Payment Card Industry (PCI)

Point-to-Point Encryption

P2PE Solutions Master Document

October 2025

Document History and Revisions

Date	Revision	By Whom	What was changed	Jira
12/10/2019	8.0	DBarnet	Updated for Verifone P400	
10/28/2020	9.0	DBarnet	Annual Review and Update	
12/09/2020	9.1	DBarnet	Updated for Pax A920	
13/13/2021	9.1	DBarnet	Reviewed	
07/06/2022	10.0	DBarnet	Update Document, Added A92-Pro, A35, A77	
05/05/2023	10.1	DBarnet	Document Updates	
8/18/2023	11	Dbarnet	Document Update, Added A50	
14/04/2025	11.1	KTrajkovski	Document Update, removing unsupported terminals	ADOPS-12
4/18/2025	12	DBarnet	Versioning and Update	ADOPS-12
9/11/2025	12.1	DBarnet	Council updates	ADOPS-12
10/08/2025	12.2	DBarnet	Council Approval and Updated Reference number	ADOPS-12

Table of Contents

Entity Name Clarification

For clarity, all references to Visa Acceptance Solution, Cybersource, and Payworks in this document refer to same entity. The names by be used interchangeably.

3A-1 Overall P2PE Solution (Per PCI P2PE V3.2)

The Visa Acceptance Solutions Point-to-Point encryption (P2PE) solution supports the PAX A920, A920 Pro, A920 MAX, A35, A77, A50 and IM 30 terminals.

3A.1.1 Solution Components

3A.1.1.1 PAX A920 Components

The Visa Acceptance Solutions P2PE solution implemented with the PAX A consists of following components:

P2PE Domain	PAX A920 Component Description
Domain 1 Encryption Application and Device Management	PAX A920 terminal Encryption used is 3DES/DUKPT PAX Encryption Management
Domain 2 Application Security	BroadPOS P2PE 1.02.xx
Domain 3 P2PE Solution Management	Visa Acceptance Solutions P2PE
Domain 4 Decryption Environment	Visa Acceptance Solutions P2PE Note: PIN Translation occurs in Visa Systems (see architecture diagram below)
Domain 5 P2PE Cryptographic Key Operations and Device Management	Visa Acceptance Solutions P2PE UCP KIF SPT Portal (KIF) PAX (CA/RA)

3A.1.1.2 PAX A920 PRO Components

The Visa Acceptance Solutions P2PE solution implemented with the PAX A consists of following components:

P2PE Domain	PAX A920 Pro Component Description
Domain 1 Encryption Application and Device Management	PAX A920 terminal Encryption used is 3DES/DUKPT PAX Encryption Management
Domain 2 Application Security	BroadPOS P2PE 1.02.xx
Domain 3 P2PE Solution Management	Visa Acceptance Solutions P2PE
Domain 4	Visa Acceptance Solutions P2PE

P2PE Domain	PAX A920 Pro Component Description
Decryption Environment	Note: PIN Translation occurs in Visa Systems (see architecture diagram below)
Domain 5 P2PE Cryptographic Key Operations and Device Management	Visa Acceptance Solutions P2PE UCP KIF SPT Portal (KIF) PAX (CA/RA)

3A.1.1.3 PAX A920 MAX Components

The Visa Acceptance Solutions P2PE solution implemented with the PAX A consists of following components:

P2PE Domain	PAX A920 MAX Component Description
Domain 1 Encryption Application and Device Management	PAX A920 MAX terminal Encryption used is 3DES/DUKPT PAX Encryption Management
Domain 2 Application Security	BroadPOS P2PE 1.02.xx
Domain 3 P2PE Solution Management	Visa Acceptance Solutions P2PE
Domain 4 Decryption Environment	Visa Acceptance Solutions P2PE Note: PIN Translation occurs in Visa Systems (see architecture diagram below)
Domain 5 P2PE Cryptographic Key Operations and Device Management	Visa Acceptance Solutions P2PE UCP KIF SPT Portal (KIF) PAX (CA/RA)

3A.1.1.4 PAX A35 Components

The Visa Acceptance Solutions P2PE solution implemented with the PAX A consists of following components:

P2PE Domain	PAX A35 Component Description
Domain 1 Encryption Application and Device Management	PAX A35 terminal Encryption used is 3DES/DUKPT PAX Encryption Management
Domain 2 Application Security	BroadPOS P2PE 1.02.xx
Domain 3	Visa Acceptance Solutions P2PE

P2PE Domain	PAX A35 Component Description
P2PE Solution Management	
Domain 4 Decryption Environment	Visa Acceptance Solutions P2PE Note: PIN Translation occurs in Visa Systems (see architecture diagram below)
Domain 5 P2PE Cryptographic Key Operations and Device Management	Visa Acceptance Solutions P2PE UCP KIF SPT Portal (KIF) PAX (CA/RA)

3A.1.1.5 PAX A77 Components

The Visa Acceptance Solutions P2PE solution implemented with the PAX A consists of following components:

P2PE Domain	PAX A77 Component Description
Domain 1 Encryption Application and Device Management	PAX A77 terminal Encryption used is 3DES/DUKPT PAX Encryption Management
Domain 2 Application Security	BroadPOS P2PE 1.02.xx
Domain 3 P2PE Solution Management	Visa Acceptance Solutions P2PE
Domain 4 Decryption Environment	Visa Acceptance Solutions P2PE Note: PIN Translation occurs in Visa Systems (see architecture diagram below)
Domain 5 P2PE Cryptographic Key Operations and Device Management	Visa Acceptance Solutions P2PE UCP KIF SPT Portal (KIF) PAX (CA/RA)

3A.1.1.6 PAX A50 Components

The Visa Acceptance Solutions P2PE solution implemented with the PAX A consists of following components:

P2PE Domain	PAX A50 Component Description
Domain 1 Encryption Application and Device Management	PAX A50 terminal Encryption used is 3DES/DUKPT PAX Encryption Management

P2PE Domain	PAX A50 Component Description
Domain 2 Application Security	BroadPOS P2PE 1.02.xx
Domain 3 P2PE Solution Management	Visa Acceptance Solutions P2PE
Domain 4 Decryption Environment	Visa Acceptance Solutions P2PE Note: PIN Translation occurs in Visa Systems (see architecture diagram below)
Domain 5 P2PE Cryptographic Key Operations and Device Management	Visa Acceptance Solutions P2PE UCP KIF SPT Portal (KIF) PAX (CA/RA)

3A.1.1.7 PAX IM 30 Components

The Visa Acceptance Solutions P2PE solution implemented with the PAX A consists of following components:

P2PE Domain	PAX IM 30 Component Description
Domain 1 Encryption Application and Device Management	PAX IM 30 terminal Encryption used is 3DES/DUKPT PAX Encryption Management
Domain 2 Application Security	BroadPOS P2PE 1.02.xx
Domain 3 P2PE Solution Management	Visa Acceptance Solutions P2PE
Domain 4 Decryption Environment	Visa Acceptance Solutions P2PE Note: PIN Translation occurs in Visa Systems (see architecture diagram below)
Domain 5 P2PE Cryptographic Key Operations and Device Management	Visa Acceptance Solutions P2PE UCP KIF SPT Portal (KIF) PAX (CA/RA)

3A.1.2 Solution Architecture:

3A.1.2.1 PAX A920 Solution Architecture:

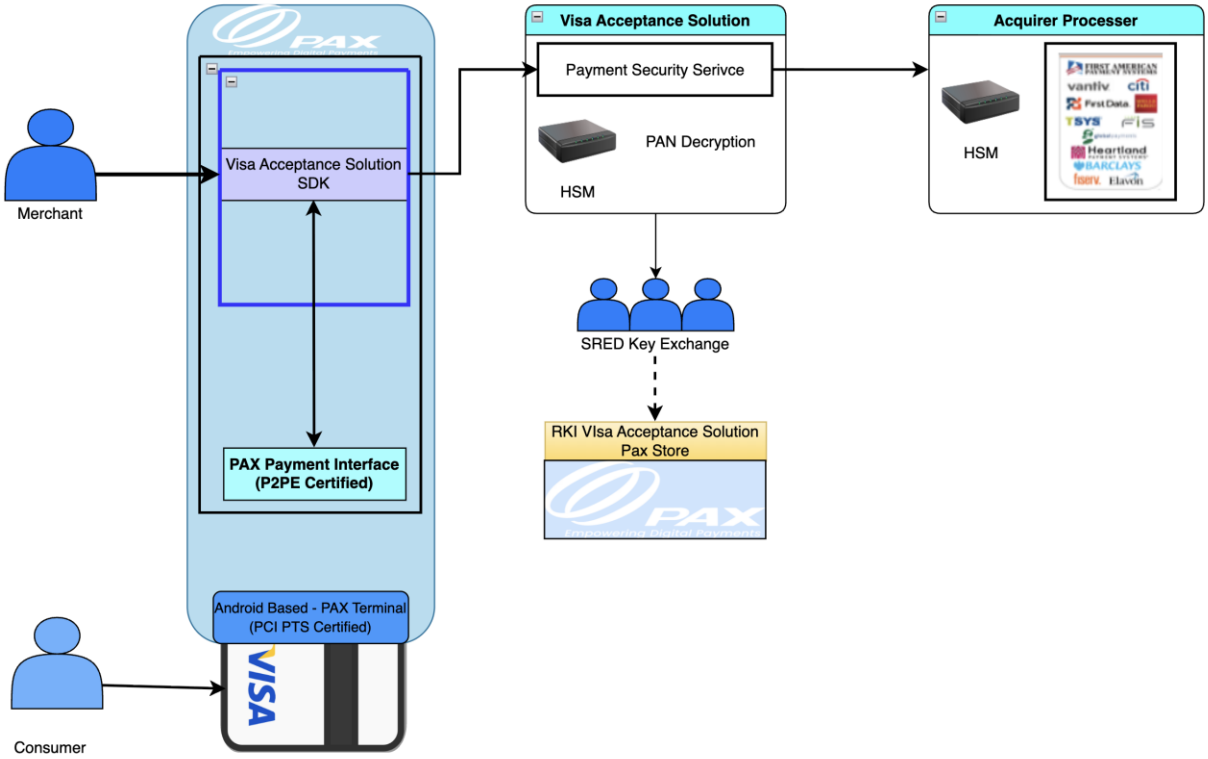


Figure 2

Figure 2 represents a high-level architecture of Visa Acceptance Solutions P2PE solution implemented with the PAX A920 terminal.

1. Data is encrypted in PTS listed SRED enabled terminal using P2PE listed PAX BroadPOS P2PE payment application.
2. Encrypted Data is transferred from PAX BroadPOS P2PE to Acceptance Devices SDK (Software Development Kit) which is resides in merchant environment.
3. Acceptance Devices SDK securely connects to Visa Accetance Solution platform and transmits data over for decryption.
4. Visa Accetance Solution receives the data and decrypts it, using PCI approved hardware HSMs.
5. Once the data is decrypted, Visa Accetance Solution repackages the data and transmits it to Visa Acceptance Solutions over a secure connection.
6. Visa Acceptance Solutions transmits the payment data to the appropriate acquirer.
7. Acquirer authorizes the transaction and sends the authorization back to Visa Acceptance Solutions.

8. Visa Acceptance Solutions tokenizes the payment data and transmits it back to Visa Accetance Solution which then passes it on to the merchant.

There is no PAN data in the clear transmitted back to the merchant.

3A.1.2.2 PAX A920 Pro Solution Architecture:

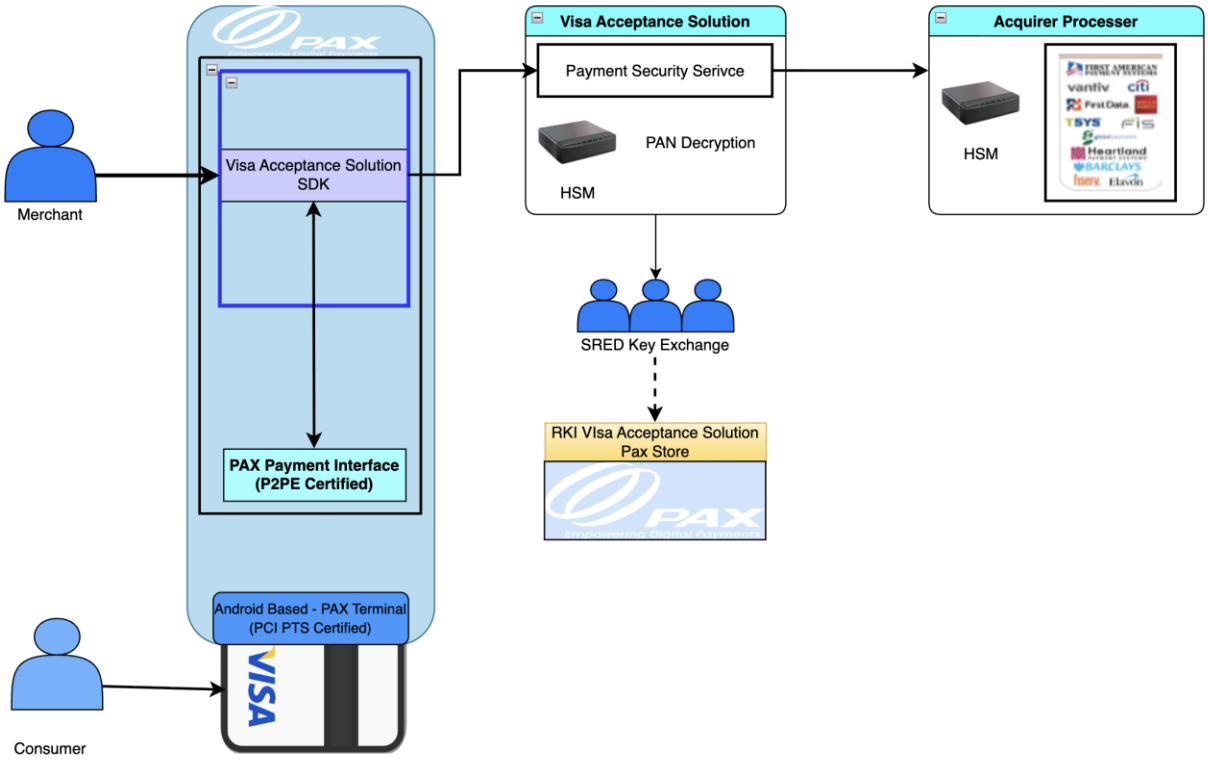


Figure 3

Figure 3 represents a high-level architecture of Visa Acceptance Solutions P2PE solution implemented with the PAX A920 Pro terminal.

