SECURITY POLICY

cVEND plug

Contactless Payment and Ticketing Module

FEIG ELECTRONIC GmbH
Lange Strasse 4
D-35781 Weilburg-Waldhausen
Tel.: +49 6471 3109-0
http://www.feig.de

With the edition of this document, all previous editions become void. Indications made in this document may be changed without previous notice.

Contents

1. History

Version	Status	Author	Date	Notes
0.1	Preliminary	Rafael Keller	2015-03-04	Initial draft version
0.2	Preliminary	Rafael Keller	2015-06-15	Chaper 7
0.3	Preliminary	Rafael Keller	2015-06-23	Chaper 7 update
1.1	Final	Rafael Keller	2015-07-02	cVEND plug
1.2	Final	Michael Jung	2015-07-05	Updated End-Of-Live Procedure Added section on Application Signing Added section on Cryptographic Services

2. Introduction

This document relates to the “cVEND plug Unattended Contactless Payment Terminal” product. It specifies the security policies that are to be implemented to comply with the PCI PTS approval of the device.

3. General

3.1. Product Type

cVEND plug is a secure card reader to handle contactless payment transactions without PIN entry.

3.2. Product Identification

Figure 1 shows cVEND plug in front view, figure 2 in rear view. For the installation of cVEND plug follow chapter 4.

Figure 1: cVEND plug front view - not installed

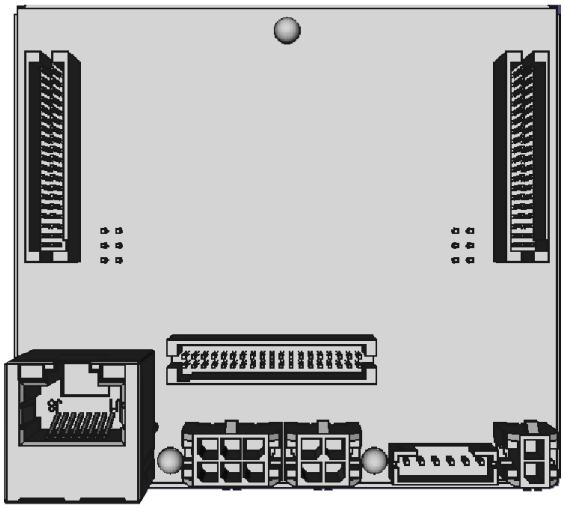

Figure 2: cVEND plug rear view - not installed

3.3. Product Name

cVEND plug product name is printed on the cVEND plug label located around the Ethernet jack (see figure 3). The label at the back of the device shall not be teared off, covered or altered.

3.4. Hardware Version Number

cVEND plug hardware version number is printed on the cVEND plug label located around the Ethernet jack.

3.5. Software Version Number

cVEND plug software version number is printed on the cVEND plug label located around the Ethernet jack.

.

