PCI Software Security Framework (SSF) Implementation Guide

for

Credit Authorization Gateway Engine (CAGE) Secure

Version 1.1

Innovative Control Systems, Inc.

November 16, 2022

Table of Contents

Revision History

Name	Date	Reason For Changes	Reviewed By	Version
Shamprasad D.	09/07/2022	Original Doc for PCI SSF		1.0
Shamprasad D.	10/25/2022	Incorporated QSA recommended changes	Rich H. Kris R.	1.1

Important

The Payment Card Industry (PCI) Software Security Framework (SSF) implementation guide must be updated whenever there are changes to CAGE Secure application that affect the PCI SSF requirements, reviewed annually, and update as needed. Annual review of the implementation guide must account for any changes to PCI SSF requirements which may require updating the document as needed.

1. Introduction

1.1 Purpose

PCI SSF is comprised of a Secure Software Life Cycle (SLC) Standard v1.1 and a Secure Software Standard v1.1 requirements for software vendors to develop secure payment applications. PCI SLC defines a set of security requirements along with assessment procedures and guidance to help software vendors design, develop, and maintain secure software throughout the software lifecycle. PCI Secure Software Standard defines a set of security requirements, with corresponding assessment procedures, guidance for adequately protecting the integrity and confidentiality of sensitive data and payment transactions.

This PCI SSF implementation guide applies to you, if you are using the CAGE Secure application in your business to store, process or transmit payment card information. The implementation guide includes information on the CAGE Secure application, installation, security, configuration, operation, and security of payment card transactions in your business.

The purpose of this document is to ensure how the CAGE Secure application meets all the PCI SSF standards. More importantly, this document gives guidelines for merchants/customers on installation and operation of the CAGE Secure payment application, and how to securely handle cardholder data in a card data environment to facilitate PCI compliance efforts.

Merchants/Customers who use payment applications and handle payment card information must comply with PCI DSS standards. Failure to comply with standards can result in legal action and heavy fines if a security breach occurs. For more details on PCI security standards, please visit the below PCI website link.
https://www.pcisecuritystandards.org/

1.2 Document Use

This document is intended for merchants/customers who use the PCI SSF approved CAGE Secure application. The PCI SSF implementation guide provides proper installation, configuration, and use of the ICS CAGE Secure application in a payment system to securely handle cardholder data. Using the PCI SSF approved payment application and having this implementation guide does not make a merchant PCI compliant. It is the responsibility of merchants/customers who use the CAGE Secure application to go through PCI DSS assessment to become PCI compliant.

1.3 Acronyms

CAGE	Credit Authorization Gateway Engine
DSS	Data Security Standards
E2EE	End-to-End Encrypted
EMV	Europay, Master Card and Visa
ICS	Innovative Control Systems
PA QSA	Payment Application Qualified Security Assessor
PAN	Primary Account Number
PCI	Payment Card Industry
POS	Point of Sale
SSC	Security Standards Council

SLC Software Life Cycle
SSF Software Security Framework
SSS Secure Software Standard

1.4 References

This document is written in accordance with Secure Software Requirements and Assessment Procedures Version 1.1 documentation which can be found on the below link.
https://www.pcisecuritystandards.org/document_library

2. Difference between PCI Compliance and SSF

As a software vendor who develops payment applications, our responsibility is to be "PCI SSF Validated." We have performed an assessment and payment application validation review with our independent assessment firm Payment Application Qualified Security Assessor (PA-QSA), to ensure that our platform does conform to industry best practices when handling, managing, and storing payment related information.

PCI SSF is the standard against which Payment Application has been tested, assessed, and validated.

PCI Compliance is then later obtained by the merchant and is an assessment of your actual server (or hosting) environment called the Cardholder Data Environment (CDE).

Obtaining "PCI Compliance" is the responsibility of you, the merchant, and your hosting provider, working together, using PCI compliant architecture with proper hardware and software configurations and access control procedures.

The PCI SSF Validation is intended to ensure that the CAGE Secure Application will help you facilitate and maintain PCI Compliance with respect to how the payment application handles user accounts, passwords, encryption, and other payment data related information.

The PCI has developed security standards for handling cardholder information in a published standard called the PCI DSS. The security requirements defined in the DSS apply to all members, merchants, and service providers that store, process, or transmit cardholder data.

The PCI DSS requirements apply to all system components within the payment application environment which is defined as any network device, host, or application included in, or connected to, a network segment where cardholder data is stored, processed, or transmitted.

3. The 12 Requirements of the PCI DSS

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

4. Application Summary

Name	**CAGE Secure**
Version Number	**6.2.1.1**
Operating System	**Windows 10, Windows 11**
Code Base	**.Net, C#**
Application Description	CAGE Secure is a Windows based .Net application that communicates to a secure PCI PTS certified SRED card reader device and receives encrypted card holder data and transmits to the processor for authorization. The application is a middleware that resides in each of the unattended POS systems.
Application Environment	The CAGE Secure application is used by ICS unattended POS products which require credit authorization to accept payments from end users who purchase a car wash service. ICS unattended POS products are sold to individuals and corporate car wash owners.
Hardware Required	There are 2 sets of separate hardware certified with Fiserv processor. 1. Verifone UX Series • UX300 Card reader • UX400 NFC • UX100 PINPad 2. IDTech VP5300 Series • VP5300 Card reader • VP5300 NFC • SmartPIN L100 The below hardware set is certified with Heartland processor. 1. IDTech VP5300 Series • VP5300 Card reader • VP5300 NFC •

5. Responsible Parties

5.1 Customers

Customers are merchants, service providers, or others who buy or receive the CAGE Secure application to store, process, or transmit cardholder data as part of authorizing or settling of payment transactions.
Customers are responsible for:

- Implementing a PCI SSF compliant CAGE Secure application into a PCI DSS compliant environment.
- Configuring the CAGE Secure application (where configuration options are provided) according to the CAGE Secure application PCI SSF Implementation Guide provided by the vendor.
- Configuring the CAGE Secure application in a PCI DSS compliant manner.
- Maintaining the PCI DSS compliant status for both the environment and the CAGE Secure application configuration

5.2 Resellers and Integrators

Resellers and integrators are those entities that sell, install, and/or service payment applications on behalf of software vendors or others. Resellers and integrators are responsible for:

- Implementing a PCI SSF compliant CAGE Secure application into a PCI DSS compliant environment.
- Configuring the CAGE Secure application (where configuration options are provided) according to the CAGE Secure application PCI SSF Implementation Guide provided by the vendor.
- Configuring the CAGE Secure application in a PCI DSS compliant manner.
- Servicing the CAGE Secure application (for example, troubleshooting, delivering remote updates, and providing remote support) according to the CAGE Secure application PCI SSF Implementation Guide and PCI DSS.

5.3 Vendors

Vendors are those who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, and then sell, distribute, or license these payment applications to third parties (customers or resellers/integrators). Vendors are responsible for:

- Creating PCI SSF compliant CAGE Secure application that will facilitate and does not prevent their customers' PCI DSS compliance. (The CAGE Secure application should not require an implementation or configuration setting that violates a PCI DSS requirement.).
- Following PCI DSS requirements whenever storing, processing, or transmitting cardholder data (for example, during customer troubleshooting).
- Creating a CAGE Secure application Implementation Guide, specific to each payment application.

- Educating customers, resellers, and integrators on how to install and configure the CAGE Secure application in a PCI DSS compliant manner.
- Ensuring the CAGE Secure application meets PCI SSF standards by successfully passing a PCI SSF QSA review as specified in this document.

6. Payment Application in a PCI Compliant Environment

The following areas must be considered for proper implementation in a PCI compliant environment.