1. Data is encrypted in PTS listed SRED enabled terminal using P2PE listed PAX BroadPOS P2PE payment application.
2. Encrypted Data is transferred from PAX BroadPOS P2PE to Acceptance Devices SDK (Software Development Kit) which is resides in merchant environment.
3. Acceptance Devices SDK securely connects to Visa Accetance Solution platform and transmits data over for decryption.
4. Visa Accetance Solution receives the data and decrypts it, using PCI approved hardware HSMs.
5. Once the data is decrypted, Visa Accetance Solution repackages the data and transmits it to Visa Acceptance Solutions over a secure connection.
6. Visa Acceptance Solutions transmits the payment data to the appropriate acquirer.

7. Acquirer authorizes the transaction and sends the authorization back to Visa Acceptance Solutions.
8. Visa Acceptance Solutions tokenizes the payment data and transmits it back to Visa Accetance Solution which then passes it on to the merchant.

There is no PAN data in the clear transmitted back to the merchant.

3A.1.2.3 PAX A920 MAX Solution Architecture:

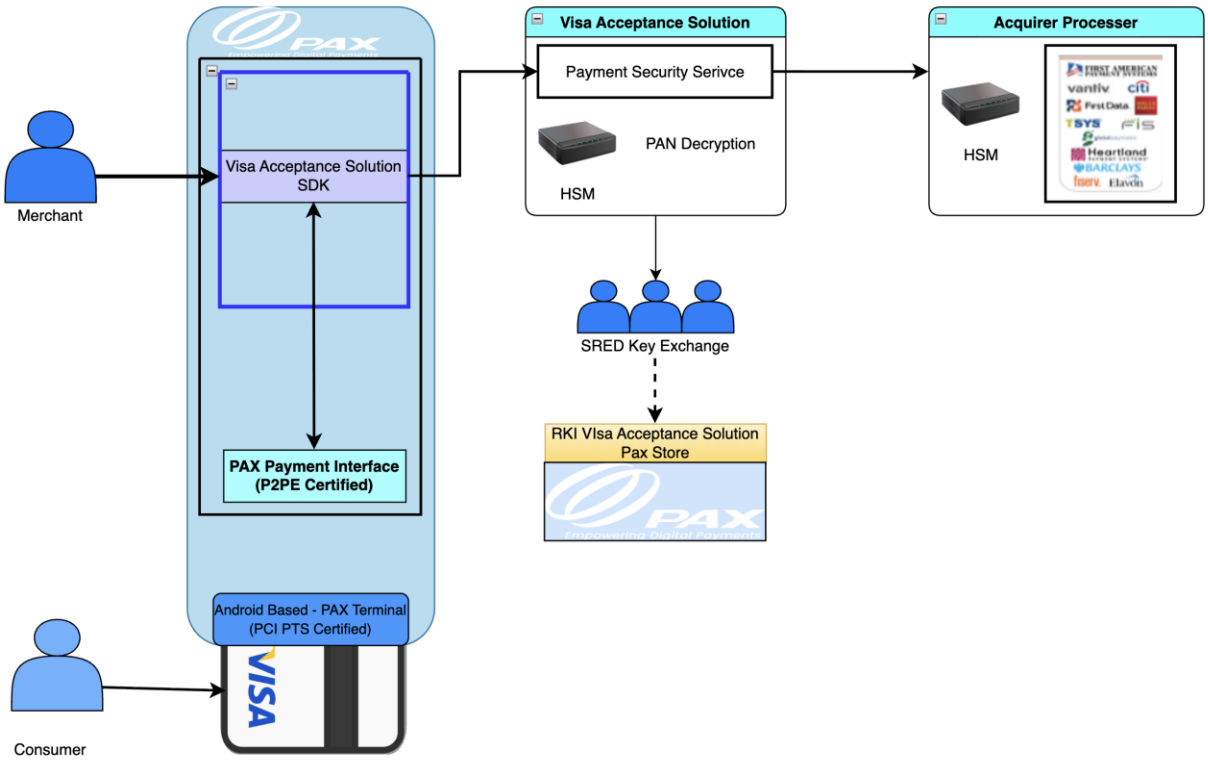


Figure 4

Figure 4 represents a high-level architecture of Visa Acceptance Solutions P2PE solution implemented with the PAX A920 MAX terminal.

1. Data is encrypted in PTS listed SRED enabled terminal using P2PE listed PAX BroadPOS P2PE payment application.
2. Encrypted Data is transferred from PAX BroadPOS P2PE to Acceptance Devices SDK (Software Development Kit) which is resides in merchant environment.
3. Acceptance Devices SDK securely connects to Visa Accetance Solution platform and transmits data over for decryption.
4. Visa Accetance Solution receives the data and decrypts it, using PCI approved hardware HSMs.
5. Once the data is decrypted, Visa Accetance Solution repackages the data and transmits it to Visa Acceptance Solutions over a secure connection.

6. Visa Acceptance Solutions transmits the payment data to the appropriate acquirer.
7. Acquirer authorizes the transaction and sends the authorization back to Visa Acceptance Solutions.
8. Visa Acceptance Solutions tokenizes the payment data and transmits it back to Visa Accetance Solution which then passes it on to the merchant.

There is no PAN data in the clear transmitted back to the merchant.

3A.1.2.4 PAX A35 Solution Architecture:

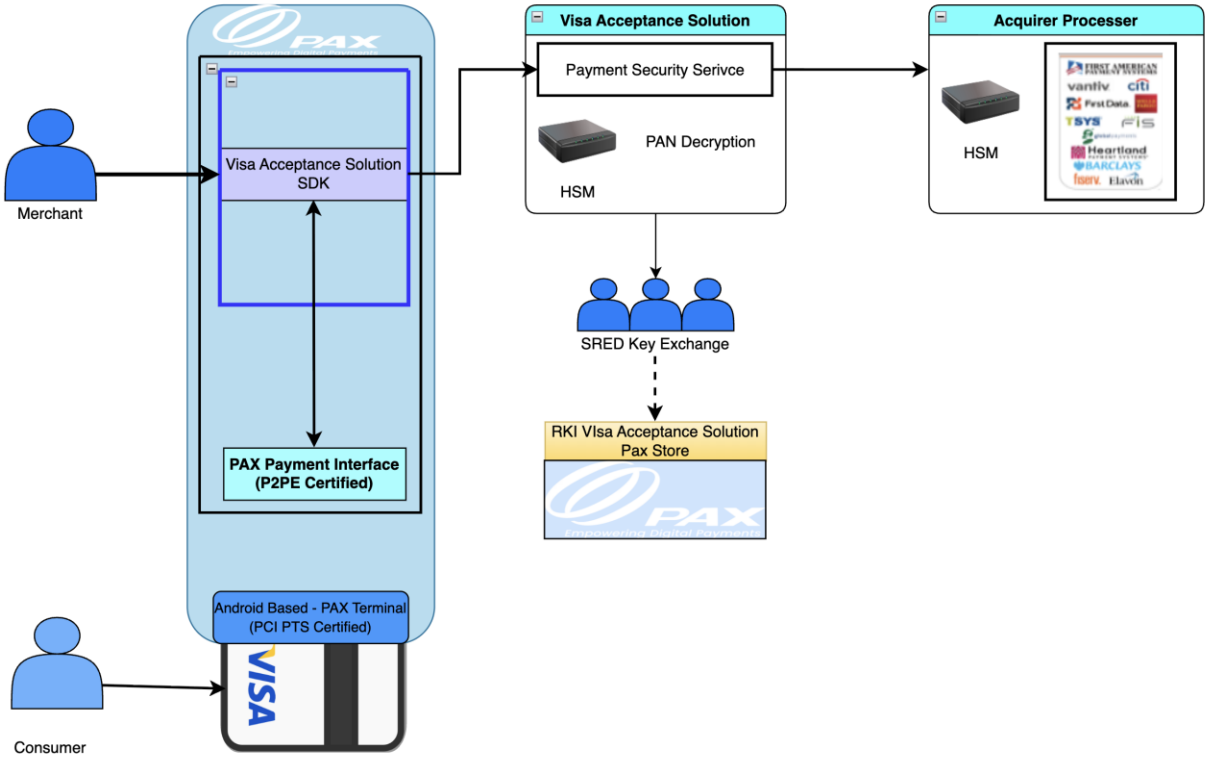


Figure 5

Figure 5 represents a high-level architecture of Visa Acceptance Solutions P2PE solution implemented with the PAX A35 terminal.

1. Data is encrypted in PTS listed SRED enabled terminal using P2PE listed PAX BroadPOS P2PE payment application.
2. Encrypted Data is transferred from PAX BroadPOS P2PE to Acceptance Devices SDK (Software Development Kit) which is resides in merchant environment.
3. Acceptance Devices SDK securely connects to Visa Accetance Solution platform and transmits data over for decryption.
4. Visa Accetance Solution receives the data and decrypts it, using PCI approved hardware HSMs.
5. Once the data is decrypted, Visa Accetance Solution repackages the data and transmits it to Visa Acceptance Solutions over a secure connection.

6. Visa Acceptance Solutions transmits the payment data to the appropriate acquirer.
7. Acquirer authorizes the transaction and sends the authorization back to Visa Acceptance Solutions.
8. Visa Acceptance Solutions tokenizes the payment data and transmits it back to Visa Accetance Solution which then passes it on to the merchant.

There is no PAN data in the clear transmitted back to the merchant.

3A.1.2.5 PAX A77 Solution Architecture:

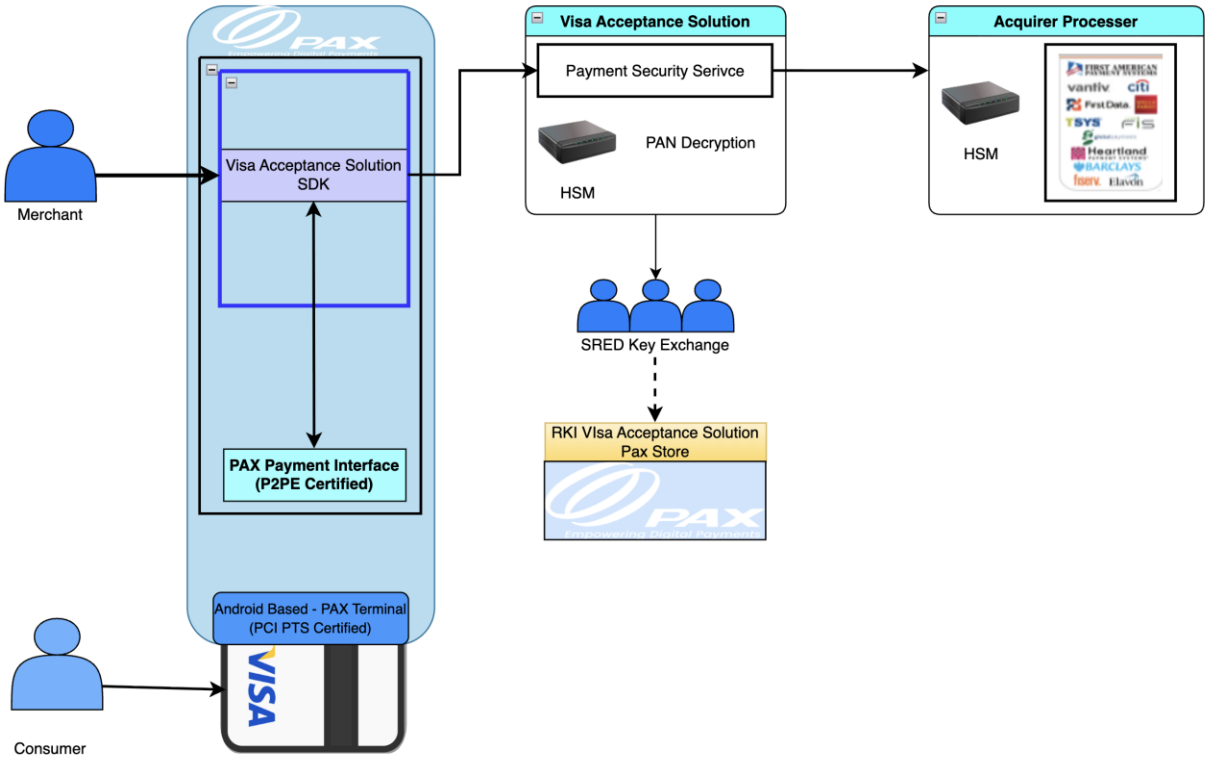


Figure 6

Figure 6 represents a high-level architecture of Visa Acceptance Solutions P2PE solution implemented with the PAX A77 terminal.