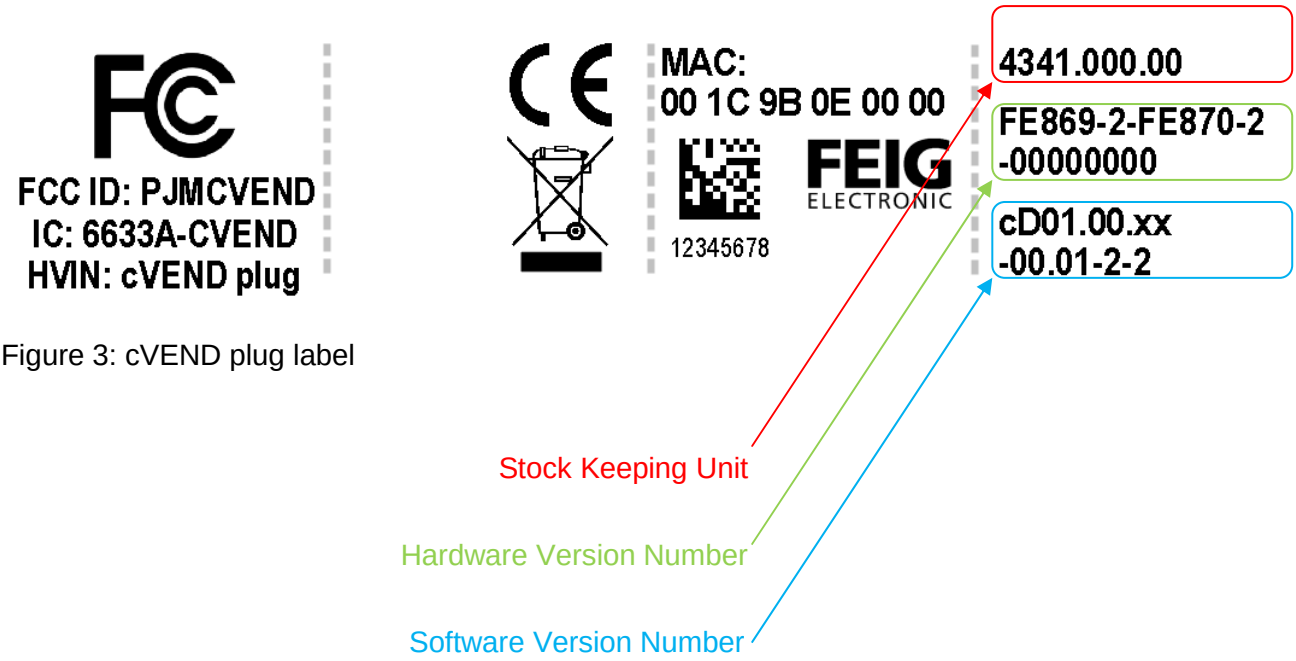

Figure 3: cVEND plug label

4. Guidance

4.1. Initial Security Inspection

The system integrator of cVEND plug must visually inspect every received cVEND plug device after shipping from FEIG ELECTRONIC before integrating the cVEND plug device into his installation.

Furthermore the system integrator is advised to check every device on a regular basis after receipt and installation.

4.2. Periodic Inspection

The system integrator, merchant or acquirer has to check:

- The cVEND plug label is undamaged.
- The serial number on the label corresponds to the inventory.
- There is no flashing red tamper led after power on (see figure 1 for the position of the led).
- There is no tamper buzzer after power on.
- There are no cables or wires connected to any port of cVEND plug or associated equipment, other than needed for intended use.

If a tamper event is observed, the merchant or acquirer must contact the system integrator immediately and remove cVEND plug from service and keep cVEND plug available for potential forensics investigation.

4.3. Installation Guide

Installation of cVEND plug must be carried out according to the cVEND plug installation manual [1].

The installation manual and the security guidance [2] have references for the system integrator:

- How to check the completeness of the delivered equipment.
- The storage location of the referenced documents.
- The information about power and cable connections.
- The technical specifications of the device (i.e. temperature, humidity, voltage)
- The safety recommendations.
- The security recommendations.

For flush integration into non conducting housings one round opening with a diameter of 28,5 mm is necessary to show the back-lit contactless symbol. To comply with EMVCo regulations:

- The contactless logo must be visible.
- The upper edge of the cVEND plug plastic dome and the target terminal front plate must be on the same level.
- Avoid any kind of conducting material surrounding the cVEND plug.
- Do not use conducting materials for fastening.

4.4. End of Life

Before decommissioning the device all sensitive data and keys must be erased. This is done by short-circuiting the battery supply as shown in the picture below with any conducting tool (e.g. a power resistor < 10 Ohm).

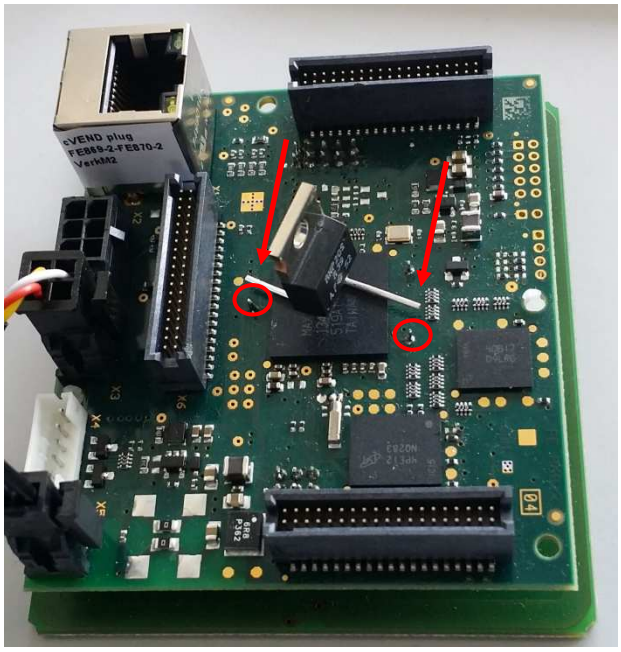

Figure 4: End-of-Life: Short circuit the battery supply

5. Hardware Security

The security of the terminal is not compromised by altering environmental conditions.

