Trustwave®
Smart security on demand

trustwave.com

# EVALUATION OF PAYMENT APPLICATION DATA SECURITY STANDARD (PA-DSS) ELIGIBILITY WITH CAYAN GENIUS AND CAYAN TRANSPORT

## Prepared for:

CAYAN™

## Date prepared:

15 July 2015

## Prepared by:

Marc Bayerkohler, QSA, PA-QSA, QSA (P2PE), PA-QSA (P2PE)

**CORPORATE HEADQUARTERS**
70 West Madison Street
Suite 1050
Chicago, IL 60602

Tel: +1 (312) 873 7500

**EMEA HEADQUARTERS**
Westminster Tower
3 Albert Embankment
London, SE1 7SP

Tel: +44 (0) 845 456 9611

**ASIA-PACIFIC HEADQUARTERS**
Level 2, 48 Hunter Street
Sydney NSW 2000
Australia

Tel: +61 (0) 2 9236 4200

**LATIN AMERICA HEADQUARTERS**
Rua Cincinato Braga, 340 nº 71 - Edificio Delta Plaza
Bairro Bela Vista - São Paulo - SP
CEP: 01333-010 – BRASIL

Tel: +55 (11) 4064 6101

## Table of Contents

# Executive Summary

Cayan engaged Trustwave, operating under Trustwave Holdings, Inc. (“Trustwave") to conduct an evaluation of how the use of their Cayan Genius or Cayan Transport products could affect PCI scope, in particular the applicability of PA-DSS to other third-party applications which are integrated with Genius or Transport.

The Genius payment platform allows businesses to accept payments using a Customer Engagement Device (CED). This is a hardware device that can collect cardholder data, referred to by the PCI Council as a PIN Entry Device (PED), or sometimes described as a ‘payment terminal’ in the industry. The Cayan Transport is a hosted payment page, which allows businesses to accept payments by entering the cardholder data directly into a web browser.

Both Genius and Transport can work along side and be integrated with other third-party software used by businesses to facilitate purchases. For example, a business may have a Point of Sale (POS) system used by cashiers, or perhaps an application for entering Mail Order / Telephone Order (MOTO) transactions, or an ecommerce presence with a shopping cart. Genius and Transport can be integrated with these third-party applications to enable payment acceptance.

Third-party applications using Genius or Transport can be designed which facilitate payment transactions, but which never come into direct contact with cardholder data themselves. All cardholder data collection, storage, processing, and transmission can be done by the Cayan products, which pass only non-cardholder data such as purchase amount or tokens to the third-party software.

If the third-party software does not store, process, or transmit cardholder data, it is generally determined by the PCI SSC not to be a payment application, and therefore is ineligible for PA-DSS validation.

# Methodology and Scope of Review

Trustwave reviewed Cayan's internal technical documentation and interviewed Cayan engineers and architects to understand the design and function of the systems. No laboratory testing was done.

The following products were in scope for this evaluation:

Cayan Genius™

Cayan Transport™

The products were evaluated using their current versions as of the date of the report. Cayan Genius version 4.3.3.1 specifically was evaluated, but following Cayan's versioning methodology, the evaluation should apply to all 4.3.* versions. The version of Cayan's Store and Forward component evaluated was Build 559.

# Applicability of PA-DSS to Applications

Businesses often rely on third-party payment applications and services providers to facilitate their compliance with the PCI Data Security Standard (PCI DSS). These third-party payment applications must be validated against the Payment Application Data Security Standard (PA-DSS). According to the PCI Security Standards Council (PCI SSC), to be eligible for PA-DSS validation, an application must "store, process, or transmit cardholder data as part of authorization or settlement".

Third-party applications using Genius or Transport can be designed which facilitate payment transactions, but which never come into direct contact with cardholder data themselves. All cardholder data collection, storage, processing, and transmission can be done by the Cayan products, which pass only non-cardholder data such as purchase amount or tokens to the third-party software.

If the third-party software does not store, process, or transmit cardholder data, it is generally determined by the PCI SSC not to be a payment application, and therefore is ineligible for PA-DSS validation. If the third-party software has no contact with cardholder data, and no payment functionality outside of the integration with Genius or Transport, it should not be considered a payment application, and therefore not eligible for PA-DSS validation.

Although it is possible to develop third-party software that is not a payment application, using Genius or Transport does not automatically remove eligibility for PA-DSS. Consult a PA-QSA for an opinion if needed.

## PA-DSS Validation for Genius and Transport

When using Genius, the cardholder data is processed by a Cayan application within the PED. Because of this, it is a payment application eligible for PA-DSS validation. The Cayan Store and Forward Proxy is also an application that processes cardholder data, and is eligible for PA-DSS validation. Cayan is pursuing validation of these applications.

# Common Elements of the Solutions

Some common elements that are used across the different solutions are described here.

## Third-party Software

Third-party software is software package written by a third-party (not Cayan) that facilitates a payment transaction. This software could provide many types of functionality for a business, including:

- Point-of-Sale (POS)
- eCommerce
- Mail Order and Telephone Order (MOTO) entry

## Transport Key

In all of the solutions, a ‘transport key’ is retrieved, either from the Cayan Gateway, or from the Cayan Store and Forward Proxy. The transport key is a unique value used to identify a transaction. It is used, for example, to enable a PED to retrieve information like the purchase amount from the Cayan Gateway. The transport key is never used as an encryption key.

## Cayan Store and Forward Proxy

The Cayan Store and Forward Proxy allows businesses to accept payments when the Cayan Gateway cannot be reached (for example, if the Internet connection has temporarily failed).