- Remove Historical Sensitive Authentication Data
- Handling of Sensitive Authentication Data
- Secure Deletion of Cardholder Data
- All PAN information is masked by default
- Cardholder Data Encryption & Key Management
- Removal of Historical Cryptographic Material

7. Card Data Environment Network Diagram

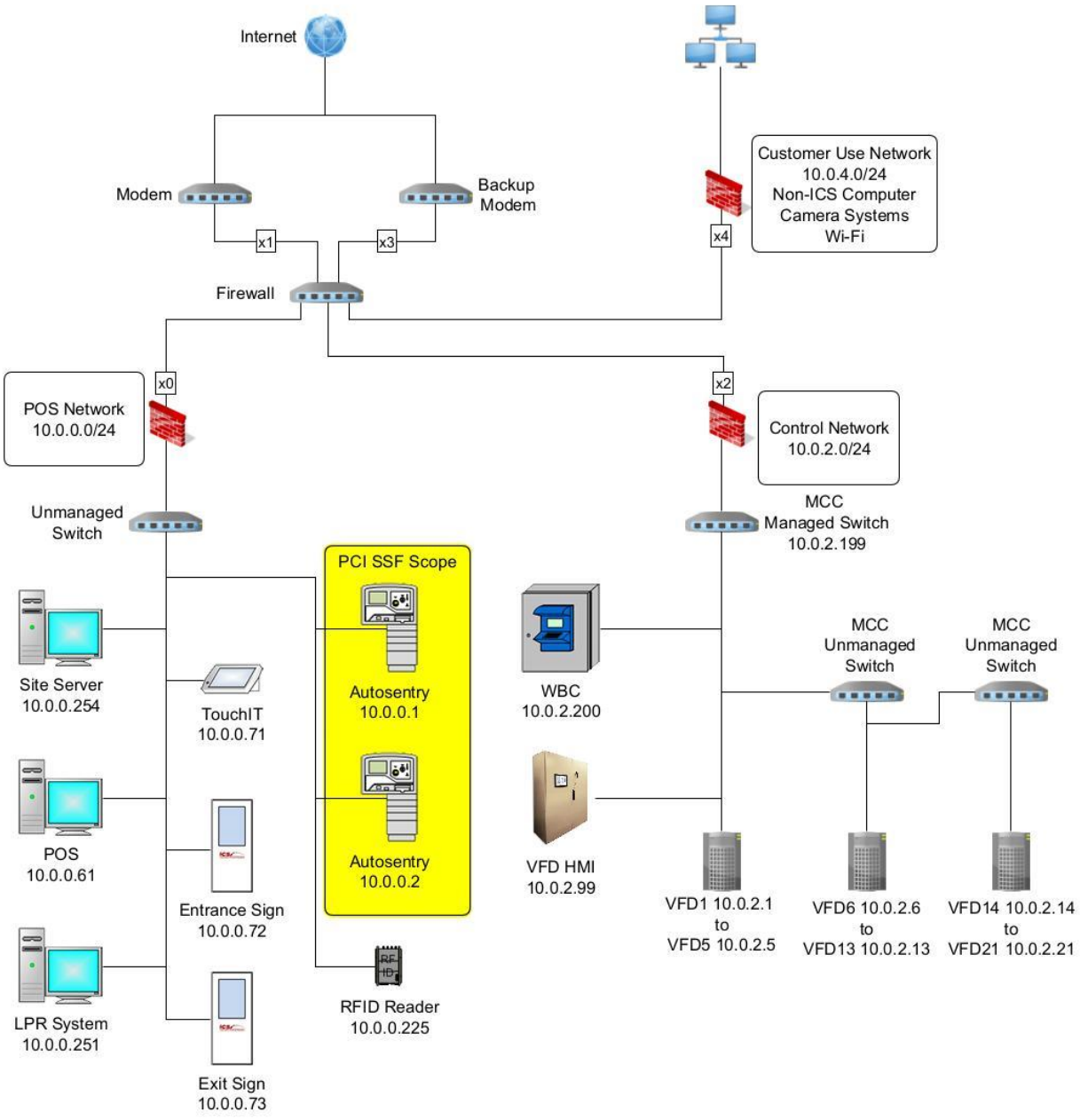


Figure 1 Card Data Environment Network Diagram

The Figure 1 above shows typical car wash environment where 2 or more unattended POS systems (AutoSentry®) are deployed. The card data environment is segmented, and all the card data flow goes directly to the processor. The management, controller and other device traffic is all separate which does not cross the card data environment.

8. End-to-End Encryption Dataflow Diagram

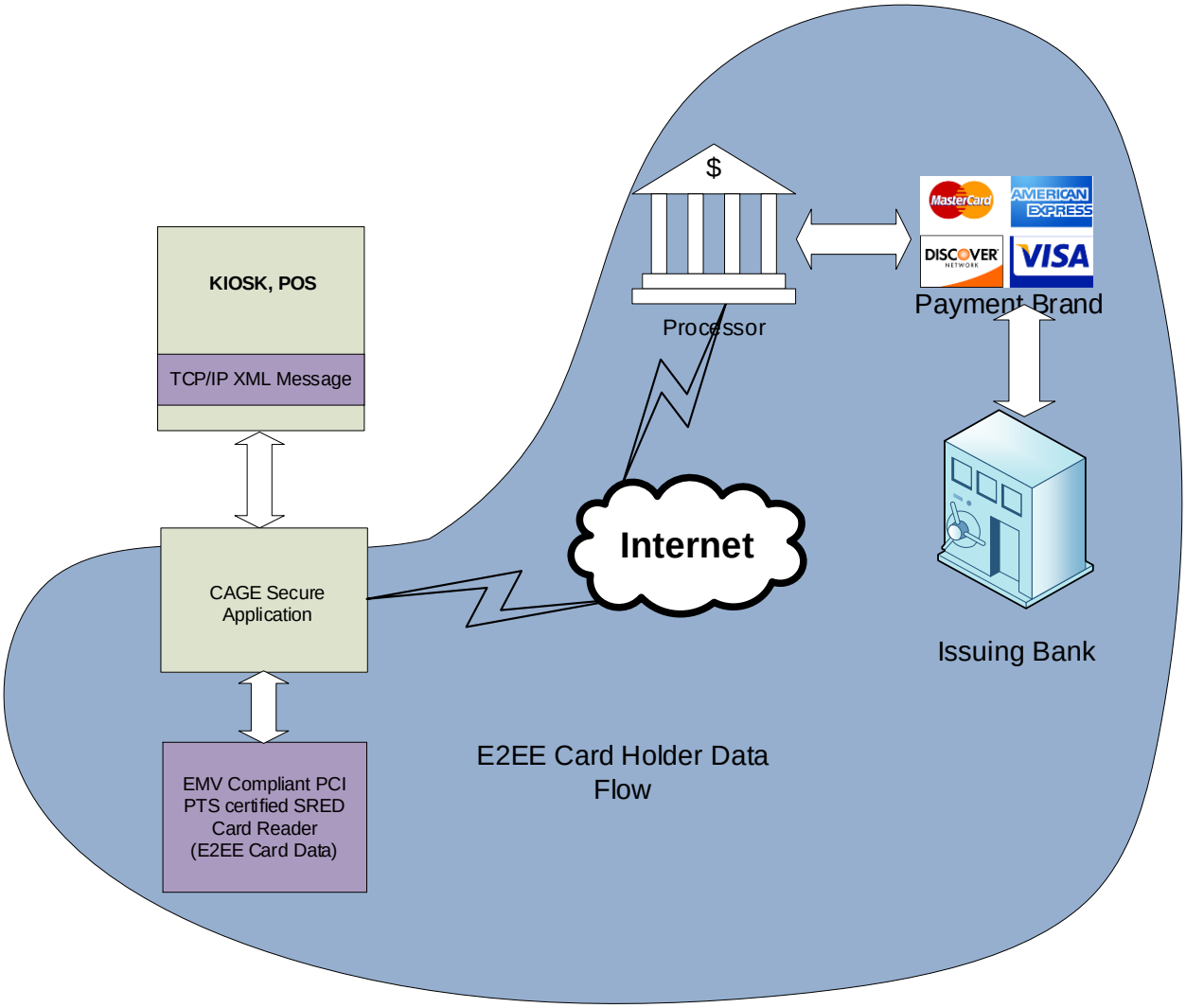


Figure 2: E2EE Credit Card Processing Dataflow Diagram

The Figure 2 above shows secure End-to-End Encrypted (E2EE) credit card processing data flow diagram, where the card holder data is encrypted at the card reader device and transported to processor over the network using secure transport connection.