1. Data is encrypted in PTS listed SRED enabled terminal using P2PE listed PAX BroadPOS P2PE payment application.
2. Encrypted Data is transferred from PAX BroadPOS P2PE to Acceptance Devices SDK (Software Development Kit) which is resides in merchant environment.
3. Acceptance Devices SDK securely connects to Visa Accetance Solution platform and transmits data over for decryption.
4. Visa Accetance Solution receives the data and decrypts it, using PCI approved hardware HSMs.

5. Once the data is decrypted, Visa Accetance Solution repackages the data and transmits it to Visa Acceptance Solutions over a secure connection.
6. Visa Acceptance Solutions transmits the payment data to the appropriate acquirer.
7. Acquirer authorizes the transaction and sends the authorization back to Visa Acceptance Solutions.
8. Visa Acceptance Solutions tokenizes the payment data and transmits it back to Visa Accetance Solution which then passes it on to the merchant.

There is no PAN data in the clear transmitted back to the merchant.

3A.1.2.6 PAX A50 Solution Architecture:

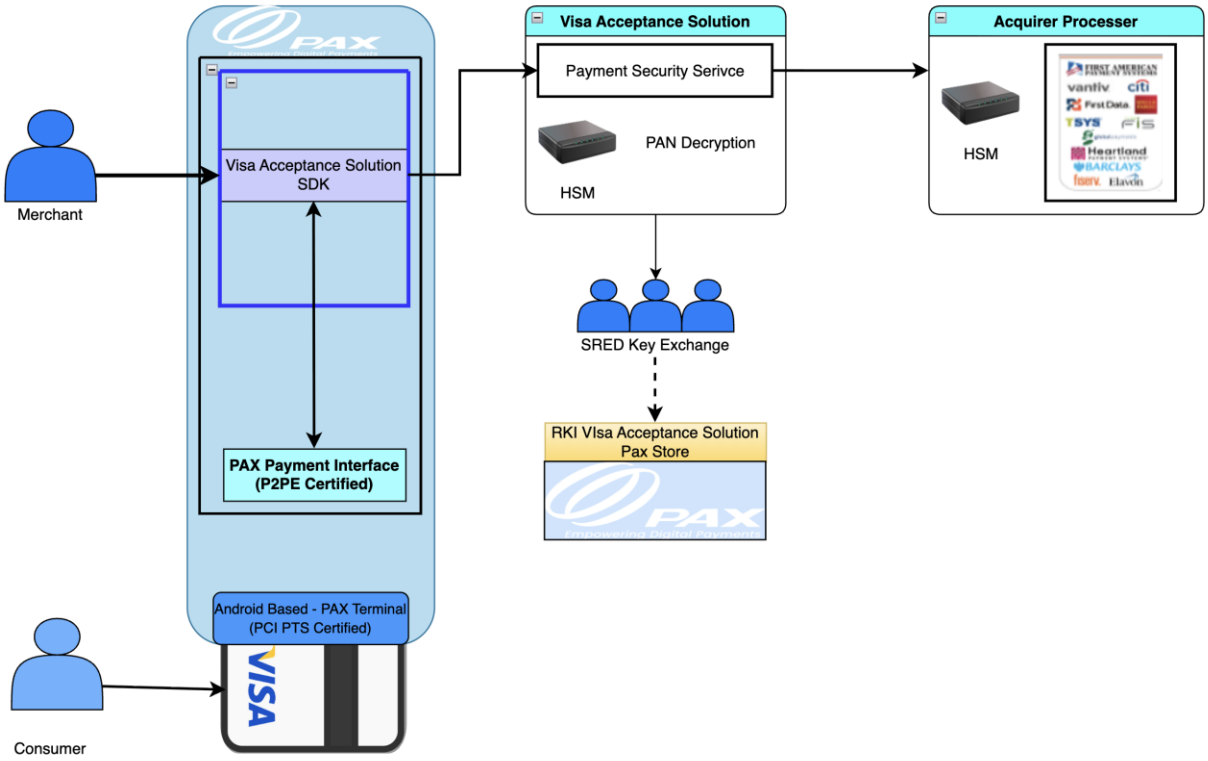


Figure 7

Figure 7 represents a high-level architecture of Visa Acceptance Solutions P2PE solution implemented with the PAX A50 terminal.

1. Data is encrypted in PTS listed SRED enabled terminal using P2PE listed PAX BroadPOS P2PE payment application.
2. Encrypted Data is transferred from PAX BroadPOS P2PE to Acceptance Devices SDK (Software Development Kit) which is resides in merchant environment.
3. Acceptance Devices SDKs ecurely connects to Visa Accetance Solution platform and transmits data over for decryption.

4. Visa Accetance Solution receives the data and decrypts it, using PCI approved hardware HSMs.
5. Once the data is decrypted, Visa Accetance Solution repackages the data and transmits it to Visa Acceptance Solutions over a secure connection.
6. Visa Acceptance Solutions transmits the payment data to the appropriate acquirer.
7. Acquirer authorizes the transaction and sends the authorization back to Visa Acceptance Solutions.
8. Visa Acceptance Solutions tokenizes the payment data and transmits it back to Visa Accetance Solution which then passes it on to the merchant.

There is no PAN data in the clear transmitted back to the merchant.

3A.1.2.7 PAX IM 30 Solution Architecture:

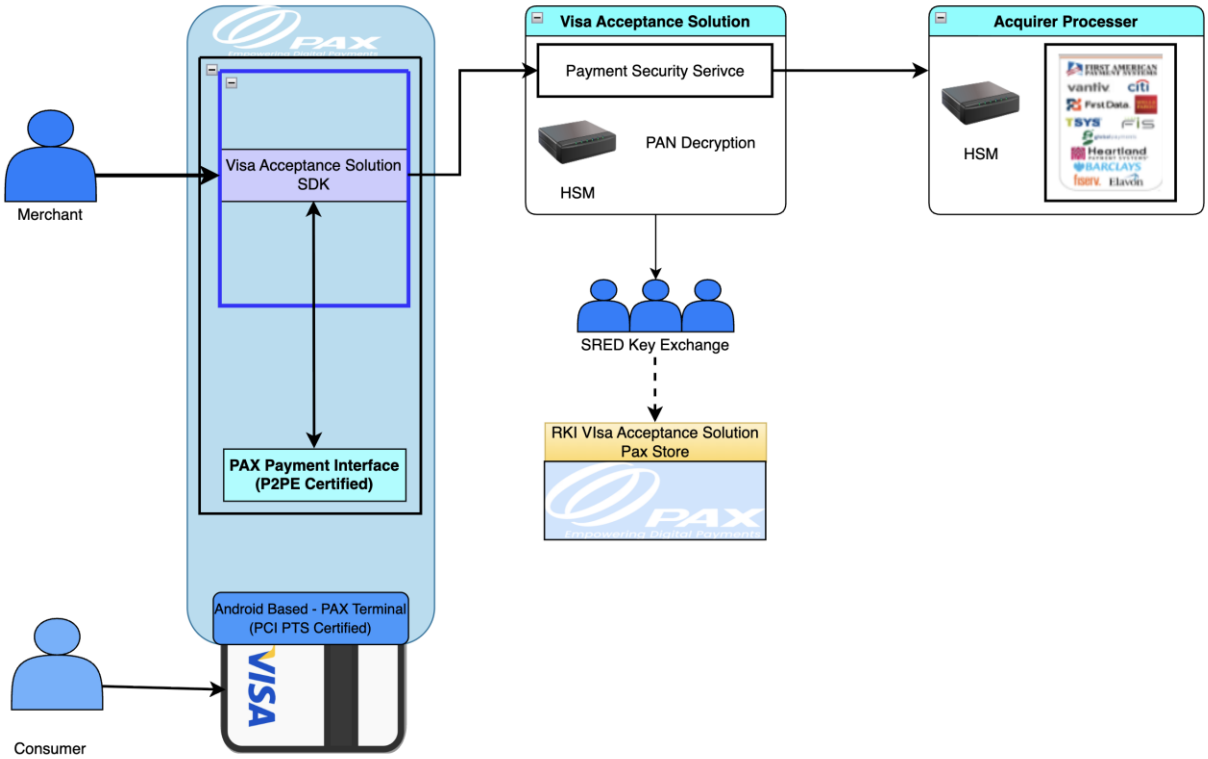


Figure 8

Figure 8 represents a high-level architecture of Visa Acceptance Solutions P2PE solution implemented with the PAX IM 30 terminal.

1. Data is encrypted in PTS listed SRED enabled terminal using P2PE listed PAX BroadPOS P2PE payment application.
2. Encrypted Data is transferred from PAX BroadPOS P2PE to Acceptance Devices SDK (Software Development Kit) which is resides in merchant environment.

3. Acceptance Devices SDK securely connects to Visa Accetance Solution platform and transmits data over for decryption.
4. Visa Accetance Solution receives the data and decrypts it, using PCI approved hardware HSMs.
5. Once the data is decrypted, Visa Accetance Solution repackages the data and transmits it to Visa Acceptance Solutions over a secure connection.
6. Visa Acceptance Solutions transmits the payment data to the appropriate acquirer.
7. Acquirer authorizes the transaction and sends the authorization back to Visa Acceptance Solutions.
8. Visa Acceptance Solutions tokenizes the payment data and transmits it back to Visa Accetance Solution which then passes it on to the merchant.

There is no PAN data in the clear transmitted back to the merchant.

3A-1.3 Data Flow Documentation

Figures 9, 10, 11 12, 13, 14, 15, and 16 below describes the data encryption zones. Following is the description of each Zone.

3A-1.3.1 PAX A920

Merchant Card Presentment Zone 1:

Zone 1 is in merchant location where a credit card is presented to the merchant for payment. Credit card is swiped, dipped, or tapped on a PTS approved terminal (with SRED encryption enabled) after the terminal prompts the card holder with payment data. Once card is used, card data is immediately encrypted in SRED and passed on encrypted to the Merchant Zone 2.

Merchant Zone 2:

Zone 2 includes Visa Accetance Solution application that manages connectivity with POS system and the terminal in semi-integrated manner. The function of Visa Accetance Solution application is to receive payments dollar amount from the Visa Accetance Solution Accept POS application and pass the request over to the terminal. Terminal API receives the payments application and prompts the consumer to use the credit card. Once data is encrypted as described in Zone 1, the data is passed back to Visa Accetance Solution application which then routes transaction and encrypted credit card data back to Visa Accetance Solution in Zone 3.

Visa Acceptance Solutions Secure Zone 3:

Zone three includes data acceptance, decryption and forwarding for authorizations. Following steps are followed over secure connectivity in this zone.

1. Visa Accetance Solution receives encrypted payment data and authorization request. It connects to HSM's to decrypt first and then formats the message in manner that is consumable by Visa Acceptance Solutions. Connectivity between Visa Accetance Solution and Visa Acceptance Solutions is over secure connections for maximum security.

2. Visa Acceptance Solutions receives the data in the clear and processes it for other products based on merchant choice. Visa Acceptance Solutions then routes the data over to appropriate processor for authorization over secure connectivity.
3. Processor accepts the payment data in the clear over secure connectivity and processes the transactions before sending the authorization backwards through the same process. No clear text PAN data is sent back to the merchant.