## PED Hardware

For Genius, two models of PEDs (PIN Entry Device) are supported, the VeriFone MX 915 and MX 925. Both of these devices are listed as approved by the PCI SSC’s PIN Transaction Security (PTS) program (when used with specific hardware and firmware versions).

# Cardholder Data Flow and Genius

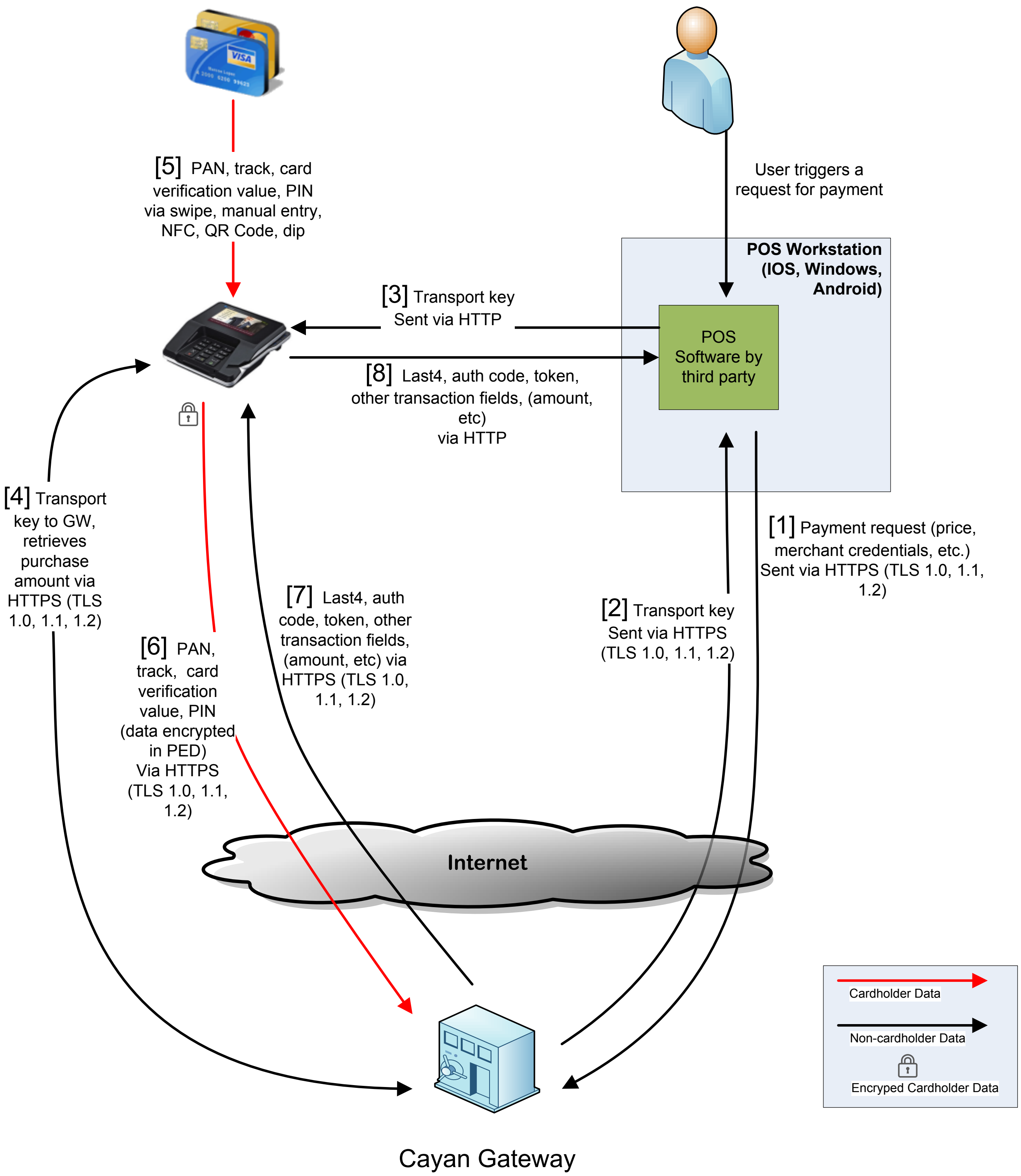
## Genius without Store and Forward

In this solution, a PED is used to collect the cardholder data and transmit it to the Cayan Gateway. The Cayan Store and Forward Proxy is not used, so transactions are not possible when the Cayan Gateway cannot be reached. Note the cardholder data flow in red, which does not touch the third-party software.

### Genius without Store and Forward Transaction Steps

1. The user initiates a transaction, and the third-party software sends a payment request with the amount and other information (but no cardholder data) to the Cayan Gateway.
2. The gateway responds with a transport key.
3. The third-party software sends the transport key to the PED using HTTP.
4. The PED uses the transport key to retrieve the purchase amount from the Cayan Gateway.
5. Cardholder data is collected by the PED and encrypted.
6. The PED sends the encrypted data to the Cayan Gateway protected with HTTPS.
7. The transaction response (e.g., authorized, declined) and other information is sent to the PED.
8. The transaction response and other information is passed back to the third-party software.