9. Application Architecture

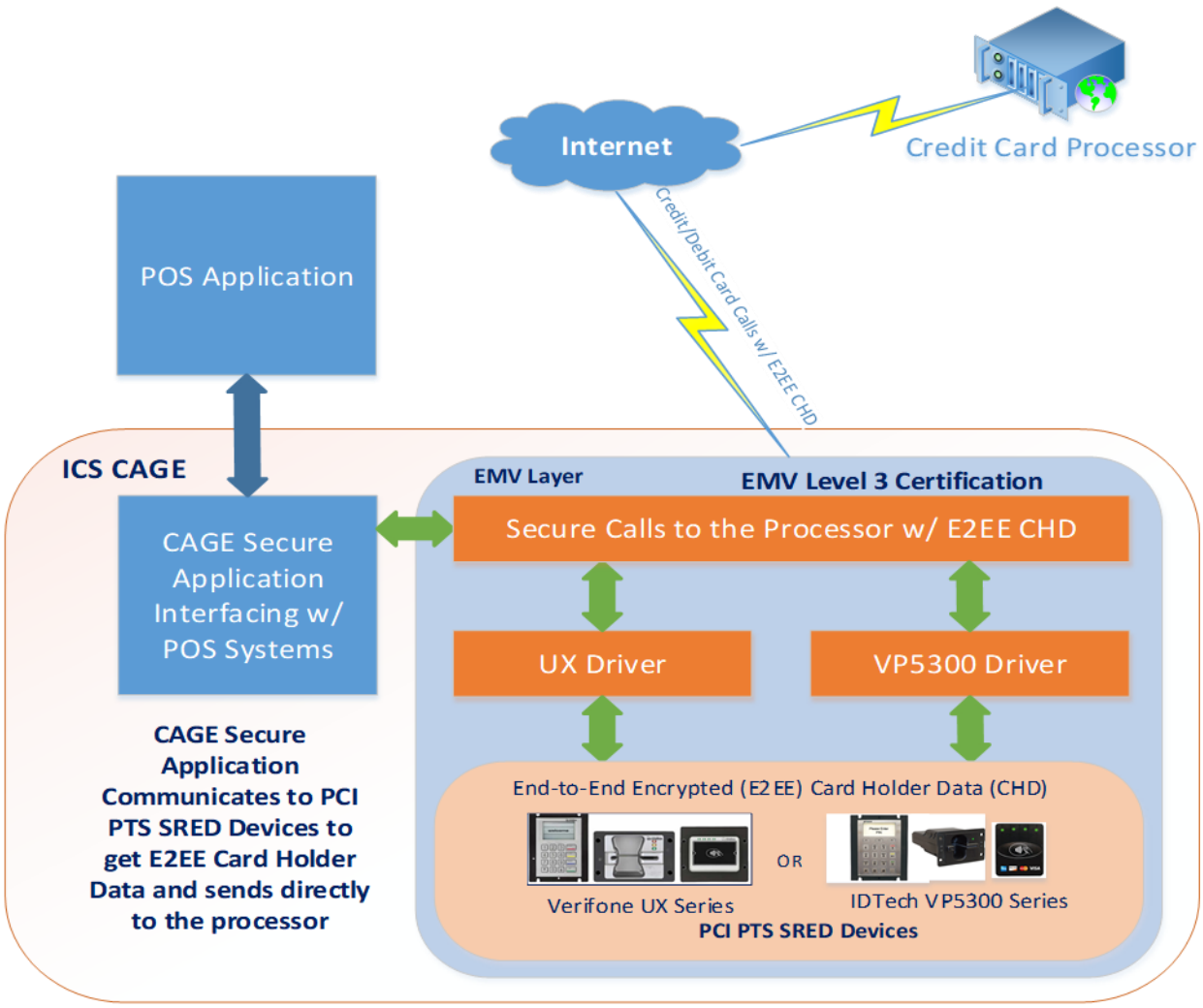


Figure 3: CAGE Secure Software Architecture

Figure 3 above shows the internal high-level architecture of the CAGE Secure application. The CAGE Secure interfaces with POS systems to accept Authorize, Void and Refund.

10. Conformance to SSF SSS Control Objectives

This summary provides overview of the PCI SSF Secure Software Standard (SSS) control objectives that are related to Implementation Security Guidance. It also explains how the Control Objective is achieved / handled in the application side and required actions for you (as a customer). The complete PCI DSS and Secure Software Standard documentation can be found at: http://www.pcisecuritystandards.org.

10.1 Control Objective 1.2.c

Sensitive functions or sensitive resources are provided by third-party software or systems	
Software Vendor conformance	CAGE Secure application uses IDTech VP5300 third-party PTS hardware and device drivers as sensitive resources. The PTS hardware and CAGE application interaction with the PTS devices are configured as per the security policy of PTS.
Guidance to merchant/customer	The merchant/customer is not required to take any action for this requirement.

10.2 Control Objective 2.1.a and 2.1.e

All functions exposed by the software are enabled by default only when and where it is a documented and justified part of the software architecture	
Software Vendor conformance	CAGE Secure application is packaged with the ICS POS payment application and installed by ICS support technician. CAGE Secure application does not expose any functions or services or protocols. CAGE Secure application does not use any insecure or unnecessary protocols. CAGE Secure is certified for Fiserv processor for Verifone UX series and IDTech VP5300 series hardware sets and Heartland processor for IDTech VP5300 series set.
Guidance to merchant/customer	The merchant/customer is not required to take any action for this requirement. Customers are advised not to enable any services, protocols, or ports which are insecure. For guidance on services,

	protocols, or ports considered to be insecure, refer to industry standards and guidance.

10.3 Control Objective 2.2

All software security controls, features, and functions are enabled upon software installation, initialization, or first use	
Software Vendor conformance	The CAGE Secure application is packaged with the ICS POS payment application and installed by ICS support technician. Security controls, features and application functions and its configuration is enabled during initial installation of the application by ICS support technician.
Guidance to merchant/customer	The merchant/customer is not required to take any action for this requirement.

10.4 Control Objective 2.3

Default authentication credentials or keys for built-in accounts are not used after installation, initialization, or first use	
Software Vendor conformance	Default login account is required for the CAGE Secure application. The login is protected by a password generated from ICS support team on demand. Default login has privilege to add users and configure CAGE as required. Customer using the CAGE Secure application create a unique user account. It enforces secure authentication for all authentication credentials that the application generates by: • Enforcing secure changes to authentication credentials by the completion of installation. • Enforcing secure changes for any subsequent changes to authentication credentials.
Guidance to merchant/customer	Default administrative accounts, groups or passwords are not required for any functioning of application. The merchant/customer should allow only authorized access to computer which runs the CAGE Secure application.

