NYC1-SCR

SECURITY POLICY

NYC1-SCR Security Policy

The examples and sample programs are for illustration only and may not be suited for your purpose. You should verify the applicability of any example or sample program before placing the software into productive use. This document, including without limitation the examples and software programs, is supplied "As-Is."

Adyen, the Adyen logo, are registered trademarks of Adyen N.V. Other brand names or trademarks associated with Adyen's products and services are trademarks of Adyen N.V. All other brand names and trademarks appearing in this manual are the property of their respective holders.

Please e-mail all comments in this document to your local Adyen Support Team or to main Adyen Support Team PCI@adyen.com.

Adyen N.V.

www.adyen.com

NYC1-SCR Security Policy

Revision History

Version	Data	Change description
0.9.0	28.02.2022	Draft version
1.0.0	05.04.2022	Release version
1.1.0	18.05.2022	Updated sections “Product Identification”, “Key Management” and “Software Security”
1.2.0	10.06.2022	Updated section “Product Identification”
1.3.0	10.06.2022	Updated section “Product Identification”
1.4.0	15.06.2022	Updated section “Product Identification”

Contents

Document Overview

This document addresses the proper use of NYC1-SCR in a secure manner including information about key-management responsibilities, administrative responsibilities, device functionality, identification and environmental requirements.

Failure to use of the device in accordance with this security policy will violate its PCI PTS 6.1 compliance and approval.

Audience

This guide provides simple descriptions of NYC1-SCR features, as well as basic information for anyone installing and configuring NYC1-SCR.

Acronyms

AES	Advanced Encryption Standard
COTS	Commercial off-the-shelf Device
DUKPT	Derived Unique Key per Transaction
N/A	Not Applicable
PCI	Payment Card Industry
PED	PIN Entry Device
PIN	Personal Identification Number
POI	Point of Interaction
RSA	Rivest Shamir Adelman Algorithm
SCR	Secure Card Reader
SHA	Secure Hash Algorithm
TDES	Triple Data Encryption Standard

References and Related Documentation

[1] NYC1-SCR User Manual

[2] NYC1-SCR Firmware API Specifications

[3] NYC1-SCR Software Design Specifications

[4] NYC1-SCR Application Development Guidelines

[5] ANSI X9.24-1-2017, Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques

[6] ANSI X9.24-2-2016: Retail Financial Services Symmetric Key Management Part 2: Using Asymmetric Techniques For The Distribution Of Symmetric Keys

[7] ASC X9 TR 31-2018: Interoperable Secure Key Exchange Block Specification

[8] ISO 9564-1, Financial services — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for PINs in card-based systems

[9] ISO 9564-2, Banking — Personal Identification Number management and security Part 2: Approved algorithms for PIN encipherment

[10] PCI PTS POI Derived Test Requirements V6.1 – March 2022

[11] RSASSA-PKCS1-V1_5 (RSA sign/verify) defined in PKCS#1 v2.1 Draft 2 January 5, 2001)

[12] Integrated Circuit Card Specification for Payment System, Book 2 Security & Key Management, Version 4.3, November, 2011

[13] ASC X9 TR 34-2019: Interoperable Method For Distribution Of Symmetric Keys Using Asymmetric Techniques: Part 1 - Using Factoring-Based Public Key Cryptography Unilateral Key Transport - Includes Corrigendum

[14] ANSI X9.24-3-2017 Retail Financial Services Symmetric Key Management Part 3: Derived Unique Key Per Transaction”

Note: [1] is delivered to the end-user, [2,3,4] are delivered to authorized application developers

Product Description

The NYC1-SCR unit is a handheld Payment Terminal with an integrated smart, magnetic stripe and contactless card reader, offering advanced security and payment processing capabilities to handle credit and debit card transactions in an attended or semi-attended environment.

NYC1-SCR supports both symmetric encryption algorithms (3DES, and AES) and asymmetric encryption (RSA).
The NYC1-SCR sleek and stylish ergonomic design offers power and performance in a smart, MSR, and contactless-integrated payment device.

Features and Benefits

Exceptional Ease of Use

- Ergonomic design is sleek, stylish, and lightweight for conveniently handing the unit to the consumer.

Critical Security Protection

- Incorporates tamper-detection circuitry to resist unauthorized intrusion and supports a broad spectrum of hardware and software-based security features.
- Integrated security modules simultaneously support sophisticated encryption (AES, DES, 3DES, RSA) and key management schemes.