## Genius without Store and Forward Diagram


[5] PAN, track, card verification value, PIN via swipe, manual entry, NFC, QR Code, dip
User triggers a request for payment
POS Workstation (IOS, Windows, Android)
[3] Transport key Sent via HTTP
POS Software by third party
[8] Last4, auth code, token, other transaction fields, (amount, etc) via HTTP
[4] Transport key to GW, retrieves purchase amount via HTTPS (TLS 1.0, 1.1, 1.2)
[1] Payment request (price, merchant credentials, etc.) Sent via HTTPS (TLS 1.0, 1.1, 1.2)
[7] Last4, auth code, token, other transaction fields, (amount, etc) via HTTPS (TLS 1.0, 1.1, 1.2)
[2] Transport key Sent via HTTPS (TLS 1.0, 1.1, 1.2)
[6] PAN, track, card verification value, PIN (data encrypted in PED) Via HTTPS (TLS 1.0, 1.1, 1.2)
Internet
Cardholder Data
Non-cardholder Data
Encryped Cardholder Data
Cayan Gateway

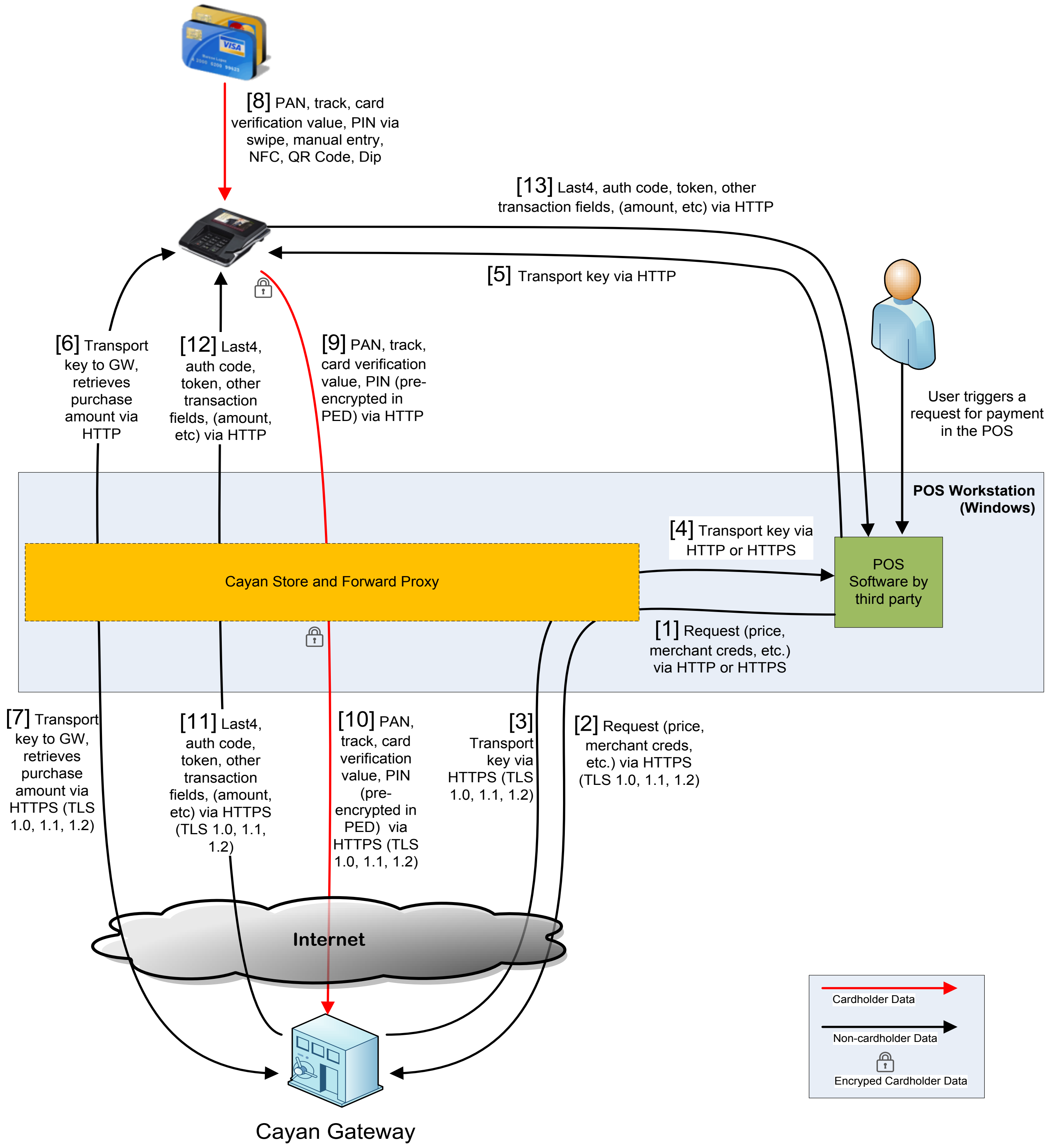
## Genius with Store and Forward – Online Mode

In this solution, a PED collects the cardholder data and passes it to the Cayan Store and Forward Proxy, which sends it to the Cayan Gateway. Note the cardholder data flow in red, which does not touch the third-party POS software.

### Genius with Store and Forward – Online Mode Transaction Steps

1. The user initiates a transaction, and the third-party POS sends a payment request with the amount and other information (but no cardholder data) to the Cayan Store and Forward Proxy.
2. The Cayan Store and Forward Proxy sends the request to the Cayan Gateway.
3. The gateway responds with a transport key.
4. The transport key is given to the third-party software.
5. The third-party software sends the transport key to the PED using HTTP.
6. The PED uses the transport key to ask the Cayan Store and Forward Proxy for purchase information.
7. The Cayan Store and Forward Proxy retrieves the purchase information from the Cayan Gateway, and passes it to the PED.
8. Cardholder data is collected by the PED and encrypted.
9. The PED sends the encrypted data to the Cayan Store and Forward Proxy.
10. The Cayan Store and Forward Proxy sends the encrypted data to the Cayan Gateway protected with HTTPS.
11. The transaction response (e.g., authorized, declined) and other information are sent to the Cayan Store and Forward Proxy.
12. The Cayan Store and Forward Proxy passes the transaction response back to the PED.
13. The PED then passes the transaction response back to the third-party software.