Temperature Range:	Operating	-25 °C to +70 °C ambient temperature
	Storage	-25 °C to +80 °C

The device contains tamper mechanisms that will trigger when a physical penetration attempt of the device is detected. A tamper event can easily be detect if:

There is a flashing red tamper led (see figure 1).

The tamper buzzer is on.

There is a tamper message send out on the serial port.

If a tamper event is observed, the merchant or acquirer must contact the system integrator immediately and remove cVEND plug from service and keep cVEND plug available for potential forensics investigation.

6. Software Security

6.1. Development

The cVEND plug firmware implements the required security measures and functions to be compliant with PCI security requirements for authenticated applications.

When developing applications, the developers must refer to the coding specifications and the best practices described in [1]. This security guidance describes how protocols and services must be used and configured for each interface that is available on cVEND plug. The document provides security guidance for account data management and remote connection authentication using cryptographic mechanisms. When developing IP enabled applications and SRED applications the developer must abide by the coding rules and best practices described in the document.

6.2.Operation

The system implements a self-test mechanism to verify the integrity of the software including firmware and user applications running on the secure devices. The self-test also covers cryptographic operations, random number generation and a presence check for required cryptographic key. The self-test is scheduled to run each 24 hours and at each start up. Each time a software update is performed on the device a restart is required to make the new software version operative.

If the self-test fails, the system goes into an out of service status and a DRS is triggered. The self-test procedure is integrated into the system firmware and runs transparent for the end user and for payment applications responsible for payment transactions.

Details are described in [1].

7. Identifying PCI Compliant cVEND plug Devices

FEIG does ship cVEND plug devices that are meant to be used for development, test and quality assurance as well as devices meant to be used with in real installations in the field. Those two classes of devices can be distinguished by means of their respective Firmware Version Identifier.

It is the responsibility of the system integrator to ensure that only PCI compliant devices are deployed in the field.

7.1. Identifying the installed Firmware Version

Applications that are running on the cVEND plug device can identify the installed firmware version by reading the contents of the file /boot/version.

The firmware version will also be reported via the 'Manufacturer' USB descriptor string. E.g. if port X2 (see [1]) of a cVEND plug device is connected to an USB host port on a Linux PC a string similar to the following will appear in the system log:

Manufacturer: FEIG Electronic GmbH - cVEND - cS01.01.23-00.01-2-2

The installed firmware version in this example is cS01.01.23-00.01-2-2

For Microsoft Windows there are freeware tools available that allow to extract USB string descriptors (E.g. "USB Descriptor Dumper" from Thesycon).

7.2. Format of the Firmware Version Identifier

Figure 5 below describes the format of the cVEND plug Firmware Version Identifier.

