The PCI Standards and Where They Apply

John Elliott

Payments, Security, Privacy and Risk Specialist | PCIP

@withoutfire

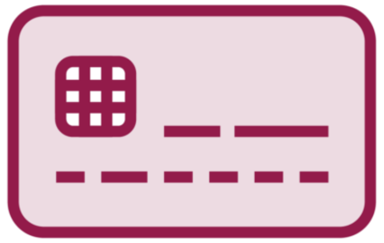
Stopping Criminals with Standards

PCI Standards

Protect Data

EMV Standards

Devalue Stolen Data



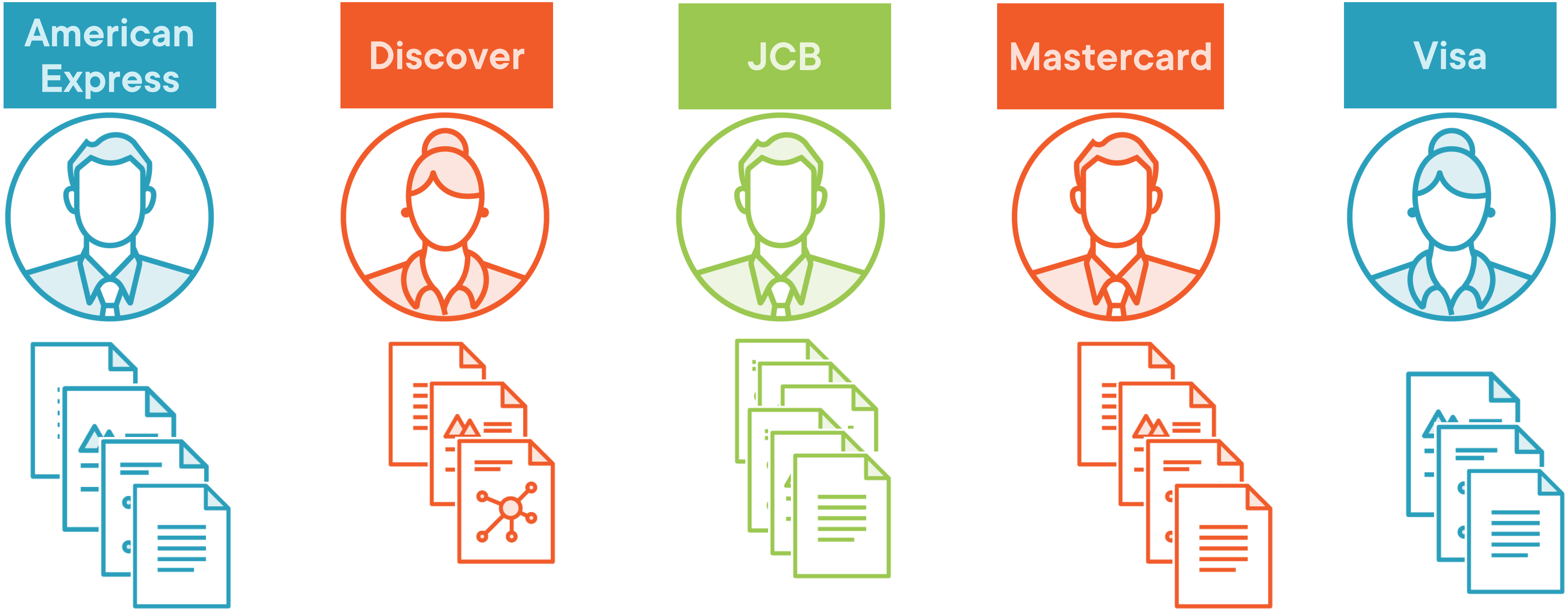
3DS

4258 7896 2476 7852

↓

4987 2175 6187 1111

The Development of Standards



American Express

Discover

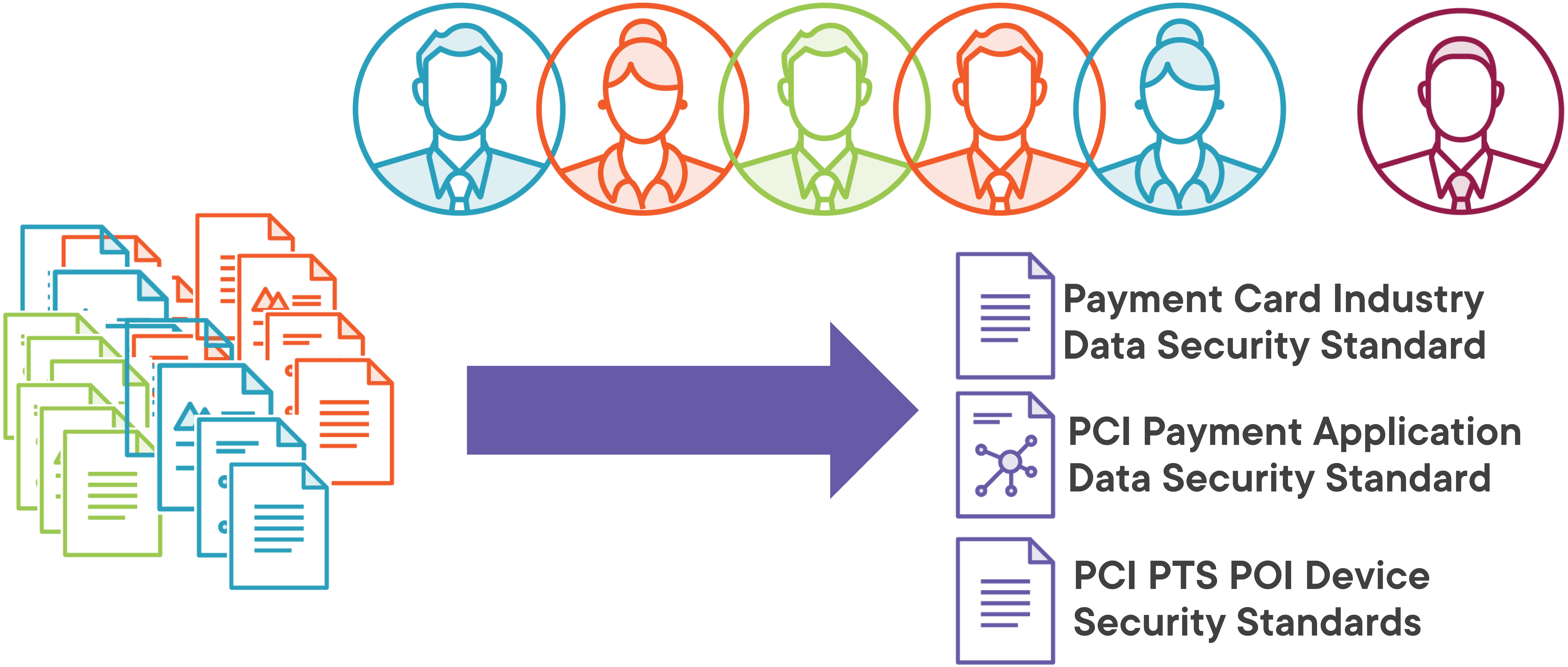
JCB

Mastercard

Visa

The PCI SSC