## Genius with Store and Forward – Online Mode Diagram


[8] PAN, track, card verification value, PIN via swipe, manual entry, NFC, QR Code, Dip
[13] Last4, auth code, token, other transaction fields, (amount, etc) via HTTP
[5] Transport key via HTTP
[6] Transport key to GW, retrieves purchase amount via HTTP
[12] Last4, auth code, token, other transaction fields, (amount, etc) via HTTP
[9] PAN, track, card verification value, PIN (pre-encrypted in PED) via HTTP
User triggers a request for payment in the POS
POS Workstation (Windows)
[4] Transport key via HTTP or HTTPS
POS Software by third party
Cayan Store and Forward Proxy
[1] Request (price, merchant creds, etc.) via HTTP or HTTPS
[7] Transport key to GW, retrieves purchase amount via HTTPS (TLS 1.0, 1.1, 1.2)
[11] Last4, auth code, token, other transaction fields, (amount, etc) via HTTPS (TLS 1.0, 1.1, 1.2)
[10] PAN, track, card verification value, PIN (pre-encrypted in PED) via HTTPS (TLS 1.0, 1.1, 1.2)
[3] Transport key via HTTPS (TLS 1.0, 1.1, 1.2)
[2] Request (price, merchant creds, etc.) via HTTPS (TLS 1.0, 1.1, 1.2)
Internet
Cayan Gateway
Cardholder Data
Non-cardholder Data
Encryped Cardholder Data

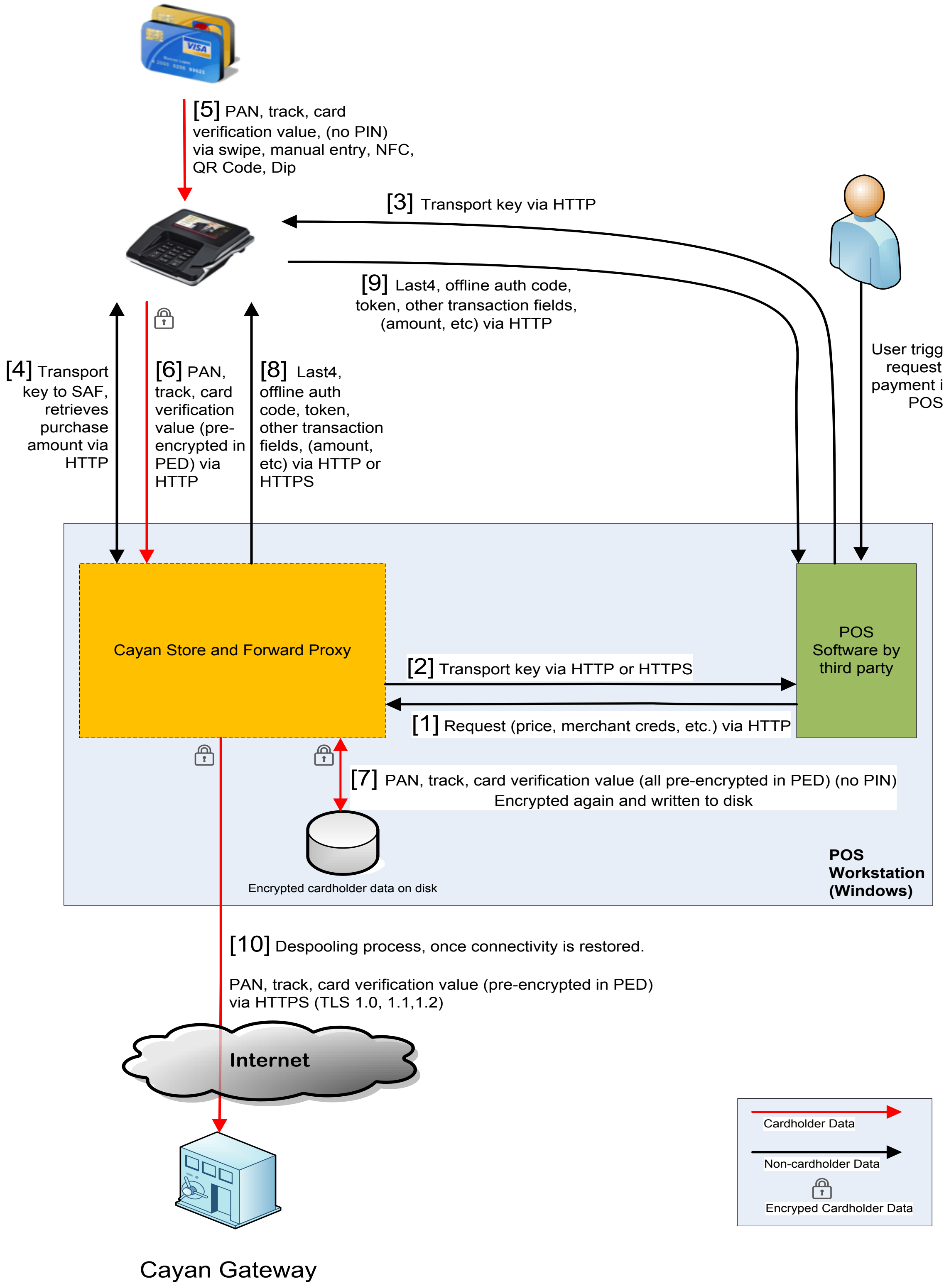
## Genius with Store and Forward – Offline Mode

In this solution, a PED collects the cardholder data and passes it to the Cayan Store and Forward Proxy, which stores it locally until the Cayan Gateway can be reached. Note the cardholder data flow in red, which does not touch the third-party POS software.