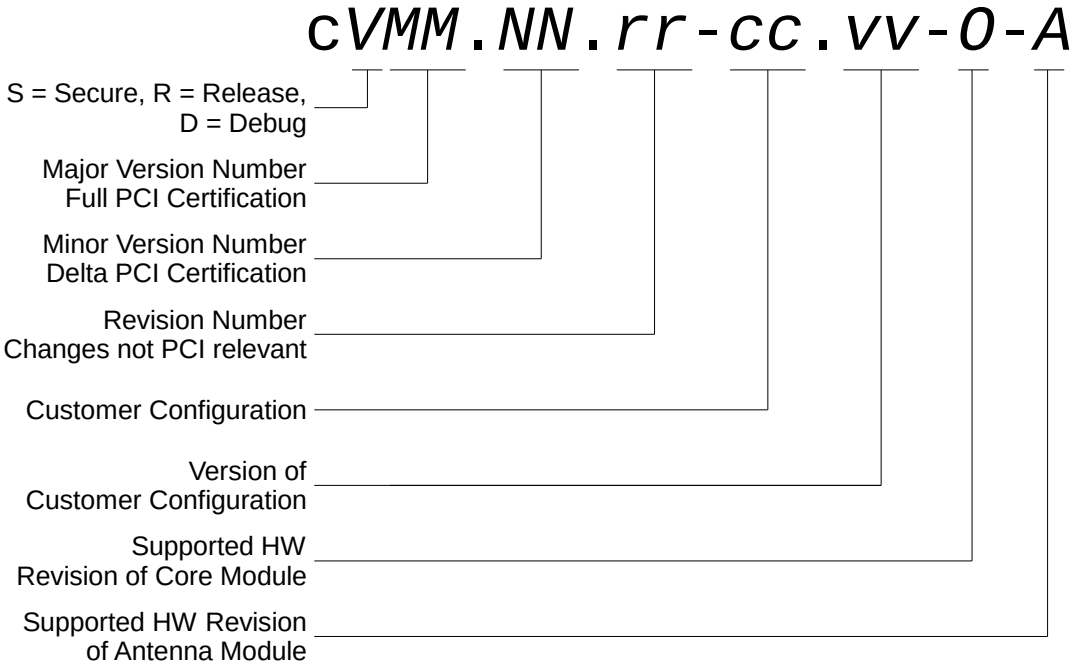

Figure 5: Format of the cVEND plug Firmware Version Identifier

A given cVEND plug firmware version is PCI compliant only if the respective Firmware Version Identifier matches the following pattern (where the * symbols might be any digit 0-9):

cS01.01.**-**.**-*-*

- The first character is the small letter ‘c’ (Identifying product cVEND plug).
- The second character is a capital letter ‘S’ (Identifying a secure device). If the second character is a capital letter ‘D’ or ‘R’ then the device is meant for development, test and quality assurance and should not be deployed in field installations.
- The third and fourth characters are digits identifying the major version number, and the sixth and seventh characters are digits representing the minor version number. Only the combination 01.01 (Major.Minor) has been PCI approved.
- The ninth and the tenth characters are digits representing the firmware revision. Changes in firmware revisions are not relevant for whether a given firmware version is PCI compliant.
- The twelfth and the thirteenth and the fifteenth and the sixteenth characters are digits identifying the firmware customization and the version of said customization, respectively. Those characters are not relevant for whether a given firmware version is PCI compliant.
- The eighteenth and the twentieth characters are digits which identify the minimum hardware revision numbers for the core and the antenna printed circuit board, which are supported by the respective firmware version. Those characters are not relevant for whether a given firmware version is PCI compliant.

Any change to cVEND plug firmware that impacts platform security will result in a change of either the major or the minor version number. The security guidelines described in this document apply to major version 01 and minor version 01 only.

8. Security Guideline

The Security Guideline [1] gives in depth information to the following topics:

- Vulnerability Disclosure
- Firmware Updates
- Application Updates
- Access to Sensitive Services
- Configuration Management
- Cryptographic Services
- Account Data Protection
- Open Protocols

It is the responsibility of the organization that uses cVEND plug to follow the Security Guideline.

9. Signing Applications

cVEND plug will grant access to sensitive services (such as the keystore) only to applications that have been digitally signed. FEIG does provide PIN protected USB SmartCard HSMs to system integrators for signing applications. Please see [1] for details.

10. Cryptographic Services

10.1. Supported Encryption Algorithms

All encryption and decryption operations with private or secret keys that involve account data must be done via specific APIs as described in [1]. The following encryption algorithms are supported:

AES-128 ECB
AES-128 CBC with ISO-Padding
AES-128 CBC with PKCS#7-Padding
TDEA-168 ECB
TDEA-168 CBC with ISO-Padding
TDEA-168 CBC with PKCS#7-Padding
RSAEP
RSAES-PKCS1-v1_5
RSAES-OAEP with MGF SHA-256/-512

10.2. Supported Digital Signature Algorithms

All signature creation and verification operations that involve account data must be done via specific APIs as described in [1]. The following signature algorithms are supported:

CMAC with AES or TDEA cipher
HMAC-SHA256
HMAC-SHA512
RSASSA-PKCS1-v1.5 with SHA-1
RSASSA-PKCS1-v1.5 with SHA-256
RSASSA-PKCS1-v1.5 with SHA-384
RSASSA-PKCS1-v1.5 with SHA-512
RSASSA-PSS with SHA-1, SHA-256, SHA-384 or SHA-512
RSASSA-PSS with SHA-256
RSASSA-PSS with SHA-384
RSASSA-PSS with SHA-512

10.3. Minimum Key Lengths for Account Data Encryption

The following minimum key lengths must be applied when encrypting account data:

Key Type	Minimum Key Length [bit]
RSA	2048
AES	128
TDEA	168

10.4. Loading of Symmetric Secret Keys

cVEND plug does provide means to im- and export symmetric secret keys into and from its keystore via specific APIs. Symmetric secret keys can be imported into a cVEND plug's keystore

from another trusted system. Or they can be exported from a cVEND plug's keystore into another trusted system.

Said 'other' trusted systems (which might or might not be other cVEND plug keystores) are identified by a pair of X.509 certificates (namely the Key Signing Key's and the Key Encryption Key's X.509 certificates), whose public keys are used

- to verify the signature of a key block (if importing into a cVEND plug keystore from another trusted system), or
- to encrypt a key block (if exporting from a cVEND plug keystore into another trusted system), respectively.

Please see [1] for further details.

10.5. Replacement of Potentially Compromised Keys

It is the responsibility of the system integrator to replace keys whenever the original key is known or suspected to have been compromised. A key has to be assumed to have been compromised if a time span has expired that would allow to determine the key via a brute-force attack.

10.6. Overview of Keys and Certificates

Table 1 specifies all keys and certificates which are used during the lifetime of cVEND plug devices.

Table 1: cVEND plug keys

Key Name	Symbolic Key Name	Purpose / Usage	Algorithm	Size (Bits)	Generated By:
Root Key Private Key	MRK_PRIV	Signing FW_PUB	RSA	2048	HSM
Root Key Public Key	MRK_PUB	Verifying FW_PUB	RSA	2048	HSM
Firmware Key Private Key	FW_PRIV	Signing firmware images and firmware update packages	RSA	2048	FEIG USB Token
Firmware Key Public Key	FW_PUB	Verifying firmware images and firmware update packages	RSA	2048	FEIG USB Token
Application Key 0 – 7 Private Key	APP*[n]*_PRIV *n* in { 0 .. 7 }	Signing application binaries and application update package	RSA	2048	FEIG USB Token
Application Key	APP*[n]*_PUB	Verifying applica-	RSA	2048	FEIG

0 – 7 Public Key	*n* in { 0 .. 7 }	tion binaries and application update packages			USB Token
DRAM Encryption Key	AES_DRAM	Encryption of DRAM content	AES	128	cVEND plug TRNG
Battery backed AES KEY	AES_BB	Encryption of device keystore content	AES	256	cVEND plug TRNG
Terminal Authentication Key Private Key	TERM_AUTH_PRIV	Device authentication.	RSA	2048	FEIG cVEND plug Keystore DRNG
Terminal Authentication Key Public Key	TERM_AUTH_PUB	Device authentication	RSA	2048	FEIG cVEND plug Keystore DRNG
Terminal Authentication Key X.509 certificate	TERM_AUTH_X509	Device authentication	X.509	2048	FEIG cVEND plug Keystore DRNG
Terminal Key Encryption Key Private Key	TERM_KEK_PRIV	Key loading	RSA	3072	FEIG cVEND plug Keystore DRNG
Terminal Key Encryption Key Public Key	TERM_KEK_PUB	Key loading	RSA	3072	FEIG cVEND plug Keystore DRNG
Terminal Key Encryption Key X.509 certificate	TERM_KEK_X509	Key loading	RSA	3072	FEIG cVEND plug Keystore DRNG
Terminal Key Signing Key Private Key	TERM_KSK_PRIV	Key loading	RSA	2048	FEIG cVEND plug Keystore DRNG
Terminal Key Signing Key Public Key	TERM_KSK_PUB	Key loading (	RSA	2048	FEIG cVEND plug Keystore DRNG
Terminal Key Signing Key X.509 certificate	TERM_KSK_X509	Key loading	RSA	2048	FEIG cVEND plug Keystore DRNG
Terminal Data Encryption Key Private Key	TERM_DEK_PRIV	Data encryption	RSA	2048	FEIG cVEND plug Keystore DRNG
Terminal Data Encryption Key Public Key	TERM_DEK_PUB	Data encryption	RSA	2048	FEIG cVEND plug Keystore DRNG
Terminal Data Encryption Key	TERM_DEK_X509	Data encryption	RSA	2048	FEIG cVEND plug