Payment Card Industry Security Standards Council



Payment Card Industry Data Security Standard

PCI Payment Application Data Security Standard

PCI PTS POI Device Security Standards

Recap

Criminals want cash and things they can trade for cash

They like physical cards

They also like authorization data taken from physical cards

The card schemes' standards tell companies how to protect cards, PINs, and data from criminals

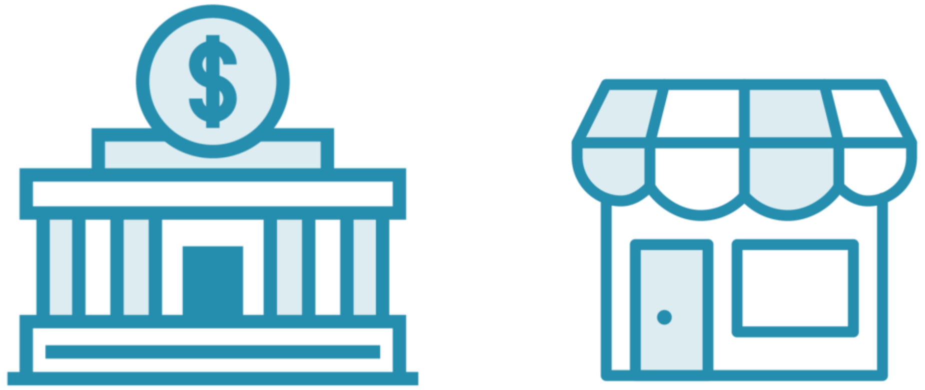
The card schemes created the PCI SSC to manage industry-wide standards