### Genius with Store and Forward – Offline Mode Transaction Steps

1. The user initiates a transaction, and the third-party POS sends a payment request with the amount and other information (but no cardholder data) to the Cayan Store and Forward Proxy.
2. The Cayan Store and Forward Proxy responds with a simulated transport key.
3. The transport key is given to the third-party software.
4. The PED uses the transport key retrieve the purchase information from the Cayan Store and Forward Proxy.
5. Cardholder data is collected by the PED and encrypted.
6. The PED sends the encrypted data to the Cayan Store and Forward Proxy.
7. The Cayan Store and Forward Proxy encrypts the cardholder data a second time and stores it on disk.
8. A simulated transaction response (e.g., authorized, declined) and other information are sent to the third-party software.
9. Once connectivity to the Cayan Gateway is restored, the Cayan Store and Forward Proxy sends the cardholder data protected by HTTPS.

## Genius with Store and Forward – Offline Mode Diagram


[5] PAN, track, card verification value, (no PIN) via swipe, manual entry, NFC, QR Code, Dip
[3] Transport key via HTTP
[9] Last4, offline auth code, token, other transaction fields, (amount, etc) via HTTP
User triggers a request for payment in the POS
[4] Transport key to SAF, retrieves purchase amount via HTTP
[6] PAN, track, card verification value (pre-encrypted in PED) via HTTP
[8] Last4, offline auth code, token, other transaction fields, (amount, etc) via HTTP or HTTPS
Cayan Store and Forward Proxy
POS Software by third party
[2] Transport key via HTTP or HTTPS
[1] Request (price, merchant creds, etc.) via HTTP
[7] PAN, track, card verification value (all pre-encrypted in PED) (no PIN) Encrypted again and written to disk
Encrypted cardholder data on disk
POS Workstation (Windows)
[10] Despooling process, once connectivity is restored.
PAN, track, card verification value (pre-encrypted in PED) via HTTPS (TLS 1.0, 1.1,1.2)
Internet
Cayan Gateway
Cardholder Data
Non-cardholder Data
Encryped Cardholder Data

# Cardholder Data Flow and Transport

## Transport without Store and Forward

In this solution, a web browser is used to collect the cardholder data and transmit it to the Cayan Hosted Payment Page. The Cayan Store and Forward Proxy is not used, so transactions are not possible when the Cayan Hosted Payment Page cannot be reached. Note the cardholder data flow in red, which does not touch the third-party software.

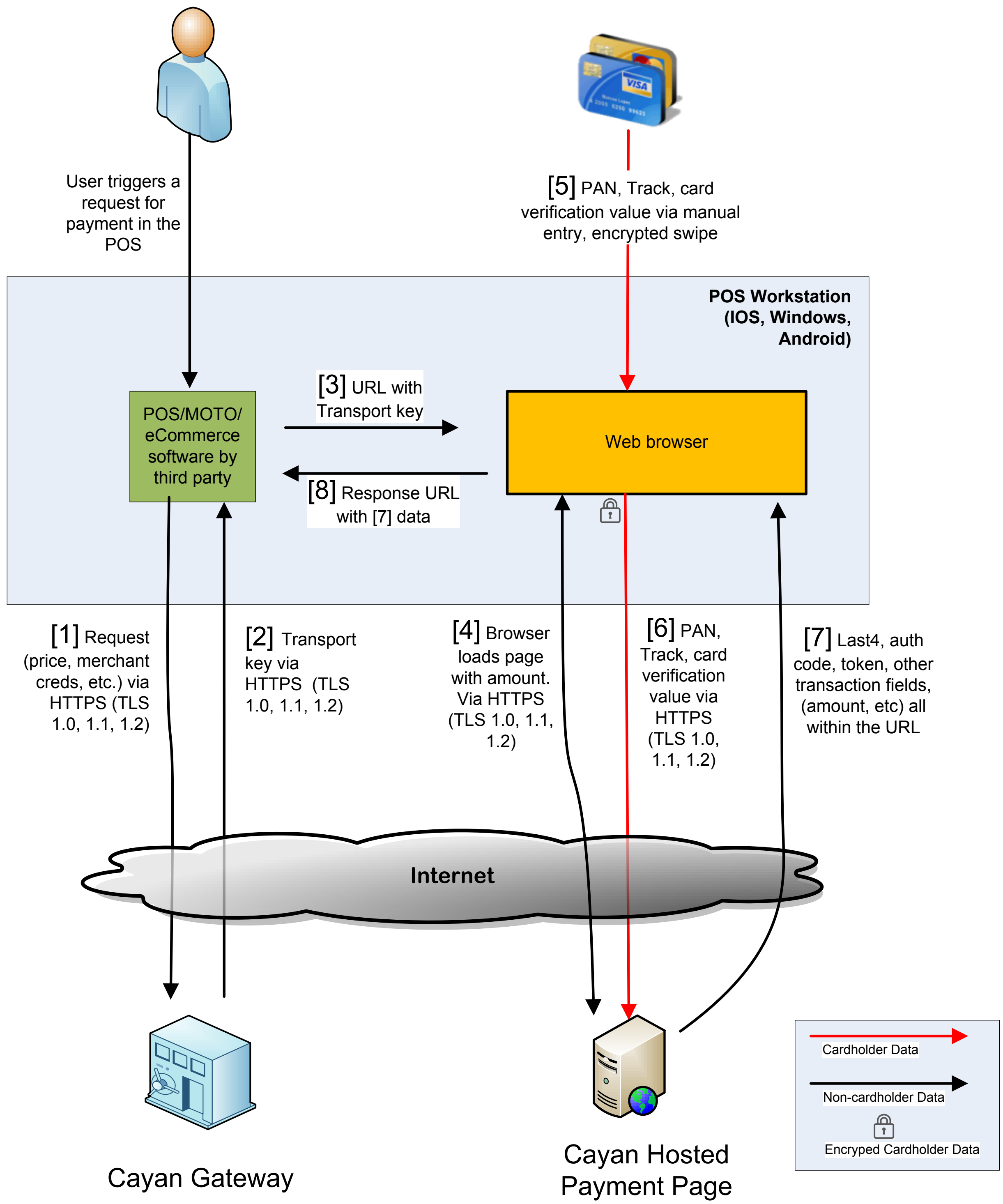
When the Cayan Store and Forward software is not present, and cardholder data is only entered directly into a browser connected to the Cayan Hosted Payment Page, Transport meets the definition of "software as a service" (SaaS) as defined by the PCI SSC in the 'Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS) v3.0 Program Guide Version 3.0', section '4.1 To Which Applications Does PA-DSS Apply?'. As such, Transport is not eligible for PA-DSS validation.