Strong Feature Set

The NYC1-SCR is designed to handle all forms of payment including:

- EMV chip
- Magstripe
- Contactless

NYC1-SCR provides connectivity options:
- USB
- Bluetooth Low Energy (how to be pairing is described in the User Manual).
- UART serial communication (over rear pads)

Product Identification

Product Name and Hardware Version

The product name and hardware version are printed on a label at the back side of the device.

The label at the back side of the device shall not be teared off or altered.

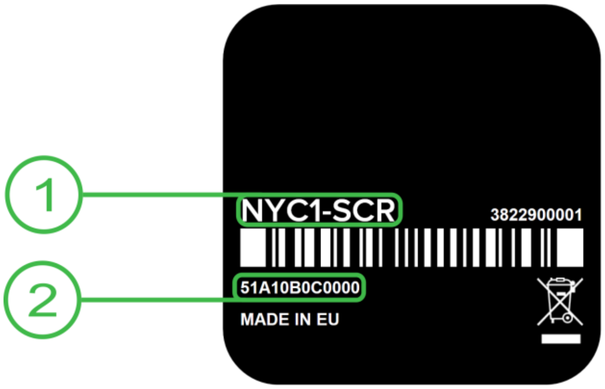

Figure 1 – Product Name and hardware version Identification

1. Product name
2. Hardware version

Position	Description	HW version
1	Fixed	5
2	Fixed	1
3	Fixed	A
4	Fixed	1
5	Variable position for different printed company logo (Value range 0-9, A-Z)	x
6	Variable position for Bluetooth module	x
7	Variable position for device Color	x
8	Fixed position; C for CTLS version and N for non CTLS version	C
9	These variables are used for minor changes to the HW that are not security relevant. (BOM changes, minor rerouting, etc…) Values range 0-9.	x
10		x
11		x
12		x

Table 1 Hardware version

All approved hardware versions can be located on the PCI PTS SSC portal.

Software Versions

The product firmware and/or application versions can be retrieved using the serial interface firmware command: 01, described in Firmware API Specifications[2] document:

3.0.xx.xx

Figure 2 – Product Firmware version Identification

*Only the first two digits (**3.0**.xx.xx) of the firmware versions are the PCI approved versions. The rest digits of the version indicate minor non-security related changes.

Position	Description	SW version
1	Fixed	3
2	Fixed (separator)	.
3	Fixed (Revised for any security changes)	0
4	Fixed (separator)	.
5	Variable position that indicates minor changes of the FW that are not related to the security mechanisms and do not require evaluation from external Security Evaluation Laboratory (adding new features or bug fixing). Variables range 0-9.	x
6		x
7	Fixed (separator)	.
8	Variable position that indicates minor changes of the FW that are not related to the security mechanisms and do not require evaluation from external Security Evaluation Laboratory (adding new features or bug fixing). Variables range 0-9.	x
9		x

Table 2 Firmware version

3.0.xx.xx

Figure 3 – Product Application version Identification

*Only the first two digits (**3.0**.xx.xx) of the application versions are the PCI approved versions. The rest digits of the version indicate minor non-security related changes.

Position	Description	SW version
1	Fixed	3
2	Fixed (separator)	.
3	Fixed (Revised for any security changes)	0
4	Fixed (separator)	.
5	Variable position that indicates minor changes of the AP that are not related to the security mechanisms and do not require evaluation from external Security Evaluation Laboratory (adding new features or bug fixing). Variables range 0-9.	x
6		x
7	Fixed (separator)	.
8	Variable position that indicates minor changes of the AP that are not related to the security mechanisms and do not require evaluation from external Security Evaluation Laboratory (adding new features or bug fixing). Variables range 0-9.	x
9		x

Table 3 Application version

All approved software versions can be located on the PCI PTS SSC portal.

Hardware Security

Initial Security Inspection

Upon receiving the NYC1-SCR terminal, the merchant or acquirer must validate the shipment origin and sender name of the terminal to be genuine by verifying the courier tracking number and sender information located on the product order paperwork/invoice.

Different company logos may be printed on the device.

The terminal must be visually inspected for signs of tampering prior to placement in the field to ensure that the device has not been tampered with and is in original pristine condition.

Note: A User Manual[1] including the following information is provided with the device:

- Equipment check list:
  - Device,
  - Cable and connectors,
  - Documents
- Power and cable connections information,
- The main characteristics of the device (i.e. Temperature, humidity, voltage)
- Safety recommendations,
- Security recommendations,
- Troubleshooting if the device does not work.

NYC1-SCR must be verified to be approved by PCI SSC as a SCR (Secure Card Reader) on the official PCI PTS SSC portal:

https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

- Locate the Product Identification Label on the back of the device and verify that the product name and hardware version number match the product name and hardware version number shown on the PCI PTS listing web site.
- Compare the first two digits of the Firmware version with the one listed in the PCI PTS listing web site.