Two Types of PCI Standards

Products and Solutions

Payment Application Data Security
Secure Software Standard
PTS Point of Interaction
PTS Hardware Security Module
Point-to-point Encryption
Software based PIN Entry on COTS
Contactless Payments on COTS
3DS Software Development Kit

Organizations



Data Security Standard
Secure Software Lifecycle
PIN
Token Service Provider
3DS Core
Card Production – Logical & Physical

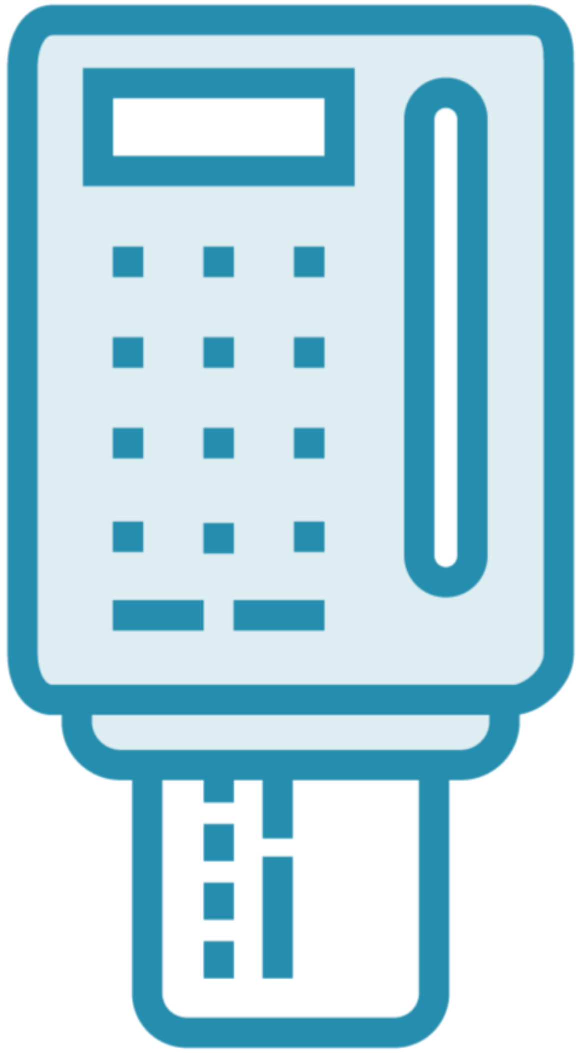
Data Security Standards

Data Security Standard (PCI DSS)

Software Security Framework
  - Software Security Standard
  - Secure Software Lifecycle

Payment Application Data Security Standard (PA DSS) – in retirement

PIN-related Standards



PIN Transaction Security (PCI PTS)
- Point of Interaction (PTS POI)
- Hardware Security Module (PTS HSM)

PIN Security Requirements (PCI PIN)

Whole Payment Systems

Point-to-Point Encryption (P2PE)

Software Based PIN Entry on Commercial-off-the-shelf Devices (SPoC)