10.5 Control Objective 2.4

The privileges and resources requested by the software from its execution environment are limited to those necessary for the operation of the software	
Software Vendor conformance	CAGE Secure application runs in Windows OS platform and does not require any elevated privileges to run.
Guidance to merchant/customer	The merchant/customer is not required to take any action for this requirement.

10.6 Control Objective 3.1

The software only retains the sensitive data necessary for the software to provide its intended functionality	
Software Vendor conformance	CAGE Secure application retains the following sensitive data that is necessary for the business operations. 1. Merchant ID 2. Authentication data 3. Last 4 digits of PAN. CAGE Secure application does not retain any transient sensitive data. CAGE Secure application does not retain any sensitive card holder data as it is E2EE encrypted at the PCI PTS SRED card reader. The configuration information which is required for merchant account setup is stored encrypted on the terminal.
Guidance to merchant/customer	The merchant/customer is not required to take any action for this requirement.

10.7 Control Objective 3.3

The software protects the confidentiality and integrity of sensitive data (both transient and persistent) during retention	
Software Vendor conformance	CAGE Secure application does not retain any transient sensitive data. CAGE Secure application retains and protects the following sensitive data. 1. The merchant ID is stored in an encrypted configuration file. 2. The authentication data is stored in an encrypted configuration file. 3. The Last 4 digit of PAN (stored in clear text as there is no need for confidentiality and integrity protection).
Guidance to merchant/customer	The merchant/customer is not required to take any action for this requirement. The protection methods are an integral module of the CAGE Secure application. Customers are not required to configure protection methods.

10.8 Control Objective 3.6

The software does not disclose sensitive data through unintended channels	
Software Vendor conformance	CAGE Secure application is tested for data disclosure attack vectors such as Error messages, all kind of logs, system memory dump, third-party services, etc. The critical sensitive card holder data as it is E2EE encrypted at the PCI PTS SRED card reader. CAGE Secure application doesn't have access to clear PAN.
Guidance to merchant/customer	The merchant/customer is not required to take any action for this requirement.

10.9 Control Objective 4.2

Software security controls are implemented to mitigate software attacks	
Software Vendor conformance	CAGE Secure application has passed all the threat modeling test cases prepared and executed by security testing team. There are no unmitigated scenarios that need to be addressed.
Guidance to merchant/customer	The merchant/customer is not required to take any action for this requirement.

10.10 Control Objective 5.1 & 5.4

5.1 Access to critical assets is authenticated. ***5.4 By default, all access to critical assets is restricted to only those accounts and services that require such access***	
Software Vendor conformance	Processor configuration credentials are only the critical assets which are protected in an encrypted file. To access the processor configuration the admin user must authenticate using the user ID and password in the CAGE Secure application. CAGE Secure application has only 2 types of user's admin and non-admin. Admin users can configure the application and non-admin can view logs only. CAGE Secure application has users configured where there is strong password policy and expires every 90 days. Authentication credentials are encrypted and stored.
Guidance to merchant/customer	ICS ships pre-loaded and pre-configured computers to customers. Computers have administrative rights and non-administrative rights. When systems leave the ICS facility, they are configured with a password which only ICS support will know. It is the responsibility of the merchants/customers to make sure the Windows OS passwords are changed to their desired ones upon installation of ICS provided PCs at the site. It is also the responsibility of merchants to configure a PCI DSS compliant manner network environment as recommended by ICS.

10.11 Control Objective 6.2

Sensitive data is secured during transmission	
Software Vendor conformance	The CAGE Secure application resides on each of the ICS POS machines and cardholder data is always End-to-End encrypted (E2EE) when transmitted to processor. Cardholder data comes encrypted from the PCI PTS SRED card readers and transmitted out to processors over TLS 1.2 or higher secure socket layer protocol. No configuration is needed as CAGE Secure always makes secure connections to processors while transmitting cardholder data.
Guidance to merchant/customer	The merchant/customer is not required to take any action for this requirement.

10.12 Control Objective 6.3

Use of cryptography for the security of critical assets	
Software Vendor conformance	The encryption of sensitive data and the function is enabled immediately after the CAGE Secure application is installed.
Guidance to merchant/customer	The merchant/customer is not required to take any action for this requirement.

10.13 Control Objective 7.2

The software supports approved key-management processes and procedures	
Software Vendor conformance	Login authentication and merchant ID credentials are stored in an encrypted file. Key management is a static key broken into multiple pieces to evade de-compilers (final assembly is also obfuscated). Protocol details: • RFC2898 byte protocol for derivation. • Rijndael managed 256 byte keys. • SHA512 managed hashing.

	• Crypto streams always employed during read/write operations. Cryptographic keys used to encrypt cardholder data are stored inside PCI PTS SRED card readers. The card reader manufacturer follows stringent PCI DSS requirements to protect the keys in the reader and disclosure and misuse of keys is not possible.
Guidance to merchant/customer	The merchant/customer is not required to take any action for this requirement.

10.14 Control Objective 8.3

The software supports secure retention of detailed activity records	
Software Vendor conformance	CAGE Secure application logs are automatically purged in the device after 6 months. PCI account data is never stored in the logs.
Guidance to merchant/customer	The merchant/customer is advised to use centralized logging to meet PCI DSS requirement. Centralized logging is provided as a separate application by ICS. The application is named as CageCLS.exe which runs as a server listening on default port 32700. All the individual CAGE Secure applications running on ICS provided POS systems need to be pointed to the centralized CageCLS application. This application runs centrally on a site server or on any other PC at the site and facilitates all the CAGE Secure applications to logging to one location. The CageCLS application stores logs in D:\ICS\Logs\Cage location. The logs are saved as separate files for each individual ICS POS device.

10.15 Control Objective 11.2

Software releases and updates are delivered in a secure manner that ensures the integrity of the software and its code	
Software Vendor conformance	The CAGE Secure application software update is provided to fix known vulnerabilities. The patch update is installation through scheduled automatic updates controlled by ICS support team. CAGE Secure application updates are downloaded directly to the POS machines as a secure bundled package, which is facilitated by the ICS Autoupdate installer. The Autoupdate utility verifies the digital signature of the machine, which ensures the POS meets the integrity and authenticity requirements before the update is delivered.
Guidance to merchant/customer	The merchant/customer should understand the versioning methodology and be able to verify the version of payment application installed, to ensure validated versions are being used.

10.16 Control Objective 12

Software Vendor Implementation Guide - The software vendor provides stakeholders with clear and thorough guidance on the secure implementation, configuration, and operation of the software	
Software Vendor conformance	The implementation guide will be distributed as an electronic .pdf copy to all ICS customers who purchase ICS products that use the CAGE Secure application. This implementation guide will be reviewed annually for any software changes or updates as well as changes to PCI SSF requirements and updated accordingly.
Guidance to merchant/customer	Merchants/Customers are advised to get latest copy of PCI SSF implementation guide from ICS support by email support@icscarwashsystems.com.

11. Module A – Account Data Protection Requirements

11.1 A.1.1 - Do Not Store Sensitive Data

Do not store sensitive authentication data after authorization (even if encrypted)	
Software Vendor conformance	CAGE Secure does not store sensitive authentication data (full track data, CAV2/CVC2/CVV2/CID, PINs/PIN blocks) after authorization.
Guidance to merchant/customer	You must make sure not to store any sensitive authentication data (full track data, CAV2/CVC2/CVV2/ CID, PINs/PIN blocks) after authorization.