Cayan's internal processing platform and payment technologies (including Transport) are validated on an annual basis for PCI DSS compliance.

### Transport without Store and Forward Transaction Steps

1. The user initiates a transaction, and the third-party software sends a payment request with the amount and other information (but no cardholder data) to the Cayan Gateway.
2. The gateway responds with a transport key.
3. The third-party software sends the transport key to the web browser within a URL.
4. The web browser uses the transport key to load the correct payment page.
5. Cardholder data is entered into the browser.
6. The browser sends the cardholder data to the Cayan Hosted Payment Page protected with HTTPS.
7. The transaction response (e.g., authorized, declined) and other information are returned to the browser.
8. The transaction response and other information are passed back to the third-party software within a URL.

## Transport without Store and Forward Diagram


User triggers a request for payment in the POS
[5] PAN, Track, card verification value via manual entry, encrypted swipe
POS Workstation (IOS, Windows, Android)
POS/MOTO/ eCommerce software by third party
[3] URL with Transport key
Web browser
[8] Response URL with [7] data
[1] Request (price, merchant creds, etc.) via HTTPS (TLS 1.0, 1.1, 1.2)
[2] Transport key via HTTPS (TLS 1.0, 1.1, 1.2)
[4] Browser loads page with amount. Via HTTPS (TLS 1.0, 1.1, 1.2)
[6] PAN, Track, card verification value via HTTPS (TLS 1.0, 1.1, 1.2)
[7] Last4, auth code, token, other transaction fields, (amount, etc) all within the URL
Internet
Cayan Gateway
Cayan Hosted Payment Page
Cardholder Data
Non-cardholder Data
Encryped Cardholder Data

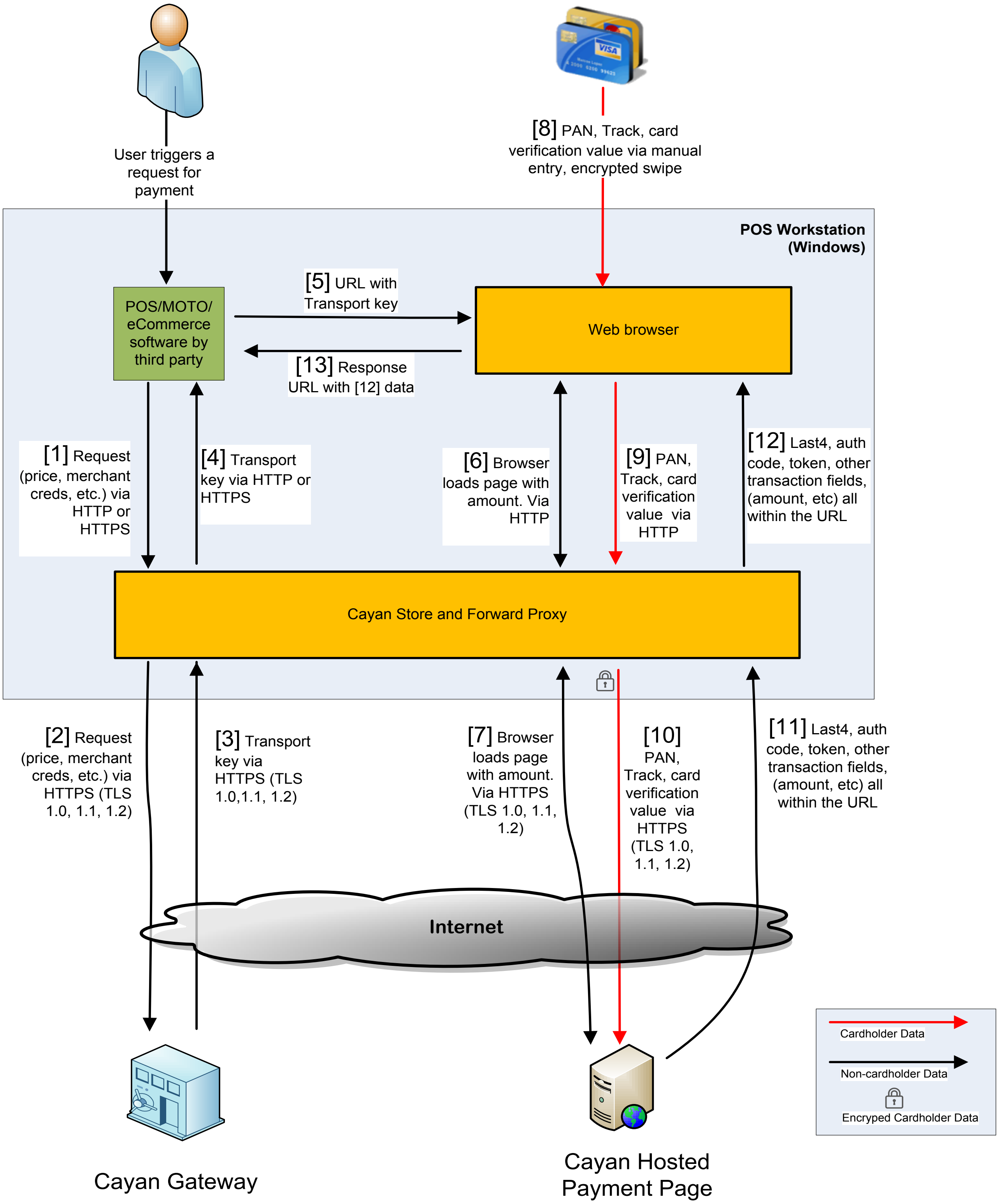
## Transport with Store and Forward – Online Mode