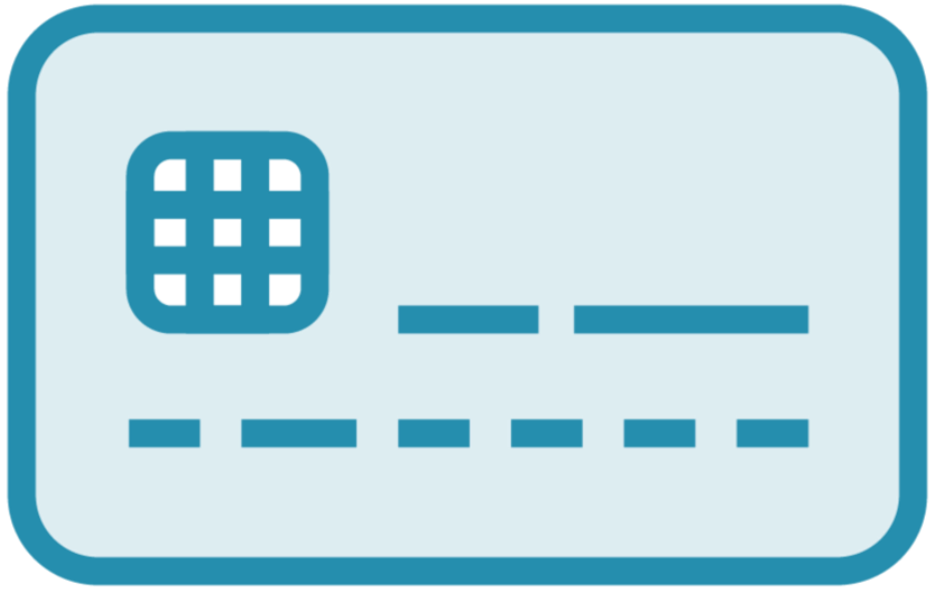
Contactless Payments on Commercial-off-the shelf Devices (CPoC)

Security of Payment Systems

Token Service Provider (TSP)

Three Domain Security (3DS)
  - **Core (3DS Core)**
  - **Software Development Kit (3DS SDK)**

Physical Cards



Card Production and Provisioning

- **Logical Security**
- **Physical Security**

PA-QSA

PCI DSS

PIN

PFI

PCIP

QIR

PED

POI

RoV

Sorry...

QSA

HSM

ASV

RoC

PTS

PA-DSS

SAQ

P2PE

AoC

Payment Card Industry Data Security Standard PCI DSS

A standard to protect cardholder data

Mostly logical controls

Some physical controls

Applies to organizations

- Merchants
- Acquirers and Issuers
- Third party service providers

PCI DSS High Level

Build and maintain a secure network and systems

Protect cardholder data

Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

PCI DSS High Level

Build and maintain a secure network and systems

Protect cardholder data

Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

PCI DSS High Level

Build and maintain a secure network and systems

Protect cardholder data

Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

PCI DSS High Level

- Build and maintain a secure network and systems
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

PCI DSS High Level

Build and maintain a secure network and systems

Protect cardholder data

Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

PCI DSS High Level

- Build and maintain a secure network and systems
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

PCI DSS High Level

Build and maintain a secure network and systems

Protect cardholder data

Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

PCI DSS High Level

Build and maintain a secure network and systems

Protect cardholder data

Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

Secure Software Standard

(Replaces PA-DSS)