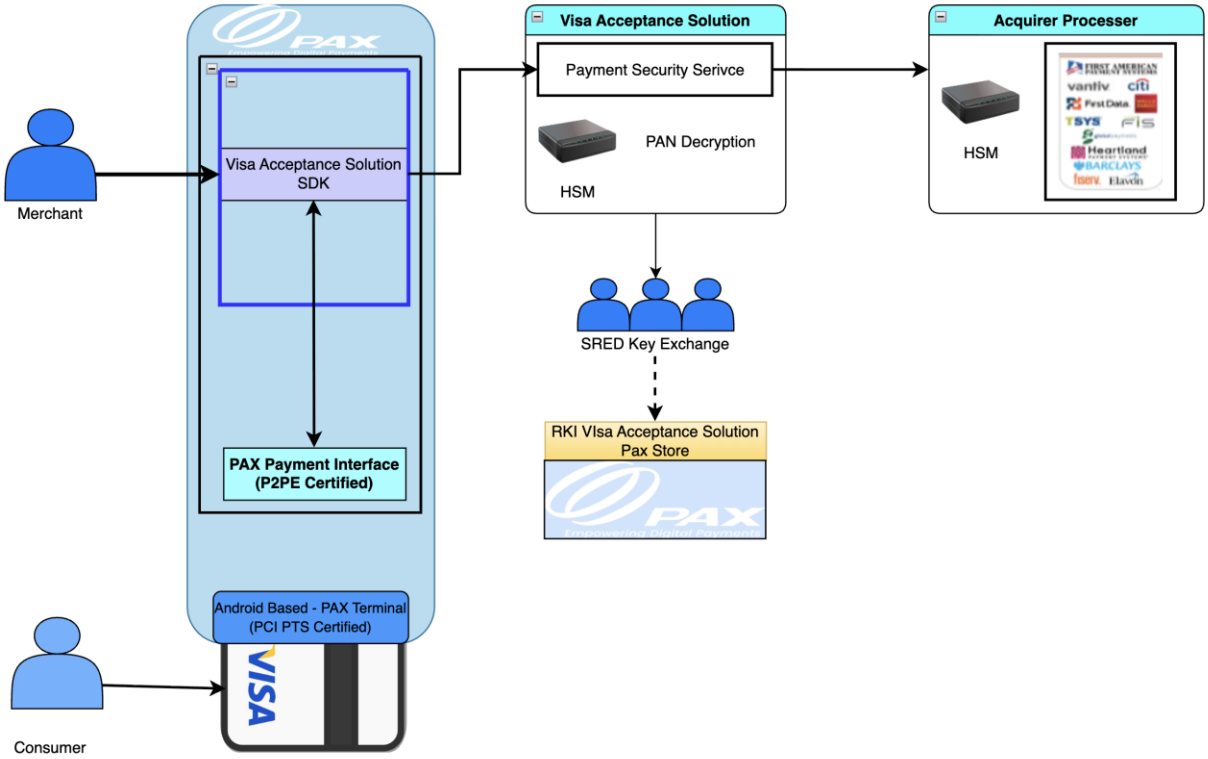


Figure 10

3A-1.3.2 PAX A920 PRO

Merchant Card Presentment Zone 1:

Zone 1 is in merchant location where a credit card is presented to the merchant for payment. Credit card is swiped, dipped, or tapped on a PTS approved terminal (with SRED encryption enabled) after the terminal prompts the card holder with payment data. Once card is used, card data is immediately encrypted in SRED and passed on encrypted to the Merchant Zone 2.

Merchant Zone 2:

Zone 2 includes Visa Accetance Solution application that manages connectivity with POS system and the terminal in semi-integrated manner. The function of Visa Accetance Solution application is to receive payments dollar amount from the Visa Accetance Solution Accept POS application and pass the request over to the terminal. Terminal API receives the payments application and prompts the consumer to use the credit card. Once data is encrypted as described in Zone 1, the data is passed back to Visa Accetance Solution application which then routes transaction and encrypted credit card data back to Visa Accetance Solution in Zone 3.

Visa Acceptance Solutions Secure Zone 3:

Zone three includes data acceptance, decryption and forwarding for authorizations. Following steps are followed over secure connectivity in this zone.

1. Visa Accetance Solution receives encrypted payment data and authorization request. It connects to HSM's to decrypt first and then formats the message in manner that is consumable by Visa Acceptance Solutions. Connectivity between Visa Accetance Solution and Visa Acceptance Solutions is over secure connections for maximum security.
2. Visa Acceptance Solutions receives the data in the clear and processes it for other products based on merchant choice. Visa Acceptance Solutions then routes the data over to appropriate processor for authorization over secure connectivity.
3. Processor accepts the payment data in the clear over secure connectivity and processes the transactions before sending the authorization backwards through the same process. No clear text PAN data is sent back to the merchant.

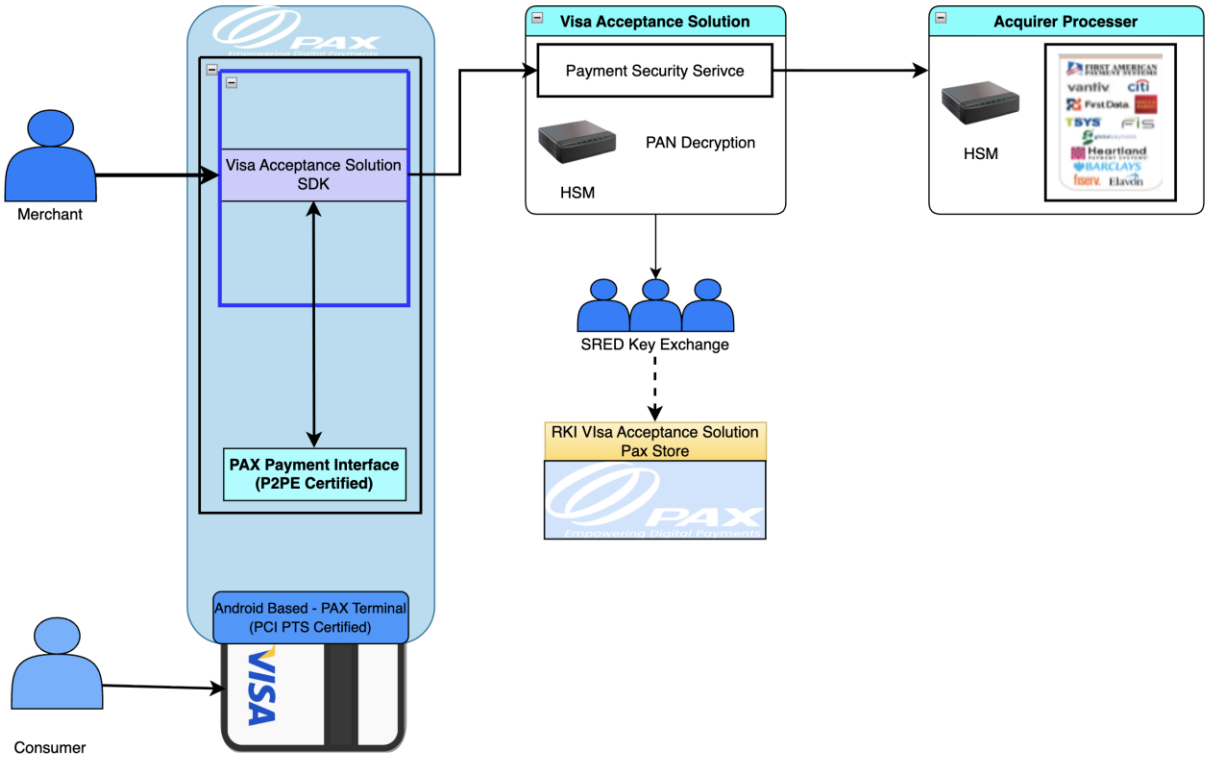


Figure 11

3A-1.3.3 PAX A920 MAX

Merchant Card Presentment Zone 1:

Zone 1 is in merchant location where a credit card is presented to the merchant for payment. Credit card is swiped, dipped, or tapped on a PTS approved terminal (with SRED encryption enabled) after the terminal prompts the card holder with payment data. Once card is used, card data is immediately encrypted in SRED and passed on encrypted to the Merchant Zone 2.

Merchant Zone 2:

Zone 2 includes Visa Accetance Solution application that manages connectivity with POS system and the terminal in semi-integrated manner. The function of Visa Accetance Solution application is to receive payments dollar amount from the Visa Accetance Solution Accept POS application and pass the request over to the terminal. Terminal API receives the payments application and prompts the consumer to use the credit card. Once data is encrypted as described in Zone 1, the data is passed back to Visa Accetance Solution application which then routes transaction and encrypted credit card data back to Visa Accetance Solution in Zone 3.

Visa Acceptance Solutions Secure Zone 3:

Zone three includes data acceptance, decryption and forwarding for authorizations. Following steps are followed over secure connectivity in this zone.

1. Visa Accetance Solution receives encrypted payment data and authorization request. It connects to HSM's to decrypt first and then formats the message in manner that is consumable by Visa Acceptance Solutions. Connectivity between Visa Accetance Solution and Visa Acceptance Solutions is over secure connections for maximum security.
2. Visa Acceptance Solutions receives the data in the clear and processes it for other products based on merchant choice. Visa Acceptance Solutions then routes the data over to appropriate processor for authorization over secure connectivity.
3. Processor accepts the payment data in the clear over secure connectivity and processes the transactions before sending the authorization backwards through the same process. No clear text PAN data is sent back to the merchant.

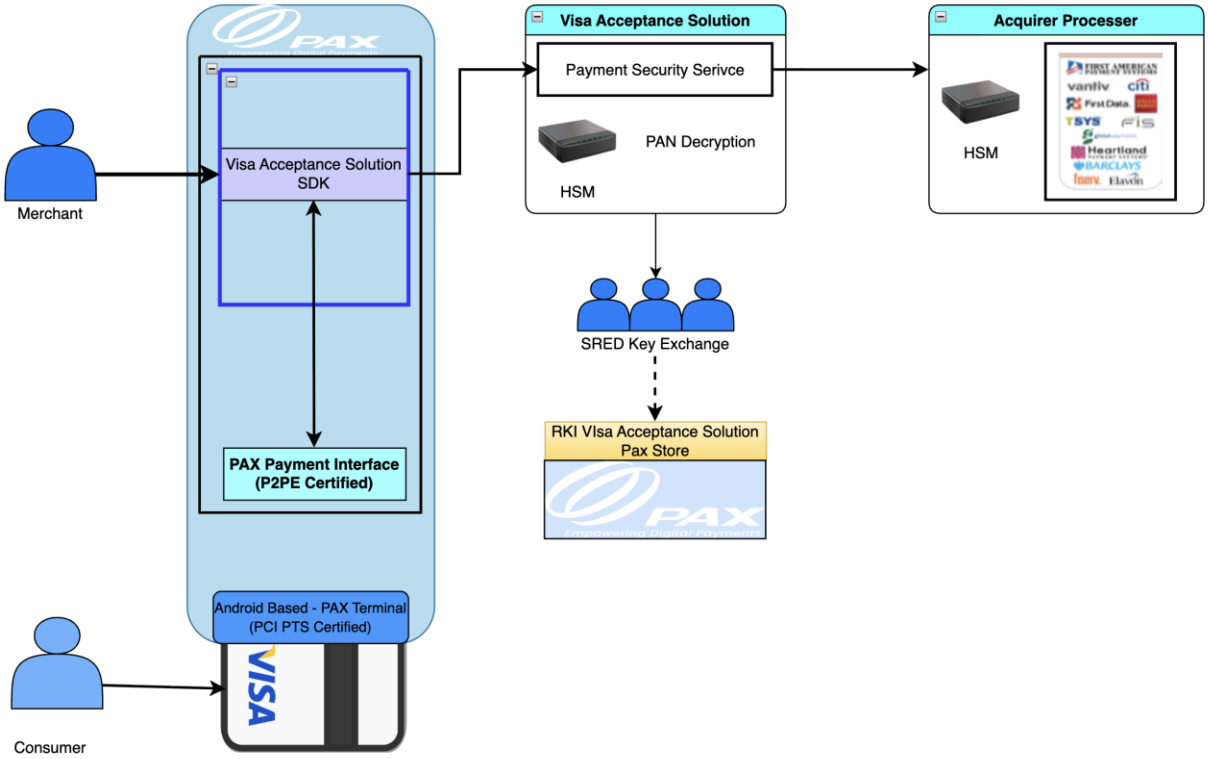


Figure 12

3A-1.3.4 PAX A35

Merchant Card Presentment Zone 1:

Zone 1 is in merchant location where a credit card is presented to the merchant for payment. Credit card is swiped, dipped, or tapped on a PTS approved terminal (with SRED encryption enabled) after the terminal prompts the card holder with payment data. Once card is used, card data is immediately encrypted in SRED and passed on encrypted to the Merchant Zone 2.

Merchant Zone 2:

Zone 2 includes Visa Accetance Solution application that manages connectivity with POS system and the terminal in semi-integrated manner. The function of Visa Accetance Solution application is to receive payments dollar amount from the Visa Accetance Solution Accept POS application and pass the request over to the terminal. Terminal API receives the payments application and prompts the consumer to use the credit card. Once data is encrypted as described in Zone 1, the data is passed back to Visa Accetance Solution application which then routes transaction and encrypted credit card data back to Visa Accetance Solution in Zone 3.

Visa Acceptance Solutions Secure Zone 3:

Zone three includes data acceptance, decryption and forwarding for authorizations. Following steps are followed over secure connectivity in this zone.

1. Visa Accetance Solution receives encrypted payment data and authorization request. It connects to HSM's to decrypt first and then formats the message in manner that is

consumable by Visa Acceptance Solutions. Connectivity between Visa Accetance Solution and Visa Acceptance Solutions is over secure connections for maximum security.

2. Visa Acceptance Solutions receives the data in the clear and processes it for other products based on merchant choice. Visa Acceptance Solutions then routes the data over to appropriate processor for authorization over secure connectivity.
3. Processor accepts the payment data in the clear over secure connectivity and processes the transactions before sending the authorization backwards through the same process. No clear text PAN data is sent back to the merchant.