Periodic Inspection and Maintenance

The following inspections must be performed on a regular daily basis after initial receipt and installation of NYC1-SCR:

- Once a day device must be detached from COTS or docking station and check back side for any visual damages. (Applicable for devices attached to COTS or docking station)
- It should be checked after turning on the device is not in a Tampered state, please refer to the "Tamper Response Event".
- There are no unusual wires connected to the ICC acceptor (Figure 4), magnetic stripe slot (Figure 5), or any of the ports on the terminal.
- There is no shim device in the ICC acceptor slot.
- The terminal serial number(on the label) corresponds to the one in the inventory paperwork.

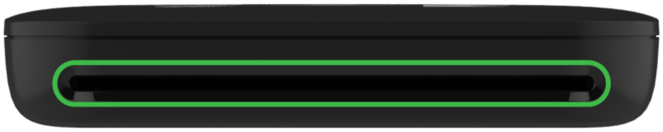

Figure 4 – IC card slot

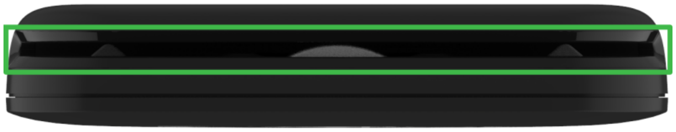

Figure 5 – Magnetic stripe slot

Note: Such checks would provide warning of any unauthorized modification to the terminal, or suspicious behavior of the terminal or suspicious behavior of individuals that have access to the terminal. In the tampered state, first LED light continually and fourth LED blinking and the use of the device is not possible. If such state is observed, the merchant or acquirer must contact the terminal helpdesk immediately, remove it from service and keep it available for potential forensics investigation. The merchant or acquirer should also check that the periodic inspections and maintenance are performed by a trusted person and log the periodic checks and maintenance operations, including name of the operator.

Terminal Service Removal

Sensitive data must be erased before refurbishing the terminal or removing it permanently from service. The terminal shall go to tampered status, a state in which sensitive data are erased.

Note: Disassembly of the device will lead to a tampered status.

Terminal Environment Conditions and Environmental Failure Protection

The specified environmental conditions to operate and store the device are:

Operating: -10°C to +45°C / 5% to 90% RH
Storage: -15°C to +70°C / 5% to 90% RH

For safe battery charging, we recommend from 0°C to +40°C / 5% to 90% RH

The security of the terminal is not compromised by altering the environmental conditions (e.g. subjecting the device to temperature or operating voltages outside the stated operating ranges does not alter the security). Any temperature or operating voltage, outside from the values in the table below, will result in a tamper condition:

	Min. value	Max. value
Temperature sensor:	-40 °C	+100 °C
Voltage sensor:	2.8V	4.1V

Table 4

Tamper Response Event

The device contains tamper mechanisms that will trigger when a physical penetration attempt of the device is detected. A merchant or acquirer can easily detect a tampered terminal:

- On front side first LED light continually and fourth LED blinking (Figure 6).
- A characteristic sound is played after power on

Any physical penetration will result in a “tamper event” This event causes the activation of tamper mechanisms that make the device inoperable out of service.

If the device is in tampered state, the merchant or acquirer should contact the terminal’s helpdesk immediately, remove it from service and keep it available for potential forensics investigation.

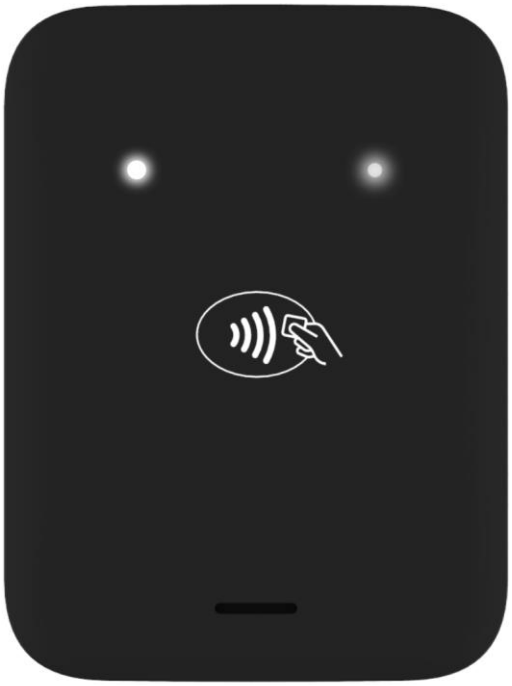

Figure 6 – Device in tampered state

Software Security

NYC1-SCR does not allow unauthorized or unnecessary functions to be executed.