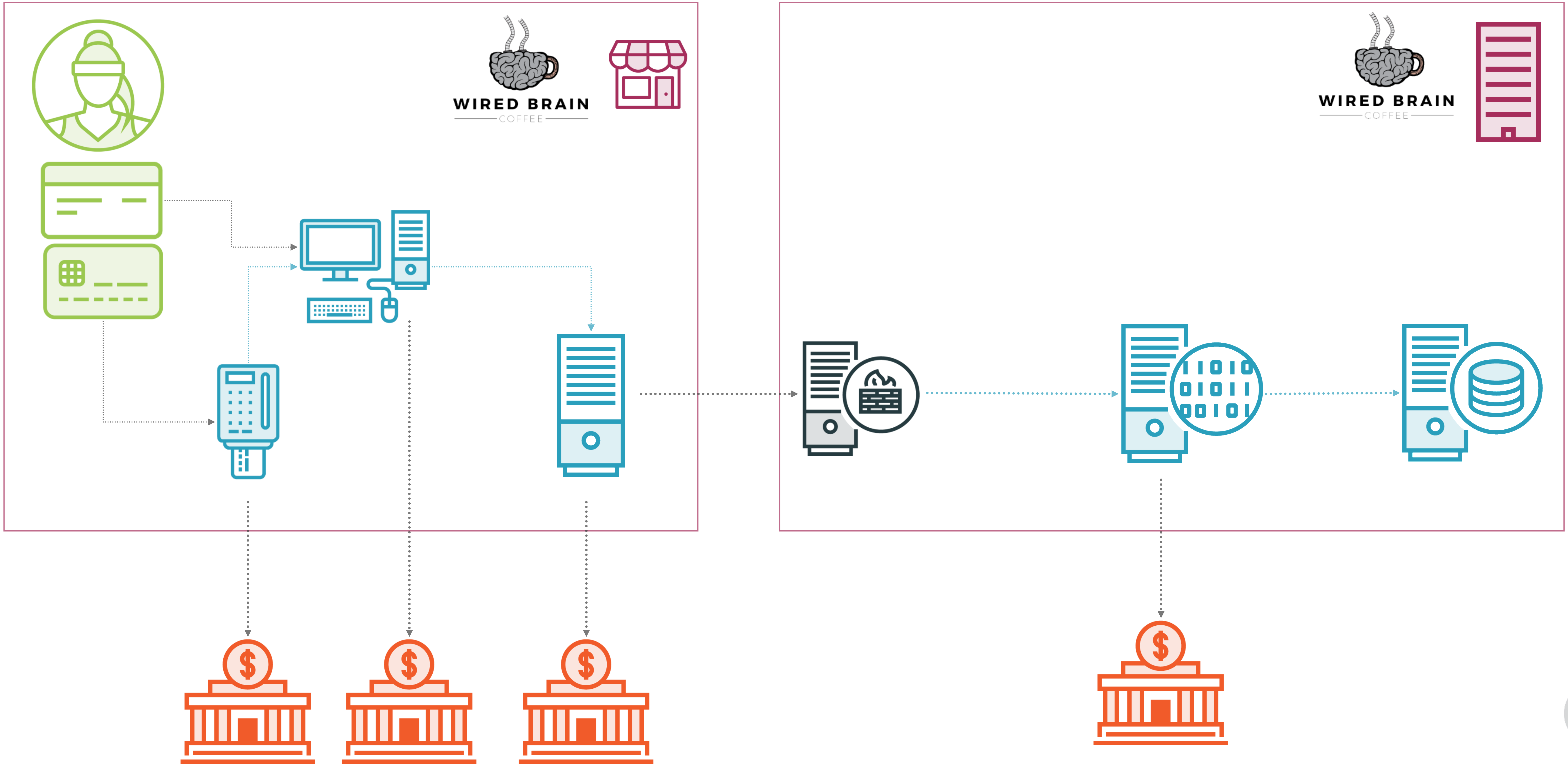
A software development standard

Intended for commercial, off-the-shelf, payment software

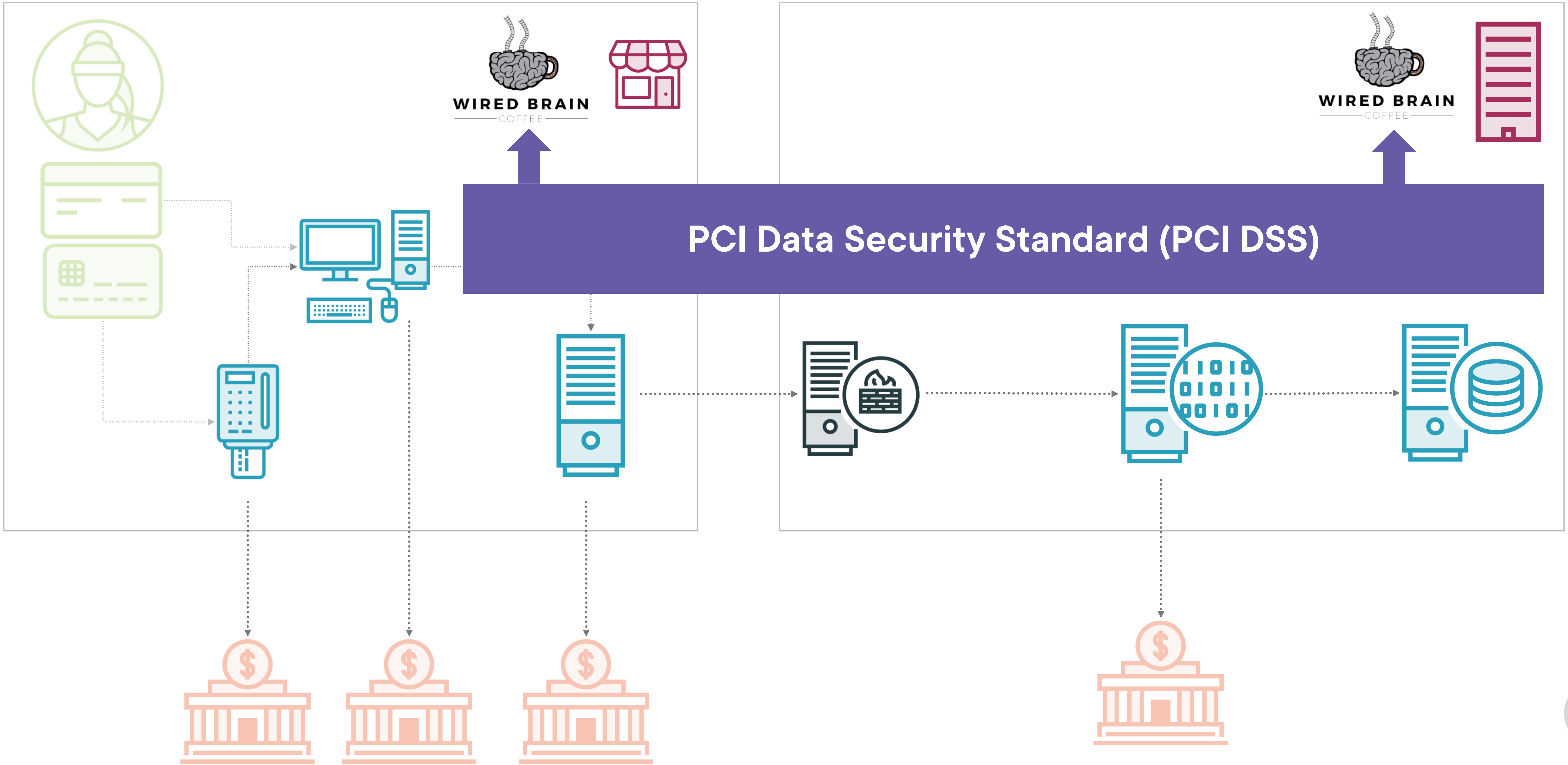