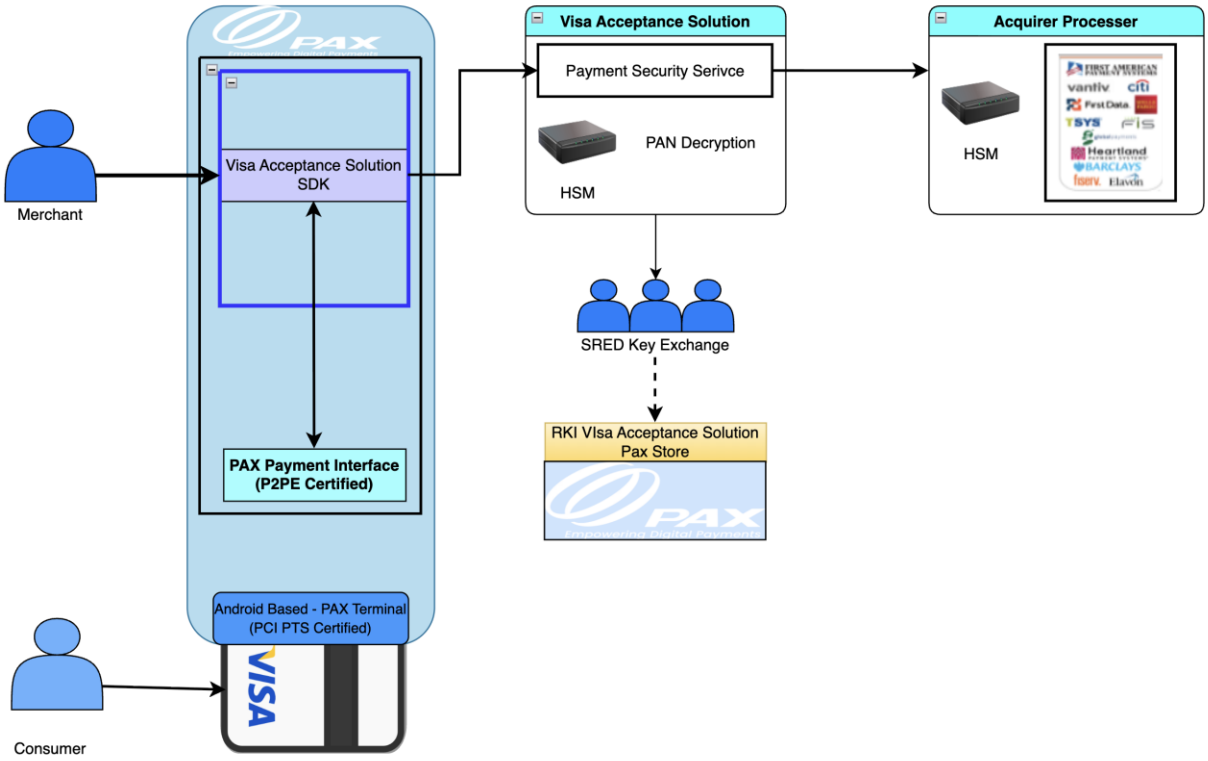


Figure 13

3A-1.3.5 PAX A77

Merchant Card Presentment Zone 1:

Zone 1 is in merchant location where a credit card is presented to the merchant for payment. Credit card is swiped, dipped, or tapped on a PTS approved terminal (with SRED encryption enabled) after the terminal prompts the card holder with payment data. Once card is used, card data is immediately encrypted in SRED and passed on encrypted to the Merchant Zone 2.

Merchant Zone 2:

Zone 2 includes Visa Accetance Solution application that manages connectivity with POS system and the terminal in semi-integrated manner. The function of Visa Accetance Solution application is to receive payments dollar amount from the Visa Accetance Solution Accept POS

application and pass the request over to the terminal. Terminal API receives the payments application and prompts the consumer to use the credit card. Once data is encrypted as described in Zone 1, the data is passed back to Visa Accetance Solution application which then routes transaction and encrypted credit card data back to Visa Accetance Solution in Zone 3.

Visa Acceptance Solutions Secure Zone 3:

Zone three includes data acceptance, decryption and forwarding for authorizations. Following steps are followed over secure connectivity in this zone.

1. Visa Accetance Solution receives encrypted payment data and authorization request. It connects to HSM's to decrypt first and then formats the message in manner that is consumable by Visa Acceptance Solutions. Connectivity between Visa Accetance Solution and Visa Acceptance Solutions is over secure connections for maximum security.
2. Visa Acceptance Solutions receives the data in the clear and processes it for other products based on merchant choice. Visa Acceptance Solutions then routes the data over to appropriate processor for authorization over secure connectivity.
3. Processor accepts the payment data in the clear over secure connectivity and processes the transactions before sending the authorization backwards through the same process. No clear text PAN data is sent back to the merchant.

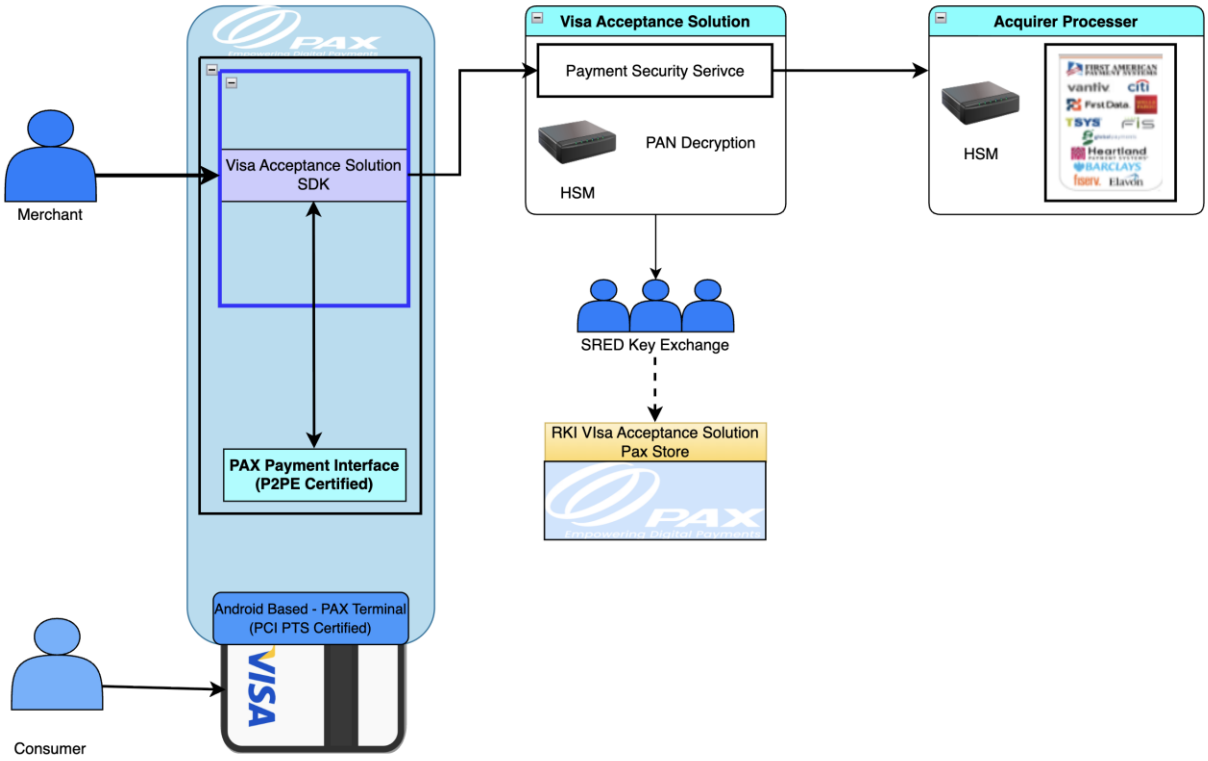


Figure 14

3A-1.3.6 PAX A50

Merchant Card Presentment Zone 1:

Zone 1 is in merchant location where a credit card is presented to the merchant for payment. Credit card is swiped, dipped, or tapped on a PTS approved terminal (with SRED encryption enabled) after the terminal prompts the card holder with payment data. Once card is used, card data is immediately encrypted in SRED and passed on encrypted to the Merchant Zone 2.

Merchant Zone 2:

Zone 2 includes Visa Accetance Solution application that manages connectivity with POS system and the terminal in semi-integrated manner. The function of Visa Accetance Solution application is to receive payments dollar amount from the Visa Accetance Solution Accept POS application and pass the request over to the terminal. Terminal API receives the payments application and prompts the consumer to use the credit card. Once data is encrypted as described in Zone 1, the data is passed back to Visa Accetance Solution application which then routes transaction and encrypted credit card data back to Visa Accetance Solution in Zone 3.

Visa Acceptance Solutions Secure Zone 3:

Zone three includes data acceptance, decryption and forwarding for authorizations. Following steps are followed over secure connectivity in this zone.

1. Visa Accetance Solution receives encrypted payment data and authorization request. It connects to HSM's to decrypt first and then formats the message in manner that is consumable by Visa Acceptance Solutions. Connectivity between Visa Accetance Solution and Visa Acceptance Solutions is over secure connections for maximum security.
2. Visa Acceptance Solutions receives the data in the clear and processes it for other products based on merchant choice. Visa Acceptance Solutions then routes the data over to appropriate processor for authorization over secure connectivity.
3. Processor accepts the payment data in the clear over secure connectivity and processes the transactions before sending the authorization backwards through the same process. No clear text PAN data is sent back to the merchant.

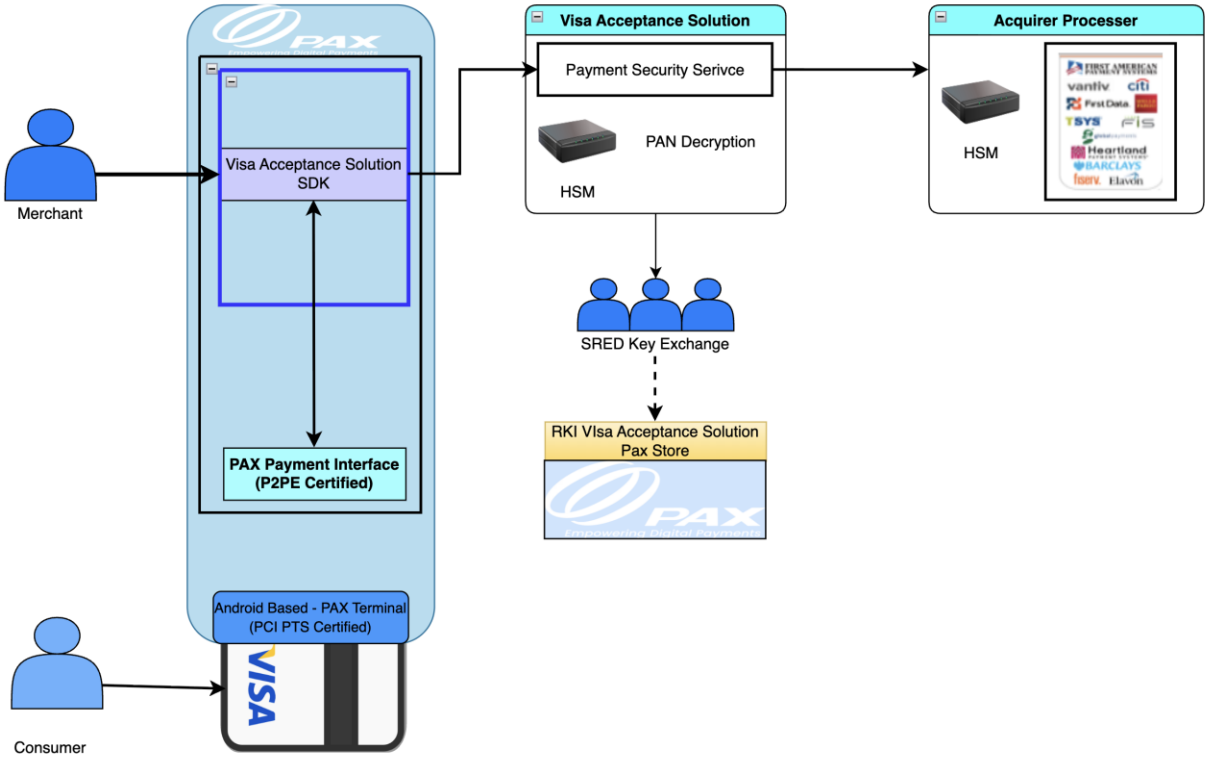


Figure 15

3A-1.3.7 PAX IM 30

Merchant Card Presentment Zone 1:

Zone 1 is in merchant location where a credit card is presented to the merchant for payment. Credit card is swiped, dipped, or tapped on a PTS approved terminal (with SRED encryption enabled) after the terminal prompts the card holder with payment data. Once card is used, card data is immediately encrypted in SRED and passed on encrypted to the Merchant Zone 2.

Merchant Zone 2:

Zone 2 includes Visa Accetance Solution application that manages connectivity with POS system and the terminal in semi-integrated manner. The function of Visa Accetance Solution application is to receive payments dollar amount from the Visa Accetance Solution Accept POS application and pass the request over to the terminal. Terminal API receives the payments application and prompts the consumer to use the credit card. Once data is encrypted as described in Zone 1, the data is passed back to Visa Accetance Solution application which then routes transaction and encrypted credit card data back to Visa Accetance Solution in Zone 3.

Visa Acceptance Solutions Secure Zone 3:

Zone three includes data acceptance, decryption and forwarding for authorizations. Following steps are followed over secure connectivity in this zone.

1. Visa Accetance Solution receives encrypted payment data and authorization request. It connects to HSM's to decrypt first and then formats the message in manner that is

consumable by Visa Acceptance Solutions. Connectivity between Visa Accetance Solution and Visa Acceptance Solutions is over secure connections for maximum security.