11.2 A.2.1 - Delete Cardholder Data

Securely delete cardholder data after customer-defined retention period.	
Software Vendor conformance	This is not applicable to CAGE Secure as it does not store any sensitive authentication data.
Guidance to merchant/customer	The merchant/customer is not required to take any action for this requirement.

11.3 A.2.2 - Mask PAN Display – Allow Only First Six/Last Four

Mask PAN when displayed so only personnel with a business need can see more than the first six/last four digits of the PAN.	
Software Vendor conformance	CAGE Secure only displays masked PAN. First 6 and last 4 digits of PAN. Example: 523456***1321. The PCI PTS SRED device never gives full 16 digit card number. No personnel with a business need (Privileged accounts e.g. admin) can ever see the full 16-digit card number. Details of all instances where PAN is displayed, including application screens and logs are available in Annex A1 Instances where PAN is displayed

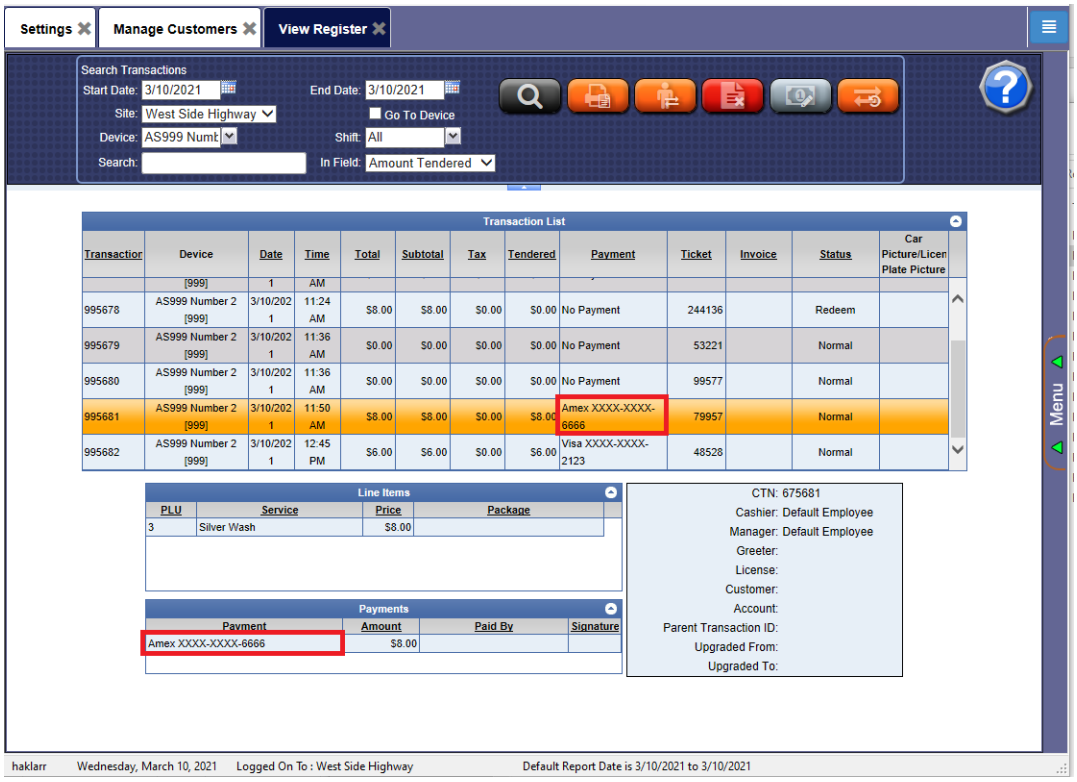
Guidance to merchant/customer	The merchant/customer is not required to take any action for this requirement as PAN is always masked.

11.4 A.2.3 – Render PAN Unreadable

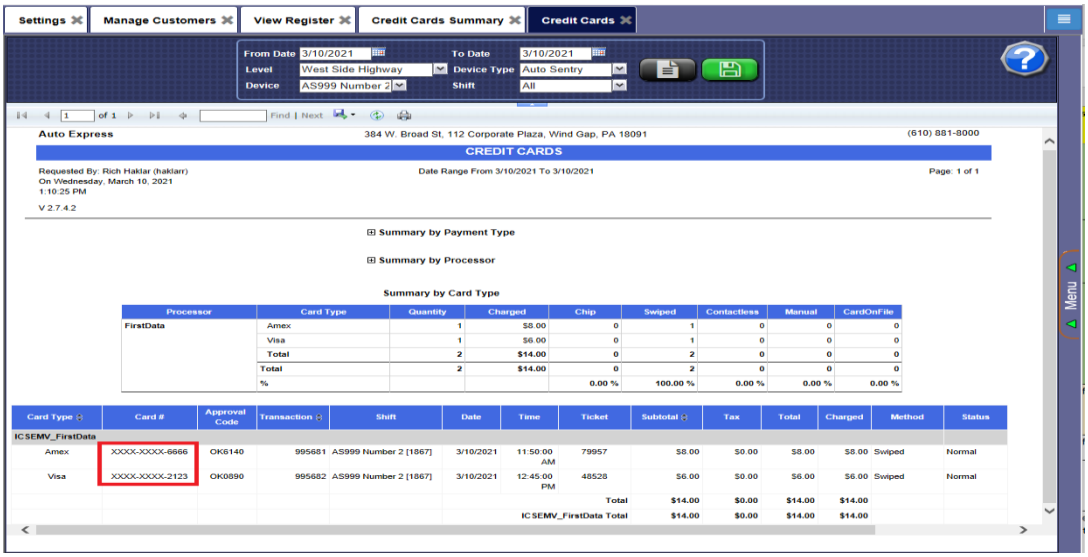
Render PAN unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs).	
Software Vendor conformance	The CAGE Secure application renders PAN unreadable in all locations. The PCI PTS SRED card reader never gives full 16 digit card number. Truncated PAN is captured in log files and reports. Full 16-digit clear text PAN is not stored anywhere in the system. Details of all instances where PAN is stored in database are available in Annex A2 Database Instances where truncated PAN is stored
Guidance to merchant/customer	The merchant/customer is not required to take any action for this requirement as PAN is rendered unreadable.