Ensures software enables compliance with PCI DSS

Intended to be modular

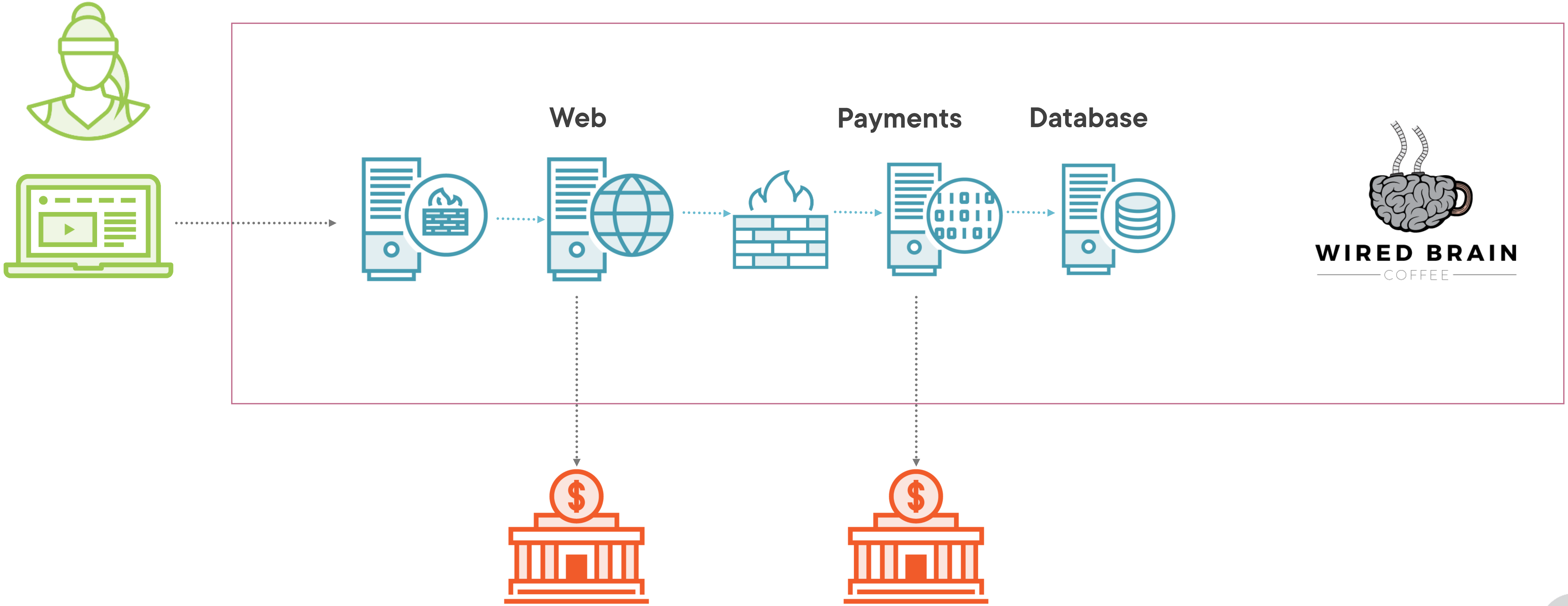
Which Standards Apply?