2. Visa Acceptance Solutions receives the data in the clear and processes it for other products based on merchant choice. Visa Acceptance Solutions then routes the data over to appropriate processor for authorization over secure connectivity.
3. Processor accepts the payment data in the clear over secure connectivity and processes the transactions before sending the authorization backwards through the same process. No clear text PAN data is sent back to the merchant.

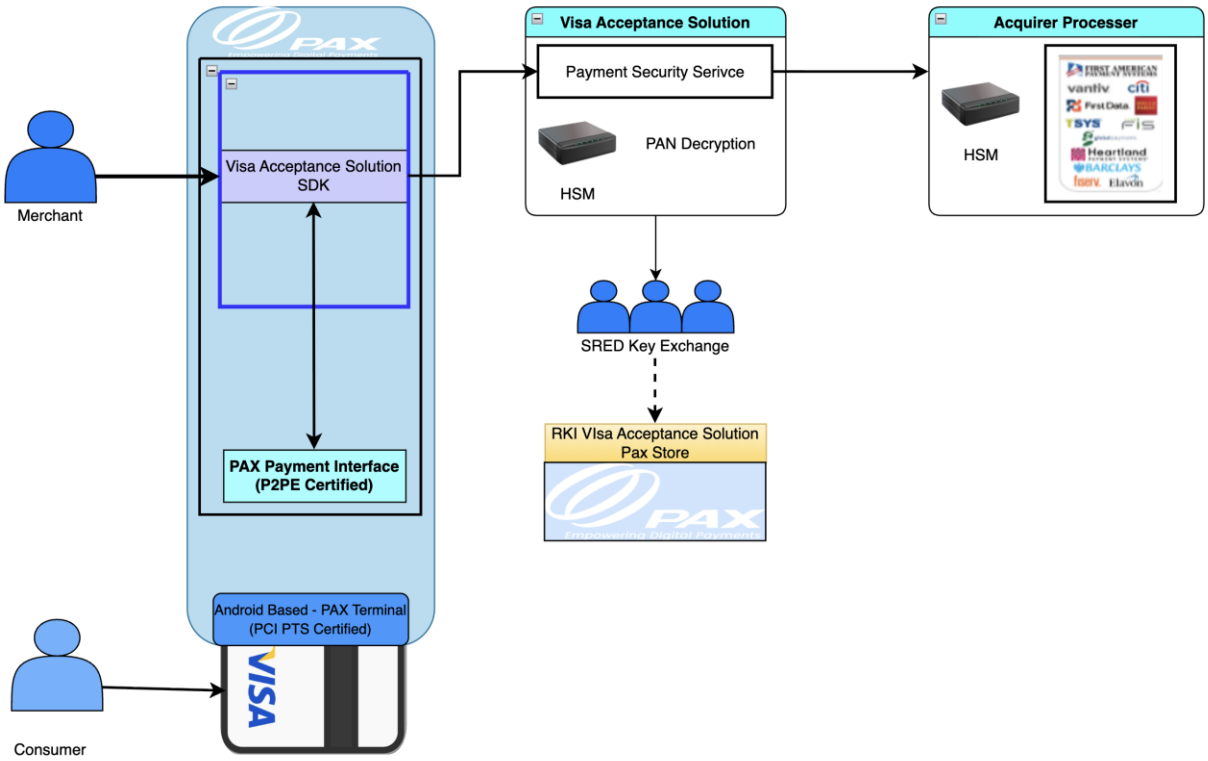


Figure 16

3A-1.4 Data Security

- Merchant does not have access to clear card data.
- Visa Acceptance Solutions solution does not allow data to be transmitted in the clear.
- Visa Acceptance Solutions does not allow full PAN to be printed on a receipt.
- No clear text PAN data is ever transmitted back to the merchant.

3A-2 Manage and Monitor Component Providers (per PCI P2PE V3.1).

Visa Acceptance Solutions requires a yearly review of all component providers to ensure their continued compliance with P2PE standards and listing status. The reports shall include at least the details specified in the “Component Providers ONLY: Report Status to Solution Providers”

sections of Domains 1 and 5, and any additional details as agreed between a component provider and the solution provider. Visa Acceptance Solutions also requires the component providers to immediately report back any changes to the solution during the year. All components are listed on PCI council P2PE approved component website.

3A-2.1 PAX A920

Domain 1 Encryption Application and Device Management	PAX A920 terminal Encryption used is 3DES/DUKPT PAX Encryption Management
Domain 2 Application Security	BroadPOS P2PE 1.02.xx
Domain 3 P2PE Solution Management	Visa Acceptance Solutions P2PE
Domain 5 Decryption Environment	Visa Acceptance Solutions P2PE
Domain 6 P2PE Cryptographic Key Operations and Device Management	Visa Acceptance Solutions P2PE Spencer Technologies (KIF) – France SPT Portal (KIF)- US PAX (CA/RA)

3A-2.2 PAX A920 PRO

Domain 1 Encryption Application and Device Management	PAX A920 PRO terminal Encryption used is 3DES/DUKPT PAX Encryption Management
Domain 2 Application Security	BroadPOS P2PE 1.02.xx
Domain 3 P2PE Solution Management	Visa Acceptance Solutions P2PE
Domain 5 Decryption Environment	Visa Acceptance Solutions P2PE
Domain 6 P2PE Cryptographic Key Operations and Device Management	Visa Acceptance Solutions P2PE Spencer Technologies (KIF) – France SPT Portal (KIF)- US PAX (CA/RA)

3A-2.3 PAX A920 MAX

Domain 1 Encryption Application and Device Management	PAX A920 MAX terminal Encryption used is 3DES/DUKPT PAX Encryption Management
Domain 2 Application Security	BroadPOS P2PE 1.02.xx
Domain 3 P2PE Solution Management	Visa Acceptance Solutions P2PE
Domain 5 Decryption Environment	Visa Acceptance Solutions P2PE
Domain 6 P2PE Cryptographic Key Operations and Device Management	Visa Acceptance Solutions P2PE Spencer Technologies (KIF) – France SPT Portal (KIF)- US PAX (CA/RA)

3A-2.4 PAX A35

Domain 1 Encryption Application and Device Management	PAX A35 terminal Encryption used is 3DES/DUKPT PAX Encryption Management
Domain 2 Application Security	BroadPOS P2PE 1.02.xx
Domain 3 P2PE Solution Management	Visa Acceptance Solutions P2PE
Domain 5 Decryption Environment	Visa Acceptance Solutions P2PE
Domain 6 P2PE Cryptographic Key Operations and Device Management	Visa Acceptance Solutions P2PE Spencer Technologies (KIF) – France SPT Portal (KIF)- US PAX (CA/RA)

3A-2.5 PAX A77

Domain 1	PAX A77 terminal Encryption used is 3DES/DUKPT

Encryption Application and Device Management	PAX Encryption Management
Domain 2 Application Security	BroadPOS P2PE 1.02.xx
Domain 3 P2PE Solution Management	Visa Acceptance Solutions P2PE
Domain 5 Decryption Environment	Visa Acceptance Solutions P2PE
Domain 6 P2PE Cryptographic Key Operations and Device Management	Visa Acceptance Solutions P2PE Spencer Technologies (KIF) – France SPT Portal (KIF)- US PAX (CA/RA)

3A-2.6 PAX A50

Domain 1 Encryption Application and Device Management	PAX A50 terminal Encryption used is 3DES/DUKPT PAX Encryption Management
Domain 2 Application Security	BroadPOS P2PE 1.02.xx
Domain 3 P2PE Solution Management	Visa Acceptance Solutions P2PE
Domain 5 Decryption Environment	Visa Acceptance Solutions P2PE
Domain 6 P2PE Cryptographic Key Operations and Device Management	Visa Acceptance Solutions P2PE Spencer Technologies (KIF) – France SPT Portal (KIF)- US PAX (CA/RA)

3A-2.7 PAX IM 30

Domain 1 Encryption Application and Device Management	PAX IM 30 terminal Encryption used is 3DES/DUKPT PAX Encryption Management
Domain 2	

Application Security	BroadPOS P2PE 1.02.xx
Domain 3 P2PE Solution Management	Visa Acceptance Solutions P2PE
Domain 5 Decryption Environment	Visa Acceptance Solutions P2PE
Domain 6 P2PE Cryptographic Key Operations and Device Management	Visa Acceptance Solutions P2PE Spencer Technologies (KIF) – France SPT Portal (KIF)- US PAX (CA/RA)

3A-2.9 Component and Component Dependency Listing Information

All components below are listed within the Visa Acceptance Solutions P2PE listed solution **Reference #: 2025-01570.001**

A. Encryption Management
    a. Visa Acceptance Solutions P2PE **Reference #: 2025-01570.001**
B. P2PE Components
        i. Portal Secure **Reference #:** 2022-01084.003
        ii. Smart Payment Technologies Key Injection Facility **Reference #:** 2024-01102.006)
        iii. paxRhino Remote Key - **Reference #:** 2023-00841.004
        iv. PAX Certification Authority (PAXCA) - **Reference #:** 2024-001238.008
        v. UCP Key Injection Facility **Reference #:** 2022-01269.002
        vi. PAX Certification Authority (PAXCA) - **Reference #:** 2024-001238.008
        vii. Smart Payment Technologies Encryption **Reference #:** 2023-01102.005
    b. P2PE Application Supported
        i. BroadPOS P2PE
            1. 1.02.xx **Reference #:** 2022-00841.003
    c. PCI-Approved Devices Supported
        i. PAX Technology A920 Pro - **Reference #:** #4-40273
        ii. PAX Technology A77 - **Reference #:** #4-40269
        iii. PAX Technology A50 - **Reference #:** #4-90062
        iv. PAX Technology A920 MAX - **Reference #:** #4-40350
        v. PAX Technology IM30 - **Reference** #: #4-30371
        vi. PAX Technology A920 - **Reference #:** #4-40215
        vii. PAX Technology A35 - **Reference #:** #4-40305
    d. PCI-Approved HSMs Supported
        i. Thales DIS CPL USA, Inc., payShield 10K - **Reference #:** 4-40266
        ii. Futurex, GSP3000 **Reference #: 4-70046**

3A-2.10 Solution Change Management and Resolution Process

Any issues found or changes to the solution can be resolved by reaching out to the following component providers under their listed information. Examples of changes that must have processes to ensure P2PE controls are changes in third-party service providers and changes in the overall solution architecture. All listings and reports are validated In January of each year. The following contacts can be reached immediately for any change management to the solution and resolution.

1. Visa Acceptance Solutions – In-person Accept: Acceptance Devices
   Youssef Elarnaodi
   Tel: +49891208568
   Email: yelarnao@visa.com
2. Secure Retail
   managedservices@secure-retail.com
   Tel: +44 (0)1530 511150

   Email: SSGsupport@spencertech.com
3. POS Portal
   Tel: +1 855-838-4611
   Email: support@posportal.com
4. PAX Technology Inc.
   PAX Customer Support
   Tel: +001 (877) 859-009
   Email: support@pax.us

3A-3 Suspicious Activity Reporting

3A 3.1 Suspicious Activity

To report suspicious activity for the following situations, a call center system is setup.

- Physical device breaches
- Tampered, missing, or substituted devices
- Unauthorized logical alterations to devices
- Failure of any device security control
- Unauthorized use of sensitive functions
- Encryption/decryption failures

3A 3.1.1 Immediate Actions and Call Center Support

All physical device breaches can be reported directly to Visa Acceptance Solutions support at following number:

1. Visa Acceptance Solutions Card Present Support

   UK Toll Free: 02039012015
   US Toll Free: (855) 477-1184

France Toll Free: +33 157329224
A live person will be available to assist.

Once a report is made to Visa Acceptance Solutions, the Customer Support Representative will take immediate actions to suspend the devices from transacting on the system.
Visa Acceptance Solutions can block terminals from transacting in its boarding tool which then connects to the Visa Accetance Solution gateway automatically and turns off the terminal.
The terminal must remain offline until the integrity of the device is verified and the P2PE encryption mechanism can be restored.

3A 3.1.2 Re-enabling a POI Device

A device can not be re-enabled until one of the following conditions is met:
• The issue has been resolved and P2PE encryption functionality is restored and re-enabled, or

• The merchant has provided written notification, signed by a merchant executive officer, formally requesting stopping of P2PE encryption services, according to the solution provider's procedures as defined in P2PE Security Requirements and Testing Procedures, Version 3.1, Requirement 3A-3.2.1.

3A 3.2 Transactions Anomaly Detection

- Visa Accetance Solution has setup a set of rules in their system for Visa Acceptance Solutions that will monitor for suspicious activity. Rule set includes:
  - Requiring authorization of each device with proper credentials.
  - Proper decryption of data through Visa Accetance Solution system. Visa Accetance Solution will error out when data presented is not encrypted.
  - Review of transactions after a threshold is met.
- Immediate shutdown of devices that are not compliant to encrypted transaction flow.
- Manual reporting to Visa Acceptance Solutions of anomaly detection and device shutdown.
- Visa Acceptance Solutions team will work directly with the client to ensure their data protection is maintained and replacement devices are shipped out.
- Visa Acceptance Solutions merchants are not allowed to stop encryption in their environment.

3A-3.3 Log of Suspected Activity

The following log will be maintained by Visa Acceptance Solutions for all active devices.