Annex A1: PAN Display on Reports and Logs

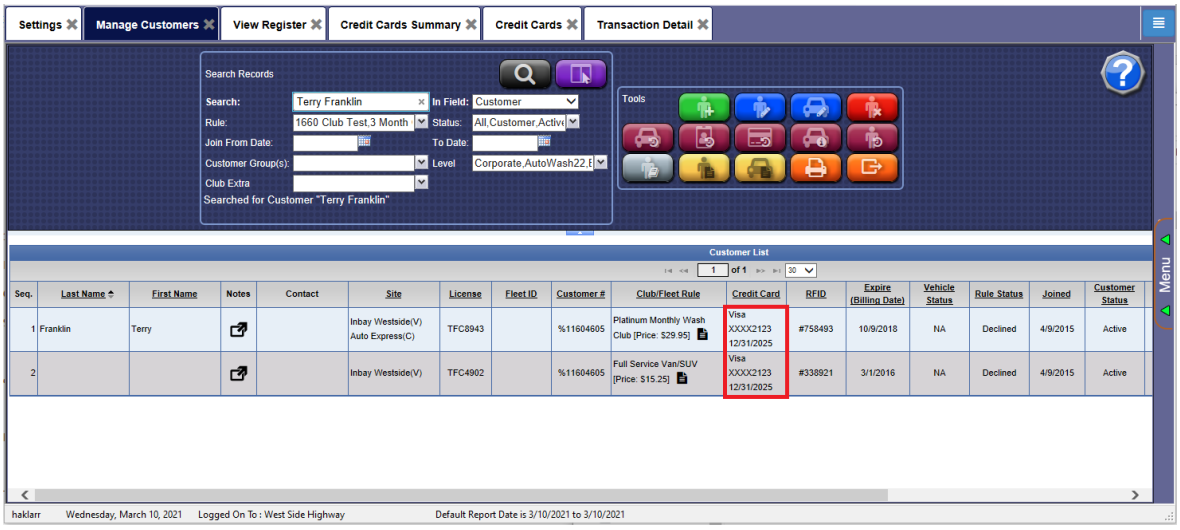
1. Register Report



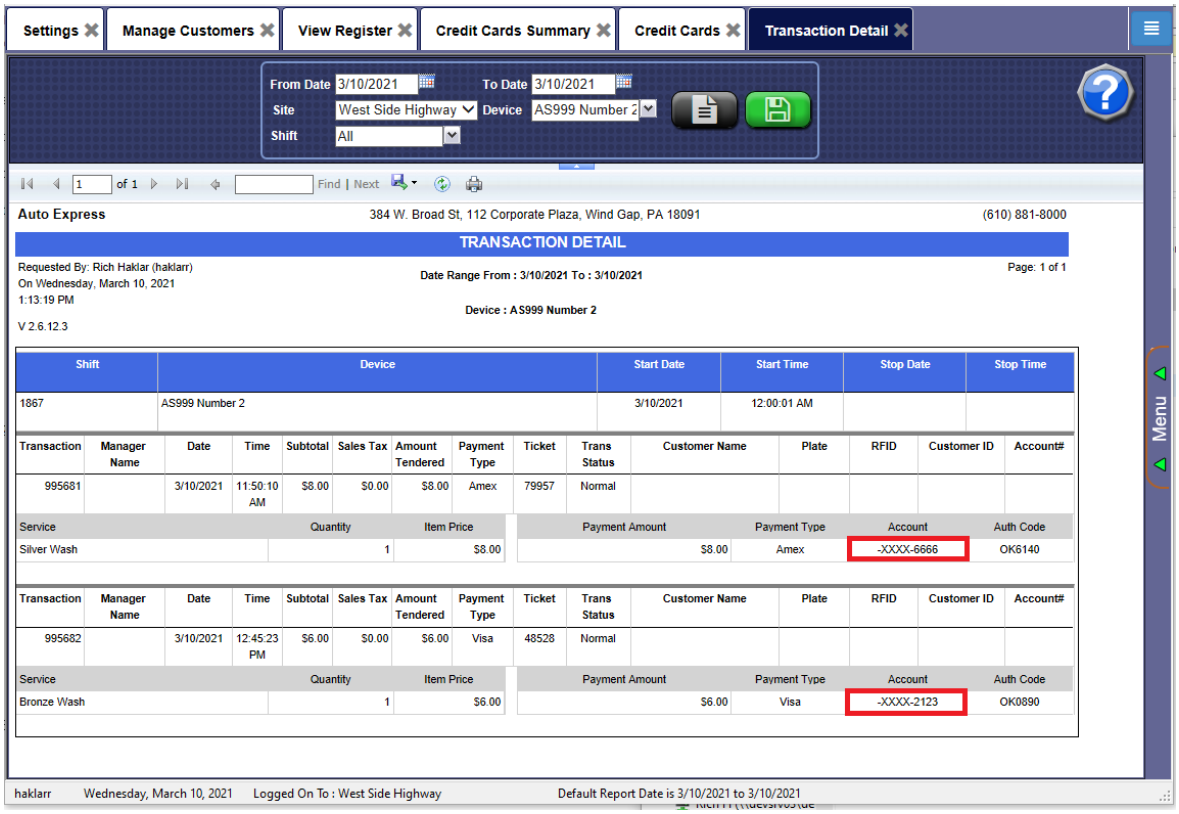
2. Credit Card Payment Report



3. Manage Customer Page



4. Transaction Detail Report



5. Receipts

Sparkle CAR WASH

QA Test Wash
1349 Jacobsburg RD
Wind Gap PA 18091
Fortsøt til bÕs

9/6/2022 Tue 8:56 AM
GREETER: Auto CTN: 616799
PWC: 41581
AS999 Number 2

Simulator4 $7.00
SUB TOTAL $7.00
TOTAL $7.00

AMOUNT TENDERED $7.00
CHANGE $0.00

PAYMENT METHOD: Visa
Account : 2149
Approval : OK3822

EntryMode: Swipe

WASH CODE
41581

Thank You!
Please Drive Safe

Sparkle CAR WASH

QA Test Wash
1349 Jacobsburg RD
Wind Gap PA 18091
Fortsøt til bÕs

9/6/2022 Tue 8:57 AM
GREETER: Auto CTN: 616798
PWC: 29222
AS999 Number 2

Simulator3 $6.00
SUB TOTAL $6.00
TOTAL $6.00

AMOUNT TENDERED $6.00
CHANGE $0.00

PAYMENT METHOD: Master
Account : 4111
Approval : 748134

Mode: ISSUER
AID: A0000000041010
TVR: 0000008000
IAD: 0110A74009020000000000000000
0000000FF
EntryMode: Chip

WASH CODE
29222

Thank You!
Please Drive Safe

Sparkle CAR WASH

QA Test Wash
1349 Jacobsburg RD
Wind Gap PA 18091
Fortsøt til bÕs

9/6/2022 Tue 8:56 AM
GREETER: Auto CTN: 616797
PWC: 93293
AS999 Number 2

Simulator1 $4.00
SUB TOTAL $4.00
TOTAL $4.00

AMOUNT TENDERED $4.00
CHANGE $0.00

PAYMENT METHOD: Master
Account : 4111
Approval : 615092

Mode: ISSUER
AID: A0000000041010
TVR: 0000808001
IAD: 0111A04009220000000000000000
0000000FF
EntryMode: ContactLess

WASH CODE
93293

Thank You!
Please Drive Safe

6. Log Files

[2021-03-10 11:49:55.665 AM] Cage Informational
********** Transaction Started
****