Software Development Guidance

The developer must abide by the coding rules and best practices described in the Application Development Guidelines [4] document.
The security guidance in the Application Development Guidelines [4] document describes how protocols and services must be used/configured for each interface that is available on the platform.
When developing applications, the developer must follow the guidance described in the Application Development Guidelines[4] document for procedural controls to ensure that the applications are properly reviewed, tested and authorized.

The document provides security guidance for account data management.

Signing Mechanisms

Firmware and application images are signed by the Manufacture using different keys. The signing is performed in a secure room. Signing equipment consists of a special Hardware Secure Module, which requires dual control.

The cryptographic algorithms utilized for signing:

- RSA 2048, used for signature verification.
- SHA256, used for calculating hash for data integrity.

Firmware and Application Update

Secure processor updates to the firmware and the application can be loaded in the device. Updates can be performed locally via a host connected to the USB interface after putting the device in download mode (explained in the user manual) or Application using Firmware API (explained in the user manual. Updates are cryptographically authenticated by the terminal. If the authenticity is not confirmed, the update is rejected. The update images are provided by Adyen N.V. to the distributors via email. The distributor will further distribute the update images to the end users. For secure operation of the device, it is recommended to always use the latest version of firmware distributed.

Application Authentication

Application code is authenticated before being allowed to run. The signature of the application code is verified. In case of incorrect signature, the update is rejected. No action is expected from the end user. The signature is based on the RSASSA-PKCS1-V1_5 SHA-256 algorithm and 2048 bit keys. The authenticity is guaranteed by the manufacturer.

Self-Tests

Self-tests are performed upon start up/reset and also periodically once a day. These tests are not initiated by an operator.
Self-tests include:

- Check of integrity and authenticity of the firmware, application and cryptographic keys
- Check of the security mechanisms for sign of tampering

Key Management

Key Loading Policy

The device does not support manual cryptographic key entry. Secure equipment, compliant with key management requirements[5,6,7,8,9], must be used for key injection.

Cryptographic Keys and credentials must be managed under dual control and split knowledge in order to prevent one person using two credentials simultaneously.

Use of the POI with different key management systems will invalidate any PCI approval of this POI.

Key Loading Methods

There are 100 key slots available in the secure firmware of the terminal.

The terminal supports two key loading methods:

- TR-31 Key Derivation Method[7]
- TR-34 Key Derivation Method[13]

Key Usage

- Encrypt/Decrypt Data
- MAC Calculation and Verification

PAN Encryption Techniques

The device implements DUKPT, as specified in ANSI X9.24.

Cryptographic Algorithms

The device supports the following algorithms:

3DES, AES, RSA, SHA

Key Table

KEY NAME	USAGE	ALGORITHM	SIZE (bits)	NUMBER OF AVAILABLE SLOTS
USER KEY	Random key for application data storage	AES	128	1
KEKTR31	Key Loading Key (TR-31 Method)	3DES AES	112/168 128/192/256	100[*1]
KEYMAC	Keys for ISO 9797-1 MAC calculation and verification.	3DES	112	100[*1]
KEYMAC1A	Keys for ISO 16609 MAC calculation and verification.	3DES	112/168	100[*1]
KEYHMAC	Key for HMAC	SHA	256	100[*1]
KEYCMAC	Key for CMAC	AES	128/192/256	100[*1]
KEYDUKPT	Key used for Data and MAC	3DES AES	112 128/192/256	100[*1]
KEYCA	EMV CA Public Keys	RSA	depends on card issuer	100
KEY CA PUB	Certification Authority root key (TR-34)	RSA	2048	1
KEY KEK PRIV	Key encryption private key (TR-34)	RSA	2048	1
KEY KEK PUB	Key encryption public key (TR-34)	RSA	2048	1

Table 5

Notes:

[*1] **Total number of slots available for all 3DES/AES type keys**

Key Replacement

Key replacement must be performed upon any known or suspected compromise of any cryptographic or sensitive information. Any key should be replaced with a new key whenever the compromise of the original key is known or suspected, and whenever the time deemed feasible to determine the key by exhaustive attack elapses. The key replacement can be performed only by the manufacturer.

Terminal Administration

Configuration Settings

The device is functional when received by the merchant or acquirer. No security sensitive configuration settings are necessary to be tuned by the end user to meet security requirements.

Default Value Update

The device is fully functional when received by the merchant or acquirer and there is no security sensitive default value that needs to be changed before operating the device.

Roles and Services

The device has no functionality that gives access to security sensitive services, based on roles. Such services are managed through dedicated tools, using cryptographic authentication.