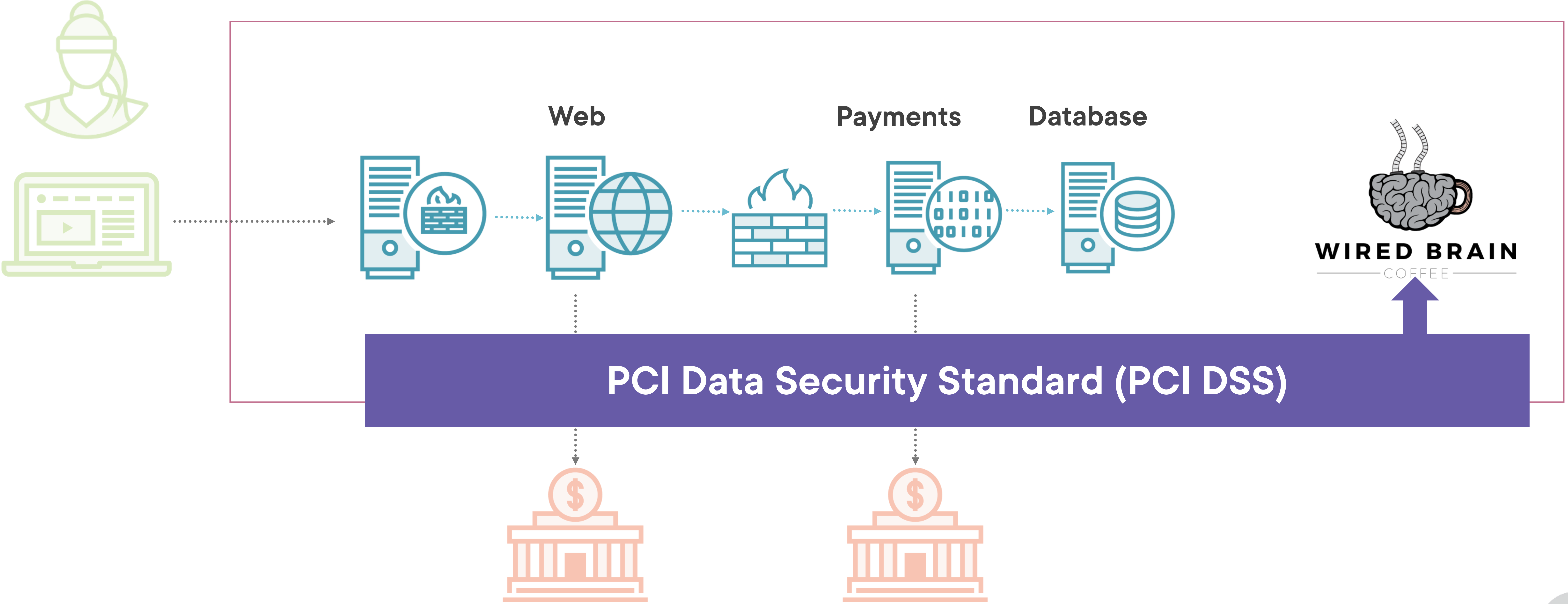
Which Standards Apply?