X.509 certificate					Keystore DRNG
Terminal CA Private Key	TERM_CA_PRIV	Signing TERM_[AUTH|KEK|DEK]_X509	RSA	2048	FEIG USB Token
Terminal CA X.509 certificate	TERM_CA_X509	Verifying TERM_[AUTH|KEK|DEK]_X509	X.509	2048	FEIG Root CA
Root CA private key	ROOT_CA_PRIV	Signing TERM_CA_X509	RSA	2048	FEIG USB Token
Root CA X.509 certificate	ROOT_CA_X509	Verifying TERM_CA_X509	X.509	2048	FEIG Root CA (self signed)
Terminal Management System X.509 certificate	TMS_X509	Terminal Management System authentication	X.509	2048 - 3072	Terminal Management System operator
Terminal Management System CA private key	TMS_CA_PRIV	Signing terminal management system X.509 certificates	RSA	2048 – 3072	Terminal Management System vendor
Terminal Management System CA X.509 certificate	TMS_CA_X509	Verifying terminal management system X.509 certificates	X.509	2048 - 3072	Terminal Management System vendor. Cross signed by FEIG with ROOT_CA_PRIV.
Key Block Protection Key for ANSI X.9 TR31 using Key Derivation (see [8])	KEY_BLOCK_PROTECT_MASTER	Key loading	AES or TDES	128 or 168	FEIG cVEND plug Keystore DRNG
Key Block Encryption Key for ANSI X.9 TR31 using Key Derivation (see [8])	KEY_BLOCK_KEK	Key loading	AES or TDES	128 or 168	FEIG cVEND plug Keystore
Key Block MAC Key for ANSI X.9 TR31 using Key Derivation (see [8])	KEY_BLOCK_MAC	Key loading	AES or TDES	128 or 168	FEIG cVEND plug Keystore
Application specific AES key	CUSTOM_AES	Application specific	AES	128	FEIG cVEND plug Keystore via C_GenerateKey or TMS via C_UnwrapKey
Application specific TDES key	CUSTOM_TDES	Application specific	TDES	128	FEIG cVEND plug Keystore via C_GenerateKey or TMS C_UnwrapKey
Application specific HMAC key	CUSTOM_HMAC	Application specific	HMAC	64 – 128	FEIG cVEND plug Keystore via C_GenerateKey or TMS C_UnwrapKey
Application specific RSA private key	CUSTOM_PRIV	Application specific	RSA	512 – 3072	FEIG cVEND plug Keystore via C_GenerateKeyPair

Application specific RSA public key	CUSTOM_PUB	Application specific	RSA	512 - 3072	FEIG cVEND plug Keystore via C_Generate-KeyPair

Details about techniques and management of the above mentioned keys and references to describing documents can be found in [1]. The cVEND plug Security Guidance also describes Key Replacement and Removal, Key Injection and Authentication processes.

11. Roles and Services

All roles supported by the device and the services and permissions available for each role:

Feig Electronic sells cVEND plug only to system integrators. Feig Electronic as **maintainer** provides guidelines how to integrate cVEND plug and maintainance to support cVEND plug for the system integrator. Feig Electronic generates and maintains customer keys, repairs the device and handles devices with tamper events. The system integrator is the **administrator** of the device. He organizes third party developed applications for cVEND plug, access to sensitive data on cVEND plug and the terminal management system. The end user is a **operator** who performs payment transactions.

12. Glossary

[POS]	Point of Sale
[TRNG]	True Random Number Generator
[DRS]	Destructive Reset Source

13. Related Documents

[1] FEIG ELECTRONIC GmbH, *cVEND Security Guidance,* pay-doc:/Customer Documentation/Security Guidance/cVEND Security Guidance.docx, 2015.

[2] American National Standards Institute, *X9 TR-31: Interoperable Secure Key Exchange Key Block Specification for Symmetric Algorithms,* pay-doc:/References/ANSI/X9 TR-31.pdf, 2010.