadable.	Restoring battery will result in device permanently entering DEFECT state. No cryptographic functions may be used.	Immediate	Return to FP.
Scrap service run	All CSPs rendered unreadable.	Device permanently enters SCRAPPED state. No cryptographic functions may be run.	Fast (<40µs)	Return to FP.

Table 8: Zeroization

9 Self-Tests

9.1 Power on self-tests

The following self-tests are performed when the module starts (either following a power on, or following the call to a reboot service):

Firmware Integrity Test

The integrity of the application firmware is verified at initial power-on of the module by comparing the generated hash against a known SHA 256 hash from PKCSPSS (RSA #3046).

Cryptographic Algorithm Tests

The following table lists the cryptographic algorithm tests for Approved security functions that are performed as part of the power-on self-tests. See Table 4 for corresponding NIST certificates.

Security Function	Type of self-test
AES 128 Encrypt/Decrypt (ECB, CBC)	Encrypt KATs (Known Answer Tests) Decrypt KATs
DBRG[5]	Instantiate KAT Generate KAT Reseed KAT
HMAC-SHA-256	HMAC-SHA-256 KAT
RSA 2048 Verify using SHA-256	Verify KAT, includes SHA-256 verification
SHA-256	SHA-256 KAT, tested as part of RSA verification

Table 9: FIPS 140-2 Cryptographic Algorithm Tests

9.2 Conditional Tests

The following conditional tests are performed:

[5] In accordance with FIPS 140-2 Implementation Guidelines December 2019 sect 9.8, the SP 800-90A compliant DRBG does not perform the continuous random number generator test as described in FIPS 140-2 section 4.9.2

Security Function	Self-Test Performed
NDRNG[6]	Repetition count test and adaptive proportion test in accordance with FIPS 140-2 Implementation Guidelines December 2019 sect 9.8.
Firmware Loading Test	On loading of programmed firmware: Performs RSA 2048 SHA 256 PKCS#1 V1.5 (RSA #3046) signature verification on loaded firmware.

Table 10: Conditional Tests

9.2.1 Critical Function Tests

The module tests the Microcontroller Operational Mode to ensure correct operation.

9.3 Error States

The module implements several self-tests during power up and as conditional self-tests linked to cryptographic operations.

In the event of an error being detected, the *NRevenector 2018* enters an error state. The device remains in the error state until it is rebooted. The error state information can be retrieved via the Get Device Status service.

Error states may be cleared only by power-cycling the module.

[6] In accordance with FIPS 140-2 Implementation Guidelines December 2019 sect 9.8, the NDRNG performs the repetition count test instead of the continuous random number generator test as described in FIPS 140-2 section 4.9.2

10 Mitigating Other Attacks

The device includes environmental failure protection means for the battery voltage and the module temperature. If an attack is detected then the contents of the cryptographic integrated circuit's battery powered key storage are automatically zeroized, leaving the module inoperable.

The device includes environmental failure protection means for the main input voltage, and the internal core voltage. If one of these conditions is outside a defined range the device is held in the reset condition. The device also includes environmental failure protection such that temperature changes outside the normal operating ranges will not compromise the security of the device.

The device includes a protection means to test for drift in the main clock frequency of the processor. The cryptographic module's processor also incorporates a layer of metal shielding as one of its layers, used to detect attempts at intrusion at a die level. In the event of an intrusion attempt being detected, the contents of its battery powered key storage are automatically zeroized leaving the module inoperable.

The failure protection for the battery voltage and temperature, and the tamper detection for the physical breach of the module's physical boundary are present using power from the battery even when the device is switched off. The module's processor responds by destroying the stored plaintext CSPs.

11 Glossary and Abbreviations

Term	Definition
AES	Advanced Encryption Standard
CKG	Cryptographic Key Generation
CSPs	Critical Security Parameters
CO	Cryptographic Officer
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EMI/EMC	Electromagnetic Interference/ Electromagnetic Compatibility
FP	Francotyp-Postalia Holding AG
HMAC	Hash-based Message Authentication Code
KAS	Key Agreement Scheme
KDF	Key Derivation Function
MAC	Message Authentication Code
MKEK	Data Encryption Master Key
NVDAK	Non-Volatile Data Authentication Key
NVDEK	Non-Volatile Data Encryption Key
PBKDF	Password-Based Key Derivation Function
PRDIs	Postal Relevant Data Items
PSD	Postal Security Device
RSA	Rivest–Shamir–Adleman (asymmetric algorithm)
RSAK	Remote Session Authentication Key
RSEK	Remote Session Encryption Key
SHS	Secure Hash Algorithm
TDES or Triple DES	Triple Data Encryption Standard
UID	User ID
USPS	United States Postal Service

Table 11: Glossary and Abbreviations

12 References

Reference	Publication
FIPS 140-2 Derived Test Requirements (DTR)	January 2011
FIPS 140-2 Implementation Guidance (IG)	December 2019
FIPS 140-2 Publication (PUB)	May 2001
FIPS 180-4	August 2015
FIPS 186-4	July 2013
FIPS 197	November 2001
FIPS 198-1	July 2008
NIST SP 800-38A	December 2001
NIST SP 800-56A	Revision 1, March 2007; Revision 3, April 2018
NIST SP 800-56C	Revision 1, April 2018
NIST SP 800-67	Revision 2, November 2017
NIST SP 800-90A	June 2015
NIST SP 800-90B	January 2018
NIST SP 800-133	December 2012

Table 12: References