Merchant ID	Store ID/Location	Terminal ID	Terminal Make/ Model/ Serial #	Date/Time of incident	Duration of device downtime	Date/Time that Issue was resolved.	Incidence details *

* Details to include if any account data was transmitted from the POI device(s) during the time that encryption was malfunctioning or disabled

3A-3.4 Service Monitoring and Incident Management, Escalation Process

The intent of this section is to provide an overview of the Visa Acceptance Solutions monitoring and incident management processes that support and restore service disruptions on the Visa Acceptance Solutions platform. This section will describe the scope of support and a sample framework of how to determine priority and severity of incidents impacting the customer.

3A-3.4.1 Service Monitoring and Incident Management Overview

Visa Acceptance Solutions has the capability to support clients that experience issues impacting their businesses. Issues are typically reported in one of two ways: client-reported or Visa Acceptance Solutions-detected. Internal tools and systems help monitor different levels of activity to detect any anomalies in the network in real-time. When clients encounter issues impacting their ability to run their normal business transactions, they can contact Visa Acceptance Solutions customer support (reference "business as usual" process flow in Customer Support module).

As indicated in the Customer Support module, Visa Acceptance Solutions clients will follow a new support process for card-present (CP) scenarios. For card-not-present (CNP) scenarios, clients will follow the "business as usual" Visa Acceptance Solutions support process referenced in the previous module as well. However, for cases that are more critical and may impact multiple clients across the Visa Acceptance Solutions platform, there is an incident management process established to troubleshoot, communicate, and resolve these issues. For more severe incidents that require cross-functional business involvement, the crisis management team will be engaged to provide additional support and communication, and to assist with activating the Business Incident Response Plan (BIRP).

There are multiple triggers and thresholds that could dictate the severity of an incident, which will then determine the level of priority, communication, and engagement needed to address the issue. The following tables are a framework of what is currently used for the overall Visa Acceptance Solutions incident management process, with sample triggers and thresholds that may be used.

Priority Level	Triggers/Thresholds		Actions
P1 – Critical	Network/System/Interface Outage	• 100% hard down on any of the following interfaces: ○ Payment Gateway ○ Enterprise Business Center (EBC)	• Target first response: 10 minutes from time ticket was logged • All hands-on deck until issue is mitigated
	Failed/Declined Transactions	• Intermittent transactional impact 30 minutes in duration or greater	

		• Impact of 1000 transactions or greater within 10 minutes in duration	• Frequency of communication to customer: Updates as pertinent until resolution • Target time to resolve: 2 hours (24x7x365) • Root cause completed within 3 business days • 3rd Parties may contact the Visa Acceptance Solutions NOC and/or Visa Acceptance Solutions Customer Support to notify about issues detected and start investigation
	Financial Impact	• Settlement/Funding Delay • Major business impact (e.g., >$100,000 USD revenue loss, reputational damage, etc.)	
	External and third-party impacting events	• Third party outages (e.g., Six, Visa Accetance Solution, etc.) • Define criteria for 3rd party outages • 3rd Party Processor and Software connections/partners monitored at both ends, with NOC-to-NOC communication in place as needed	

	Reporting	• Gateway report generation issues, resulting in potential reconciliation issues:
		  ○ Payment batch summary
		  ○ Payment batch detail
		  ○ Payment event details reports	

Priority Level	Triggers/Thresholds		Actions

P2 – High	Network/System/Interface Outage	• Degradation to following interfaces:
		  ○ Gateway
		  ○ Enterprise Business Center (EBC)
			• Target first response: 30 minutes from time ticket was logged
			• Product Development and Operations engaged until mitigated
			• Frequency of communication to customer: Updates as pertinent until resolution
			• Target time to resolve: 4 hours (business hours)
			• Root cause completed within 5 business days
			• 3rd Party may contact either the Visa Acceptance Solutions NOC and/or Card Present Support to alert of detected issues

	Failed/Declined Transactions	• Intermittent transactional impact 20 minutes in duration or greater • Impact of 500 transactions or greater within 10 minutes in duration	
	Financial Impact	• Greater than $50,000 USD business impact (e.g., revenue loss, reputational damage, etc.)	
	External and third-party impacting events	• Third party outages (e.g., Six, Visa Accetance Solution, etc.) • 3rd Party Processor and Software connections/partners monitored at both ends, with NOC-to-NOC communication in place as needed	

Priority Level	Triggers/Thresholds		Actions
P3 – Medium	Failed/Declined Transactions	• Intermittent transactional impact 10 minutes in duration or greater • Impact of 250 transactions or greater within 10 minutes in duration • Workaround is available until issue is fixed	• Target first response: 2 hours from time ticket was logged • Frequency of communication to customer: Updates as pertinent until resolution
	Financial Impact	• Greater than $10,000 USD business impact (e.g., revenue loss, reputational damage, etc.)	

	External and third-party impacting events	• Third party outages (e.g., Six, Visa Accetance Solution, etc.) • 3rd Party Processor and Software connections/partners monitored at both ends, with NOC-to-NOC communication in place as needed	• Target time to resolve: 8 hours (business hours) • Root cause completed within 5 business days • 3rd Parties may contact the Visa Acceptance Solutions NOC and/or Visa Acceptance Solutions Customer Support to notify about issues detected and start investigation
	Maintenance or releases	• Routine VISA ACCEPTANCE SOLUTIONS maintenance or releases that should be done after hours/non-peak hours • Routine 3rd party maintenance or releases that should be done after hours/non-peak hours	

Priority Level	Triggers/Thresholds		Actions
P4 – Minor	Any other issues	• Ad hoc report requests • Data export requests • Change of business rules • Incident that does not interfere with store activity (e.g., planned releases and maintenance)	• Target first response: 24 hours from time ticket was logged • Frequency of communication to customer: Updates as pertinent until resolution • Target time to resolve: 1 business day

3A-3.5 Incident Response Reporting

The following items must be addressed in an Incident Repsonse Report for any applicable incident response for P2PE control failures, the following is required but not limited to:

- Identification that a failure has occurred
- Identifying the root cause
- Determining remediation needed to address root cause
- Identifying and addressing any security issues that occurred during the failure
- Updating the solution and/or controls to prevent cause from recurring

3B P2PE Implementation Manual (PIM)

3B-1.1 PIM's

Visa Acceptance Solutions has developed, maintained, and disseminated required P2PE Instruction Manual (PIM) to merchants for the below listed devices. The PIM is distributed to a new merchant when they are onboard for a below listed device in a P2PE solution and provided to merchants upon request.

PIMs for each of the below terminals can be located also on the Visa Acceptance Solutions Knowledge Base.

Content for the PIM is maintained in accordance with the mandatory PIM Template.

PIMs:

- Pax A920
- Pax A920 Pro
- Pax A920 Max
- Pax A35
- Pax A77
- Pax A50
- IM 30

3B-1.2 Yearly PIM Review

Visa Acceptance Solutions P2PE PIMs will be reviewed on annual basis to ensure all information is current. Visa Acceptance Solutions will also update the PIMs when new components or devices are added. All affected merchants will be notified with the changes to the PIMs. Reviews and updates to the PIMs and to this document will be tracked by under a Jira Ticket, with the ticket being assigned to individuals during the review process.

3C Miscellanous

3C-1 Formal Agreements with Providers

PAX

Secure Retail

UCP KIF

POS Portal

3C-2 SCD Management

The third parties listed have approved agreements to provide the Solution Provider with the following:

- Notification of any changes that require a Delta Change per the P2PE Program Guide
- Details of the change, including the reason for the change
- Updated list of any dependencies included in the Delta Change (e.g., POI devices, P2PE applications, and/or HSMs) used in the solution

- Evidence of adherence to PCI's process for P2PE Delta Changes

Third Parties: PAX, Secure Retail, POS Portal

Addendum A

Postproduction Support Overview

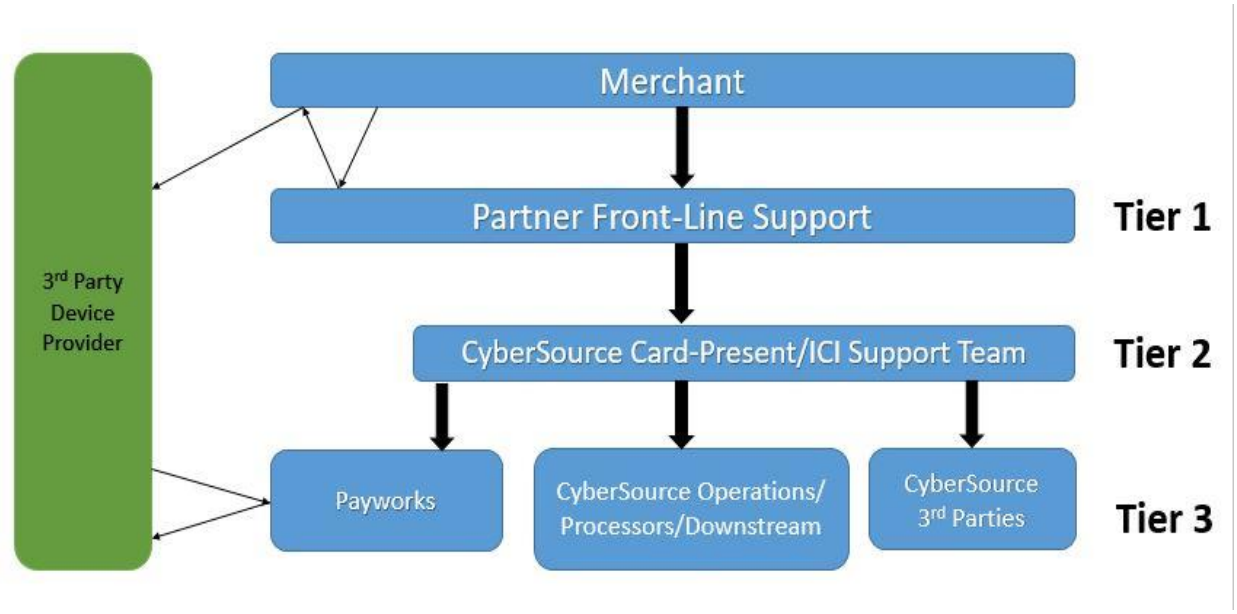
Postproduction Support

This section provides an overview of the Visa Acceptance Solutions customer support model and process, with a specific focus on the Visa Acceptance Solutions Card Present/Integrated Commerce (ICI) Support Model. This section will include the scope of services and support to be provided, high-level process flows, troubleshooting guidance, and roles and responsibilities.

The support model for the Integrated Commerce Solution is multi-tiered. A Front-Line Support Partner will act as the Tier 1 or "first stop" to handle basic support for card-present transactions, devices, and setup. This team will also handle initial triage of issue types that require escalation to—and are backed up by—the Visa Acceptance Solutions Integrated Commerce Card Present (CP) Support Team.

Areas of escalated support assistance would fall under the following responsible parties÷

- Visa Acceptance Solutions Card Present (CP) Support for back-end payment, reporting, reconciliation, or transaction data issues
- Device Distributor for fulfillment, installation, or post-live hardware-related issues
- Acceptance Solution Provider (via the Visa Acceptance Solutions CP Support team) for issues relating to the Acceptance Devices SDKsetup, configuration, or software live-update issues.



Visa Acceptance Solutions is currently building out its cross-regional support model and will share updates as this is accomplished. This current model and specifics of this document pertain to UK. Implementations (where Secure Retail is the Distributor), French implementations (where Spencer Technologies is the Distributor), and U.S. implementations

(where POS Portal is the Distributor). Additional partners and/or steps may come into play as the model is further developed and applied across geographical regions (additional partners in EMEA, the U.S., etc.).