In this solution, a web browser is used to collect the cardholder data and transmit it to the Cayan Store and Forward Proxy, which passes it to the Cayan Hosted Payment Page. Note the cardholder data flow in red, which does not touch the third-party software.

### Transport with Store and Forward – Online Mode Transaction Steps

1. The user initiates a transaction, and the third-party POS sends a payment request with the amount and other information (but no cardholder data) to the Cayan Store and Forward Proxy.
2. The Cayan Store and Forward Proxy sends the request to the Cayan Gateway.
3. The gateway responds with a transport key.
4. The transport key is given to the third-party software.
5. The third-party software sends the transport key to the browser within a URL.
6. The browser users the transport key to ask the Cayan Store and Forward Proxy for purchase information.
7. The Cayan Store and Forward Proxy retrieves the purchase information from the Cayan Hosted Payment Page, and passes it to the browser.
8. Cardholder data is entered into the browser.
9. The browser sends the cardholder data to the Cayan Store and Forward Proxy.
10. The Cayan Store and Forward Proxy sends the cardholder data to the Cayan Hosted Payment Page protected with HTTPS.
11. The transaction response (e.g., authorized, declined) and other information are sent to the Cayan Store and Forward Proxy.
12. The Cayan Store and Forward Proxy passes the transaction response back to the browser.
13. The transaction response and other information are passed back to the third-party software within a URL.

## Transport with Store and Forward – Online Mode Diagram


User triggers a request for payment
[8] PAN, Track, card verification value via manual entry, encrypted swipe
POS Workstation (Windows)
POS/MOTO/ eCommerce software by third party
[5] URL with Transport key
Web browser
[13] Response URL with [12] data
[1] Request (price, merchant creds, etc.) via HTTP or HTTPS
[4] Transport key via HTTP or HTTPS
[6] Browser loads page with amount. Via HTTP
[9] PAN, Track, card verification value via HTTP
[12] Last4, auth code, token, other transaction fields, (amount, etc) all within the URL
Cayan Store and Forward Proxy
[2] Request (price, merchant creds, etc.) via HTTPS (TLS 1.0, 1.1, 1.2)
[3] Transport key via HTTPS (TLS 1.0,1.1, 1.2)
[7] Browser loads page with amount. Via HTTPS (TLS 1.0, 1.1, 1.2)
[10] PAN, Track, card verification value via HTTPS (TLS 1.0, 1.1, 1.2)
[11] Last4, auth code, token, other transaction fields, (amount, etc) all within the URL
Internet
Cardholder Data
Non-cardholder Data
Encrypted Cardholder Data
Cayan Gateway
Cayan Hosted Payment Page