[2021-03-10 11:49:55.666 AM] Cage Informational
****
[2021-03-10 11:49:55.671 AM] Cage Informational Disabling Cards as Cage is Processing something.
[2021-03-10 11:49:55.671 AM] Cage Informational Accept Credit: False, Accept Gift: False and Accept Other: False
[2021-03-10 11:49:55.671 AM] Cage Informational Waiting for the status enquiry.
[2021-03-10 11:49:55.748 AM] Cage Debug Accept message sent.
[2021-03-10 11:49:55.748 AM] Cage Informational Ignoring cancel card read command as no card read command was sent.
[2021-03-10 11:49:55.941 AM] Cage Debug Card read command finished. Response: {"TransactionId":"00000000-0000-0000-0000-000000000000","IsEncrypted":false,"CardType":0,"Result":0,"ErrorMessage":""}
[2021-03-10 11:49:56.186 AM] Cage Informational Wait finished.
[2021-03-10 11:49:56.186 AM] Cage Informational Ignoring cancel card read command as no card read command was sent.
[2021-03-10 11:49:56.194 AM] Cage Debug ErrorMsg: Processing Please Wait..., Result: Processing, StatusCode: 0 and StatusMessage:
[2021-03-10 11:49:56.197 AM] Cage Informational Checking if any other transaction is still pending..
[2021-03-10 11:49:56.197 AM] Cage Informational Transaction check finished..
[2021-03-10 11:49:56.200 AM] Touch Informational Processing - ICS-EMV Authorize 8.00 with Transaction # 995681
[2021-03-10 11:49:56.235 AM] Cage Informational Terminal status code: Swipe, Message: Enter card data screen is shown, Processing: True
[2021-03-10 11:49:57.205 AM] Cage Debug ErrorMsg: Processing Please Wait..., Result: Processing, StatusCode: 1 and StatusMessage: Insert Card or Tap Card/Phone
[2021-03-10 11:49:57.931 AM] Cage Informational Terminal status code: HeartbeatSuccess, Message: Heartbeat success, Processing: True
[2021-03-10 11:49:58.217 AM] Cage Debug ErrorMsg: Processing Please Wait..., Result: Processing, StatusCode: 1 and StatusMessage: Insert Card or Tap Card/Phone
[2021-03-10 11:49:59.227 AM] Cage Debug ErrorMsg: Processing Please Wait..., Result: Processing, StatusCode: 1 and StatusMessage: Insert Card or Tap Card/Phone
[2021-03-10 11:50:00.139 AM] Cage Debug ErrorMsg: Processing Please Wait..., Result: Processing, StatusCode: 1 and StatusMessage: Insert Card or Tap Card/Phone
[2021-03-10 11:50:01.050 AM] Cage Debug ErrorMsg: Processing Please Wait..., Result: Processing, StatusCode: 1 and StatusMessage: Insert Card or Tap Card/Phone
[2021-03-10 11:50:01.963 AM] Cage Debug ErrorMsg: Processing Please Wait..., Result: Processing, StatusCode: 1 and StatusMessage: Insert Card or Tap Card/Phone
[2021-03-10 11:50:01.986 AM] Cage Informational Terminal status code: ContactInserted, Message: Card was swiped, Processing: True
[2021-03-10 11:50:02.873 AM] Cage Informational Terminal status code: RequestSent, Message: Online request, Processing: True

[2021-03-10 11:50:02.873 AM] Cage Debug ErrorMsg: Processing Please Wait..., Result: Processing, StatusCode: 2 and StatusMessage: Processing Please Wait...
[2021-03-10 11:50:03.821 AM] Cage Debug ErrorMsg: Processing Please Wait..., Result: Processing, StatusCode: 2 and StatusMessage: Processing Please Wait...
[2021-03-10 11:50:04.834 AM] Cage Debug ErrorMsg: Processing Please Wait..., Result: Processing, StatusCode: 2 and StatusMessage: Processing Please Wait...
[2021-03-10 11:50:05.845 AM] Cage Debug ErrorMsg: Processing Please Wait..., Result: Processing, StatusCode: 2 and StatusMessage: Processing Please Wait...
[2021-03-10 11:50:06.857 AM] Cage Debug ErrorMsg: Processing Please Wait..., Result: Processing, StatusCode: 2 and StatusMessage: Processing Please Wait...
[2021-03-10 11:50:07.868 AM] Cage Debug ErrorMsg: Processing Please Wait..., Result: Processing, StatusCode: 2 and StatusMessage: Processing Please Wait...
[2021-03-10 11:50:08.858 AM] Cage Informational Terminal status code: ApprovalScreen, Message: Transaction approved, Processing: True
[2021-03-10 11:50:08.879 AM] Cage Debug ErrorMsg: Processing Please Wait..., Result: Processing, StatusCode: 0 and StatusMessage: Approved
[2021-03-10 11:50:08.940 AM] Touch ProcessorRequestOrResponseMessage
{"ExtendedResult":2,"AmountAuthorized":0.0,"OrderNumber":"691150028965","AuthCode":"OK6140","Token":"987643653136666","ProcessorReferenceData":"<?xml version=\"1.0\" encoding=\"utf-8\"?><FDOriginalTransData xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\" xmlns:xsd=\"http://www.w3.org/2001/XMLSchema\"><TransactionType>Sale</TransactionType><Amount>8</Amount><CardBrand>Amex</CardBrand><CardToken>987643653136666</CardToken><CardTokenExpDate>2025-12-01T00:00:00</CardTokenExpDate><CardEntryMode>Swipe</CardEntryMode><IsDebit>false</IsDebit><PinLessDebit>false</PinLessDebit><PINBypassed>false</PINBypassed><CardType>Credit</CardType><OriginalMerchantTransactionId>1150028965</OriginalMerchantTransactionId><OrderNum>691150028965</OrderNum><FleetCardData><DriverNum /><Odometer /></FleetCardData><Products /><StrEmvTlvData /><TransactionDateTime>2021-03-10T11:50:02.8846117-05:00</TransactionDateTime><E2eMethod>Rsa</E2eMethod><HostResposeData><?xml version=\"1.0\" encoding=\"utf-8\"?><GMF xmlns:xsi=\"http://www.w3.org/2001/XMLSchema-instance\" xmlns:xsd=\"http://www.w3.org/2001/XMLSchema\" xmlns=\"com/firstdata/Merchant/gmfV9.02\"><CreditResponse><CommonGrp><PymtType>Credit</PymtType><TxnType>Sale</TxnType><LocalDateTime>20210310115002</LocalDateTime><TrnmsnDateTime>20210310165002</TrnmsnDateTime><STAN>115002</STAN><RefNum>1150028965</RefNum><OrderNum>691150028965</OrderNum><TermID>00000001</TermID><MerchID>313144</MerchID><TxnAmt>800</TxnAmt><TxnCrncy>840</TxnCrncy></CommonGrp><TAGrp><Tkn>987643653136666</Tkn><TAExpDate>1225</TAExpDate></TAGrp><AmexGrp><AmExTranID>001106908289013 8</AmExTranID></AmexGrp><RespGrp><RespCode>000</RespCode><AuthID>OK6140</AuthID><AddtlRespData>APPROVED</AddtlRespData><AthNtwkID>01</AthNtwkID></RespGrp></CreditResponse></GMF></HostRespose

Data></FDOriginalTransData>","ResponseCode":"000","ResponseMessage":"Approved","Tran
sactionType":"Sale","DateTimeOfTransaction":"2021-03-10T11:50:02.8846117-
05:00","AccountNumber":"XXXX-XXXX-6666","ExpirationDate":"12/1/2025 12:00:00
AM","CardEntryType":0,"AccountType":"Credit","CardType":"Amex","KeyUpdateRequired":f
alse,"ReceiptTagsEMV":{},"Result":2}
[2021-03-10 11:50:08.940 AM] Touch Informational Received Card Removed...
[2021-03-10 11:50:08.942 AM] Touch Informational CardEntryType: Swipe
[2021-03-10 11:50:08.942 AM] Touch Debug Account number: 3796-
XXXX-XXXX-6666
[2021-03-10 11:50:08.965 AM] Cage Debug Sending EMVReceipt Receipt
to print: MID/TID: 313144/001
EntryMode: Swipe

[2021-03-10 11:50:08.966 AM] Touch Informational ####### Card approved.
AuthCode OK6140, ReferenceID 12^0, Account# 6666 and CardType AmericanExpress
#######
[2021-03-10 11:50:08.966 AM] Touch Debug Order number
691150028965~OK6140~995681~ND~NF~987643653136666^202512^0
[2021-03-10 11:50:08.990 AM] Cage Informational
****
[2021-03-10 11:50:08.990 AM] Cage Informational
********** Transaction Finished
****