Support Hours and Languages

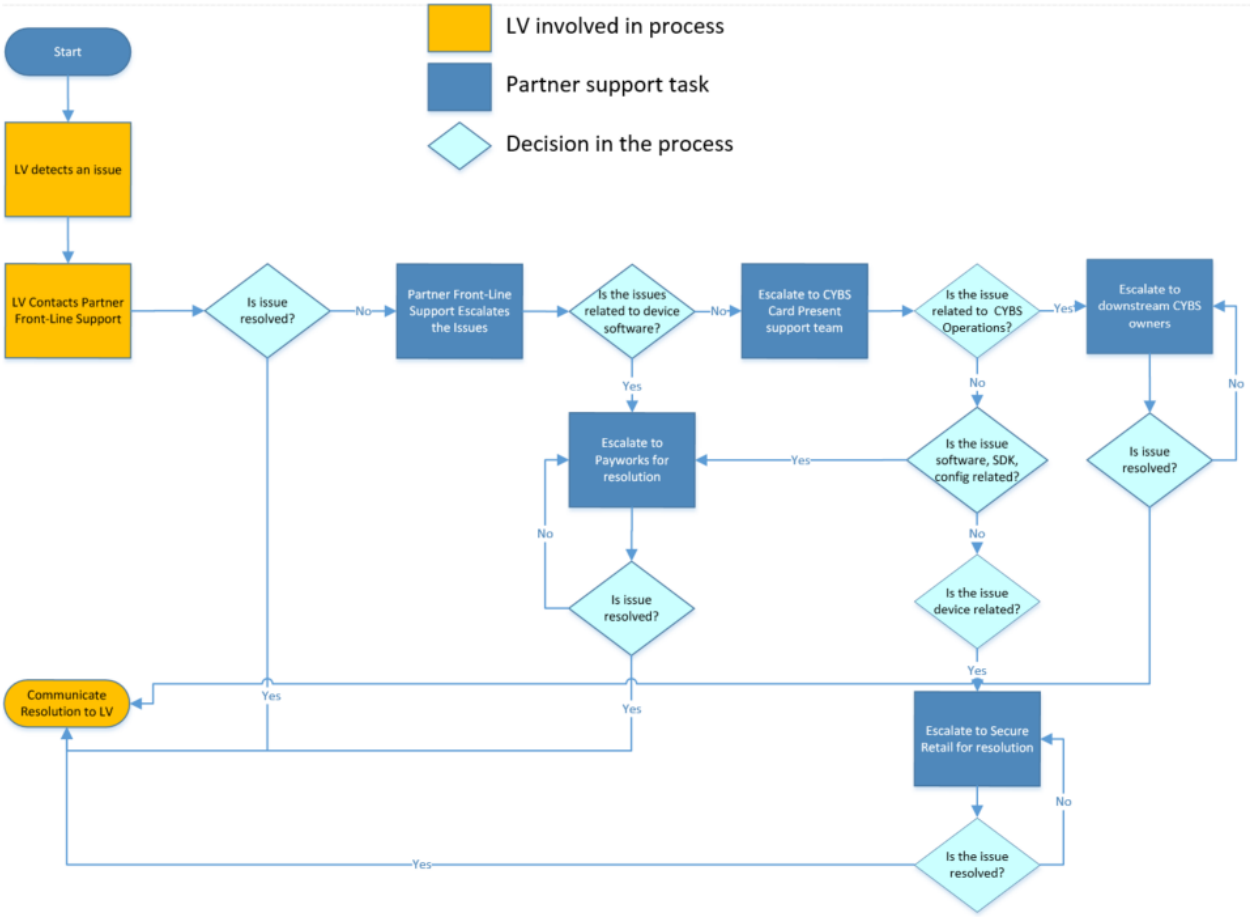
	Ramp package (e.g., initial days post-launch, until Front-Line Support partner is integrated)	Ongoing
Hours	7 days a week from one hour before store opening until one hour after store closure	7 days a week from one hour before store opening to one hour after store closure
Language	English and French	English and French

Above is an illustrative package only. Additional languages can be included in a language package option to cover multi-region implementations, though additions of new countries/regions that require not-previously supported language may require a 120+ day lead time for staffing and training purposes. Support hours illustrated here cover the store operating hours and may vary from location to location.

	Front-Line Support Partner	**Visa Acceptance Solutions Card Present (CP) Support**	**Distributor**	**Acceptance Solution Provider**
Core Function	First stop for most issues. Serves as the gatekeeper for issue resolution and initiating escalations	Back-end payment, reporting, reconciliation, or transaction data issues. Also, an escalation point for routing issues to partners of all types.	Fulfillment, installation, or post-live device-related issues	Receive escalations from other support teams related to SDK, configuration, or software live-update issues
Hours	24x7	7 days/week during business-plus-1-on-each-side hours	Distributor-dependent	
Language	English, French	English	English	English
Channels / Support models and contact	○ Phone Support ○ E-mail Support ○ eTicket Support	○ Phone Support ○ E-mail Support ○ Visa Acceptance Solutions KB/eTicketing System: https://support.VisaAcceptanceSolutions.com/VISA ACCEPTANCE SOLUTIONSkb/i	○ Phone Support ○ E-mail Support	None Directly to Merchant (escalation/Tier 2 only) ○ E-mail: integrations-VisaAcceptanceSolutions@VisaAccetanceSolution.com ○ Processing-related

		ndex?page=home ○ Visa Acceptance Solutions Business Center: https://ebc.VisaAcceptanceSolutions.com		emergencies: +49 89 215438495

Support Model Escalation Flow



Support Delivery Parties

Merchant Internal IT Support - Merchant's internal support, which could be outsourced or insourced, is primarily responsible for supporting in-store infrastructure, such as power, safety, physical security, physical wired and wireless connectivity.

Front-Line Support Partner - The Front-Line Support Partner will provide basic support for card-present transactions, devices, and setup, as well as initial triage of issue types that require escalated support assistance. The Front-Line Support Partner will be the first stop for most issues that merchant may encounter for post-live support of this solution. The Front-Line

Support team will be backed up by the Visa Acceptance Solutions CP Support team, primarily, which also has the capability to reach out to the Distributor, Acceptance Solution Provider, as well as all business-as-usual Visa Acceptance Solutions partners which may have a part in the transaction flows offered in the solution. While a Distributor plays a direct and prominent role in the initial setup, installation, and early-testing phases of the solution, it will recede to more of an escalation resource in the post-production support model.

Visa Acceptance Solutions Card Present (CP) Support - The Visa Acceptance Solutions CP Support team will serve as an escalated support resource for the solution handling Visa Acceptance Solutions gateway, back-end payments, and reconciliation services. Visa Acceptance Solutions will engage the Acceptance Solution Provider, typically via their web portal, to assist with device configuration and management. Visa Acceptance Solutions CP Support will also handle any questions or issues that have impact over both the card present and e-commerce areas of the integrated payment solution.

Distributor (aka Device Procurement/Fulfillment Partner) - The Distributor will act as an escalation point for issues relating to device fulfillment, installation, or post-live physical hardware issues from the Front-Line Support Partner and/or the Visa Acceptance Solutions CP Support team, depending on the issue type. The Distributor should be able to troubleshoot, resolve, and respond directly to the following types of issues:

- Device Procurement, Installation, and Initial Testing (i.e., upon setup/installation)
- Device Hardware and Connectivity
- Device Warranty and/or Replacement Needs

In some cases, given that typically the Distributor has a role in the installation, usage, and update process for the Acceptance Solution Provider, the merchant could also directly contact the Distributor during the installation or post-live situations, pursuant to any agreement(s) setup directly between the merchant and the Distributor.

Acceptance Solution Provider - The Acceptance Solution Provider provides transaction connectivity to Visa Acceptance Solutions and is the device software partner with responsibility for the device software, original configuration, and upgrades. They will additionally provide escalation-level (Tier 2/3) support for these areas as needed during the installation, testing, and live processing via the Visa Acceptance Solutions CP Support team and/or the Distributor.

The Acceptance Solution Provider is available as an escalation resource for the following types of issues:

- Initial Device Software Provisioning and Testing
- Post-Live Configuration Updates
- Online Software Upgrades or Downloads of the SDK Itself

Other Parties

POS Vendor - is typically responsible for the merchant's POS system, back-end applications, and merchant/system integration.

POS Integrator - is, optionally, a third-party consultancy or technical assistance provider that may help setup, install, integrate, and test the merchant's POS system. They would also work with Visa Acceptance Solutions CP Support and/or Project teams to integrate that solution with the Visa Acceptance Solutions Integrated Commerce Solution for full end-to-end capabilities.

Acquirer/Processor - is the merchant's bank and/or processing entities behind them, to which Visa Acceptance Solutions sends the transaction for processing and settlement activity.

Support Issues and Escalation Paths

Typical support use cases for this solution fall into the following categories. Although this section describes primarily post-production support, there are use cases below which span the full terminal life cycle and related support needs.

1. **Store infrastructure support**
    a. e.g... Store power outage, in-store physical security such as fire, injury, IP/Wireless connectivity. These services are not covered by Visa Acceptance Solutions's solution and should typically be addressed by Merchant IT and/or store operations teams.

Example Issue Type	**Contact Point** (Escalation Point or Front-Line Support Partner)	Back-End Responsible Party (as applicable)
No power in the store	Merchant Store Operations or I.T. Group	N/A
Someone is injured, there's smoke, there's a fire, etc.	Local Municipality Emergency Services	N/A
An alarm has been triggered	Local Municipality Emergency Services	N/A
No dial tone, no IP connectivity, no wireless connectivity	Merchant Store Operations or I.T. Group	N/A

2. **POS system support** (full lifecycle)
    a. Terminal/Hardware, e.g., device malfunction, device error messages, device connectivity to the POS system
    b. Software, e.g., POS system error/ non-functioning, software update failed.
    c. Terminal procurement and management services (aka Estate Management), e.g., replace, retire terminals

Example Issue Type	**Contact Point** (Escalation Point or Front-Line Support Partner)	Back-End Responsible Party (if applicable)
a. Terminal/Hardware, e.g., device malfunction, device error messages, device connectivity to the POS system	Distributor or Visa Acceptance Solutions CP support, depending on the issue type	Distributor, possibly with Acceptance Solution Provider support depending on issue type

Example Issue Type	**Contact Point** (Escalation Point or Front-Line Support Partner)	Back-End Responsible Party (if applicable)
b. Software, e.g., POS system error/non-functioning, software update failed	POS system vendor support or Visa Acceptance Solutions CP support, depending on the issue type	POS system vendor or Acceptance Solution Provider
c. Terminal Procurement and Maintenance services lifecycle support– see below section	Distributor or Visa Acceptance Solutions CP support, depending on the issue type	See below section

3. **Transactional support:**
    a. e.g., Unresponsive/failed transactions, transaction rejects and declines, transaction functionality
4. **Post-transactional support:**
    a. e.g., reconciliation, reporting, settlement, receipt retrieval, chargebacks

Addendum B

Troubleshooting

Accessing PAX A920 Logs

- There are 2 PAX logs in the A920 device. To get the log, the device must be connected to your computer.

- BroadPOS log
  - The BroadPOS logs are located at /sdcard/Android/data/com.pax.us.pay.std.broadpos.p2pe/files with the name broadpos_logyyyymmdd.log

- POSLink log
  - The POSLink log located in the root folder with the name POSLINKyyyymmdd.log

Accessing PAX A920 PRO Logs

- There are 2 PAX logs in the A920 PRO device. To get the log, the device must be connected to your computer.

- BroadPOS log
  - The BroadPOS logs are located at /sdcard/Android/data/com.pax.us.pay.std.broadpos.p2pe/files with the name broadpos_logyyyymmdd.log

- POSLink log
  - The POSLink log located in the root folder with the name POSLINKyyyymmdd.log

Accessing PAX A920 MAX Logs

- There are 2 PAX logs in the A920 MAX device. To get the log, the device must be connected to your computer.

- BroadPOS log
  - The BroadPOS logs are located at /sdcard/Android/data/com.pax.us.pay.std.broadpos.p2pe/files with the name broadpos_logyyyymmdd.log

- POSLink log
  - The POSLink log located in the root folder with the name POSLINKyyyymmdd.log

Accessing PAX A35 Logs

- There are 2 PAX logs in the A35 device. To get the log, the device must be connected to your computer.

- BroadPOS log
  - The BroadPOS logs are located at /sdcard/Android/data/com.pax.us.pay.std.broadpos.p2pe/files with the name broadpos_logyyyymmdd.log

- POSLink log
  - The POSLink log located in the root folder with the name POSLINKyyyymmdd.log

Accessing PAX A77 Logs

- There are 2 PAX logs in the A77 device. To get the log, the device must be connected to your computer.

- BroadPOS log
  - The BroadPOS logs are located at /sdcard/Android/data/com.pax.us.pay.std.broadpos.p2pe/files with the name broadpos_logyyyymmdd.log

- POSLink log
  - The POSLink log located in the root folder with the name POSLINKyyyymmdd.log

Accessing PAX A50 Logs

- There are 2 PAX logs in the A50 device. To get the log, the device must be connected to your computer.

- BroadPOS log
  - The BroadPOS logs are located at /sdcard/Android/data/com.pax.us.pay.std.broadpos.p2pe/files with the name broadpos_logyyyymmdd.log

- POSLink log
  - The POSLink log located in the root folder with the name POSLINKyyyymmdd.log

Accessing PAX IM 30 Logs

- There are 2 PAX logs in the IM 30 device. To get the log, the device must be connected to your computer.

- BroadPOS log
  - The BroadPOS logs are located at /sdcard/Android/data/com.pax.us.pay.std.broadpos.p2pe/files with the name broadpos_logyyyymmdd.log

- POSLink log

- The POSLink log located in the root folder with the name POSLINKyyyymmdd.log

Accessing EFTLink Logs

- If the POS system is Oracle XStore, the EFT Logs can be located in the "/Xstore_<Xstore Version Number – EG V16>/EFTLink/log/" directory.
- This directory has a log file for each day (IE eftlink_<Month MM><Day DD>.txt).
- Using the "Ticket" Number from Xstore (or the receipt) you need to search for transaction. IE if the ticket number is "123", you need to search for "<TransactionNumber>123</TransactionNumber>" in the EFT logs.
- Additionally, you can also search for the transaction by date/time. We can also search by Visa Acceptance Solutions Request ID or Visa Accetance Solution ID, but using the ticket number makes the most sense.

Sample: EFTLink Log

- If the merchant cannot supply us the log for an individual transaction, they should just send us the log for the whole day. There is nothing PCI concerning in there.
- Since multiple Visa Accetance Solution Payservers can also be installed, the logs also indicate what Payserver is being used (and thus what log file you want for the Payserver). IE: 16:00:42,652 [Thread-512] (log.EPSLogger:565) INFO - D0/6936 loading properties file EftlinkConfig.properties from C:\LVM\XSTORE_V16\EFTLINK\server1