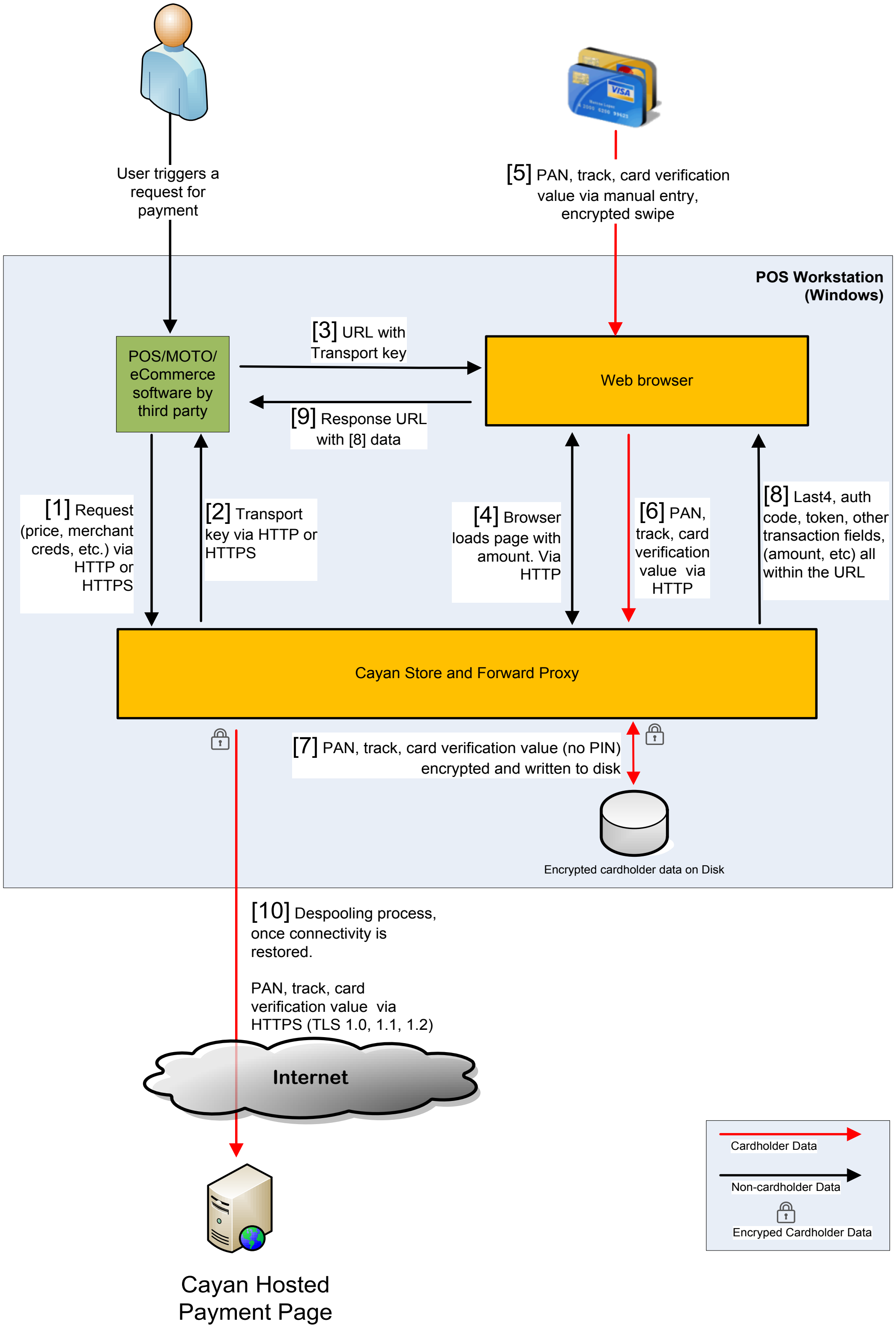
## Transport with Store and Forward – Offline Mode

In this solution, a web browser is used to collect the cardholder data and transmit it to the Cayan Store and Forward Proxy, which stores it locally until the Cayan Hosted Payment Page can be reached. Note the cardholder data flow in red, which does not touch the third-party software.

### Transport with Store and Forward – Offline Mode Transaction Steps

1. The user initiates a transaction, and the third-party POS sends a payment request with the amount and other information (but no cardholder data) to the Cayan Store and Forward Proxy.
2. The Cayan Store and Forward Proxy responds with a simulated transport key.
3. The transport key is given to the browser within a URL.
4. The browser uses the transport key retrieve the purchase information from the Cayan Store and Forward Proxy.
5. Cardholder data is entered into the browser.
6. The browser sends the cardholder data to the Cayan Store and Forward Proxy.
7. The Cayan Store and Forward Proxy encrypts the cardholder data and stores it on disk.
8. A simulated transaction response (e.g., authorized, declined) and other information are sent to the browser.
9. Once connectivity to the Cayan Hosted Payment Page is restored, the Cayan Store and Forward Proxy sends the cardholder data protected by HTTPS.

## Transport with Store and Forward – Offline Mode Diagram


User triggers a request for payment
[5] PAN, track, card verification value via manual entry, encrypted swipe
POS Workstation (Windows)
POS/MOTO/ eCommerce software by third party
[3] URL with Transport key
Web browser
[9] Response URL with [8] data
[1] Request (price, merchant creds, etc.) via HTTP or HTTPS
[2] Transport key via HTTP or HTTPS
[4] Browser loads page with amount. Via HTTP
[6] PAN, track, card verification value via HTTP
[8] Last4, auth code, token, other transaction fields, (amount, etc) all within the URL
Cayan Store and Forward Proxy
[7] PAN, track, card verification value (no PIN) encrypted and written to disk
Encrypted cardholder data on Disk
[10] Despooling process, once connectivity is restored.
PAN, track, card verification value via HTTPS (TLS 1.0, 1.1, 1.2)
Internet
Cayan Hosted Payment Page
Cardholder Data
Non-cardholder Data
Encryped Cardholder Data

# Encryption of Cardholder Data

Cardholder data at rest is always protected by strong cryptography.

## Encryption by Genius

With Genius, cardholder data is encrypted within the PED. The encryption is done by a Cayan application running on the PED, and is accomplished using VeriFone-provided encryption libraries. Cayan's application is not part of the PED's firmware. The PED itself is a tamper-resistant device which is PCI PTS (PIN Transaction Security) approved. Cayan's application was not evaluated as part of the PTS approval.

The cardholder data is encrypted with a data-encryption-key (DEK), which is a 256 bit AES symmetric key that is unique-per-transaction. The DEK is generated using a pseudo random number generator. The DEK is encrypted with a key-encrypting-key (KEK), which is a 2048 bit RSA asymmetric key. The encrypted DEK is included with the encrypted cardholder data sent to Cayan, and can only be decrypted in the Cayan datacenter using their private key.

## Encryption by Transport

With Transport, cardholder data is encrypted by the Cayan Store and Forward Proxy. The encryption is done using the Microsoft .NET 4/4.5 framework. The cardholder data is encrypted with a data-encryption-key (DEK), which is a 256 bit AES symmetric key that is unique-per-transaction. The DEK is generated using a pseudo random number generator. The DEK is encrypted with a key-encrypting-key (KEK), which is a 2048 bit RSA asymmetric key. The encrypted DEK is included with the encrypted cardholder data sent to Cayan, and can only be decrypted in the Cayan datacenter using their private key.