Annex A2: Database Instances Where PAN is Stored

1. Sales Transaction Payment Information Table

	SalesTransactionPaymentID	SiteID	SalesTransactionID	SalesTransactionPaymentTypeID	SalesTransactionPaymentGroupID	Amount	ProgramMembershipID	AuthorizationCode	Account	ProcessorOrderID
43	15088	4007004007	99000000043	116	2	20.05	NULL	TAS567	XXXX-XXXX-7892	191320560
44	15091	4007004007	99000000044	102	2	20.05	NULL	DSC656	XXXX-XXXX-9248	191320561
45	15092	4007004007	99000000045	103	2	20.05	NULL	AXS855	XXXX-XXXX-1007	191320569
46	15093	4007004007	99000000046	103	2	20.05	NULL	AXS774	XXXX-XXXX-1007	191320570
47	15094	4007004007	99000000047	103	2	20.05	NULL	AXS901	XXXX-XXXX-1007	191320571
48	15112	4007004007	99000000048	116	2	16.20	NULL	TAS014	XXXX-XXXX-7892	191320731
49	15283	4007004007	99000000049	102	2	73.95	NULL	DSC380	XXXX-XXXX-9248	191321024
50	15428	4007004007	99000000050	116	2	73.95	NULL	TAS700	XXXX-XXXX-7892	191321427
51	15638	4007004007	99000000051	116	2	20.03	NULL	TAS588	XXXX-XXXX-7892	191321940
52	15639	4007004007	99000000052	103	2	20.03	NULL	AXS442	XXXX-XXXX-1007	191321941
53	15640	4007004007	99000000053	102	2	20.03	NULL	DSC367	XXXX-XXXX-9248	191321942
54	15641	4007004007	99000000054	103	2	16.19	NULL	AXS434	XXXX-XXXX-1007	191321943
55	15642	4007004007	99000000055	116	2	73.95	NULL	TAS591	XXXX-XXXX-7892	191321944
56	15654	4007004007	99000000056	116	2	20.03	NULL	TAS958	XXXX-XXXX-7892	191321992
57	15655	4007004007	99000000057	103	2	16.19	NULL	AXS811	XXXX-XXXX-1007	191321993
58	15656	4007004007	99000000058	103	2	20.03	NULL	AXS803	XXXX-XXXX-1007	191321994
59	15657	4007004007	99000000059	102	2	20.03	NULL	DSC037	XXXX-XXXX-9248	191321995
60	15658	4007004007	99000000060	103	2	20.03	NULL	AXS831	XXXX-XXXX-1007	191321996

2. Customer Credit Information Table

	CustomerID	Ordinal	RecurringID	CreditCardNumber	CreditCardType	ZipCode	ProcessorName	SiteID	E
1	D02AD90F-AC61-4E9A-B3CA-002918F2F24A	0	enc_IWTBRBuWBTIzUALb1idZFaQLevXPahOWQHINsc+ICXUI...	1112	117	18301	ICSEMV_FirstData	4007004007	2
2	641B5E62-F358-4823-BB1E-006A9978ADBC	0	enc_OObizQV6F5gtvcCUczU1MgBERkPhveFUtiFnngvCyM=	6528	117	45829	Moneris	4007001099	2
3	AD918D64-DF47-447D-844B-00B202B839CA	0	enc_XAZ6bfwz1lGjs4KpSbVSTMBw6yJ0bQxj1aBMBYHR7VLYtC...	0021	142	75299	TransFirst	4007004007	2
4	91D7234D-C510-41B0-8DD4-00EDA8C0A627	0	enc_bFxu17NvvcgbPOYYTNjvOg==	9248	102	18091	TransFirst	4007004007	2
5	9365D9F2-D141-4604-AD52-010FCD74C795	0	enc_4Cq4UbFK3uQxyTgv9YS5kA==	9248	102	14725	TransFirst	4007004007	2
6	2C0DA5B0-3A09-4672-9353-01573A7808CA	0	enc_YnJydJlskD37wF3geTimkw==	3436	116	18353	TransactionExpress	4007004010	2
7	12B978B6-BFD3-4958-B466-01840C778A3A	0	enc_Ao2VT3FKrQSFfkSQzQvfIAoec6NPgpAgMkFR7afcr6U=	0119	116	11111	PAX_FirstData	4007004007	2
8	5EB2D9DD-95F9-4795-B365-01A81DE1B526	0	enc_Vc7347liVBDTyPur1l8kpImciMxXaF92LDVIXghuR1U=	1111	116	18091	PAX_FirstData	4007004007	2
9	2D9CEB5E-F812-4F9D-9500-01AE078CDD84	0	enc_EgSDa6SAnO5nvp6Lbm7qWw==	9580	116	18091	FreedomPay	4007004007	2
10	31B25BA1-0C39-4544-A63C-01F9CED265E9	0	enc_U8E1Xr8r6lkfUQvHUT/SFg==	3436	116	12454	TransFirst	4007004007	2
11	D201270C-22FA-42BC-B9EE-023B2131A534	0	enc_+ipgi/bivzL8VGdXUwRIXp/Z5wCltMYdKK05qy7YpgE=	4832	117	18091	PAX_FirstData	4007004007	2
12	2FCDDCD0-1FF4-4F7B-9C1F-02460BF4061B	0	enc_/Fryi5ywdvPQRdWvNhlw3N2wE7B2AHvEaVL3TOI5588=	2003	116	11111	Moneris	4007004007	2
13	09CA52FC-50E7-4398-BF04-0281C19F0CDD	0	enc_7/pp+NL3EPmgRV2X3xftEA==	6781	116	18091	FreedomPay	4007004007	2
14	591441ED-2031-4DD5-9D13-0296C509C729	0	enc_UU3OsrQuJb9+VBtRZ6fczw==	1007	103	11419	TransFirst	4007004007	2
15	26EFB0BF-07F6-4876-83C1-02A117BB4F0A	0	enc_+ipgi/bivzL8VGdXUwRIXp/Z5wCltMYdKK05qy7YpgE=	4832	117	88888	PAX_FirstData	4007004007	2
16	E7FAC2BC-E35B-426D-8EFD-02A7844FA1F0	0	enc_rLGTRD/m75lNSzduQGfjU/LtoZfmDfb3B6RXBmRRCX4=	6897	117	18036	Moneris	4007004007	2
17	4EF328C9-F089-4A5D-89BB-02EE56739D4B	0	enc_vSfs4/wrdMjQ3n6+0JuY3PROHUH62CXdLmmAtAlTjw=	4446	117	18091	PAX_FirstData	4007004007	2
18	F107E9A2-C367-458E-9E10-035128CB99F7	0	enc_U1Jkpctj5W+RltHTbkb+nrMAuEa6k5Yr+Au34RZzyVU6o1o...	0026	116	12345	TransFirst	4007004007	2

Annex A3: Application Versioning

There are 4 elements to versioning policy which is followed for CAGE Secure application

[Major Version].[Minor Version].[Revision Number].[Build Number]

[Major Version] – Indicates the main version ranging from value 1 to 99. The major version number increments if there is change in technology, hardware used or development language tool set, software architecture, source code, or components that handle or interact with sensitive data, sensitive functions, or sensitive resources.

[Minor Version] – Indicates the minor version ranging from value 1 to 99. The changes that do not trigger the high impact criteria.

[Revision Number] – Indicates the release number ranging from value 1 to 99. The revision number will change if there is a new processor certified. Revision number is reset whenever major or minor number is changed.

- 6.2.0.1 – Revision 0 to indicate certified with Fiserv processor
- 6.2.1.1 – Revision 1 to indicate certified with Heartland processor in addition to Fiserv processor

[Build Number] – Indicates the release number ranging from value 1 to 999. The build number is changed whenever there is a minor change to the functionality of the application or a feature/ or bug fix or minor enhancement to the application without affecting security or PCI requirement. Build number is reset to 1 whenever major, minor or revision number is changed.