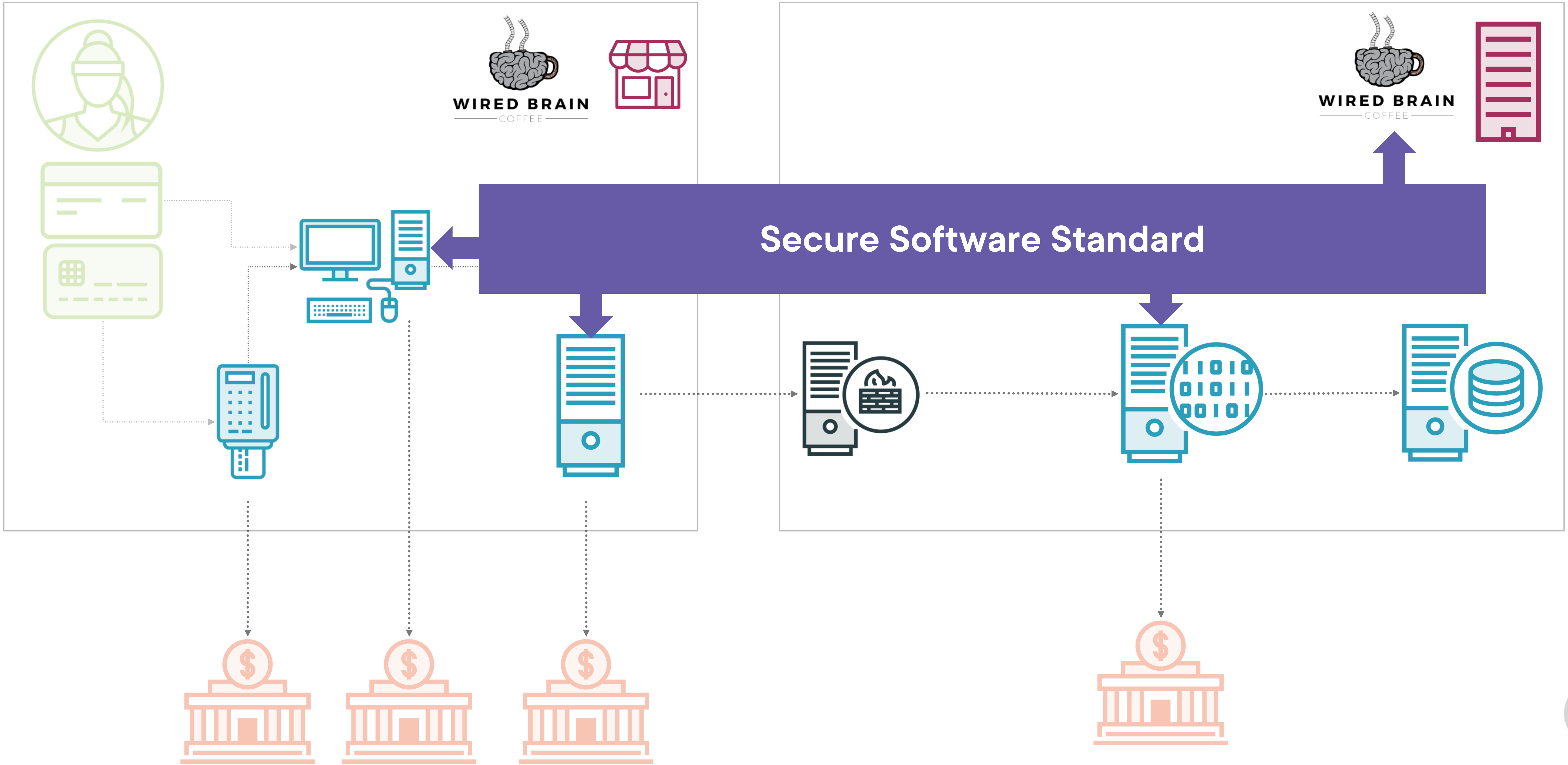
Which Standards Apply?



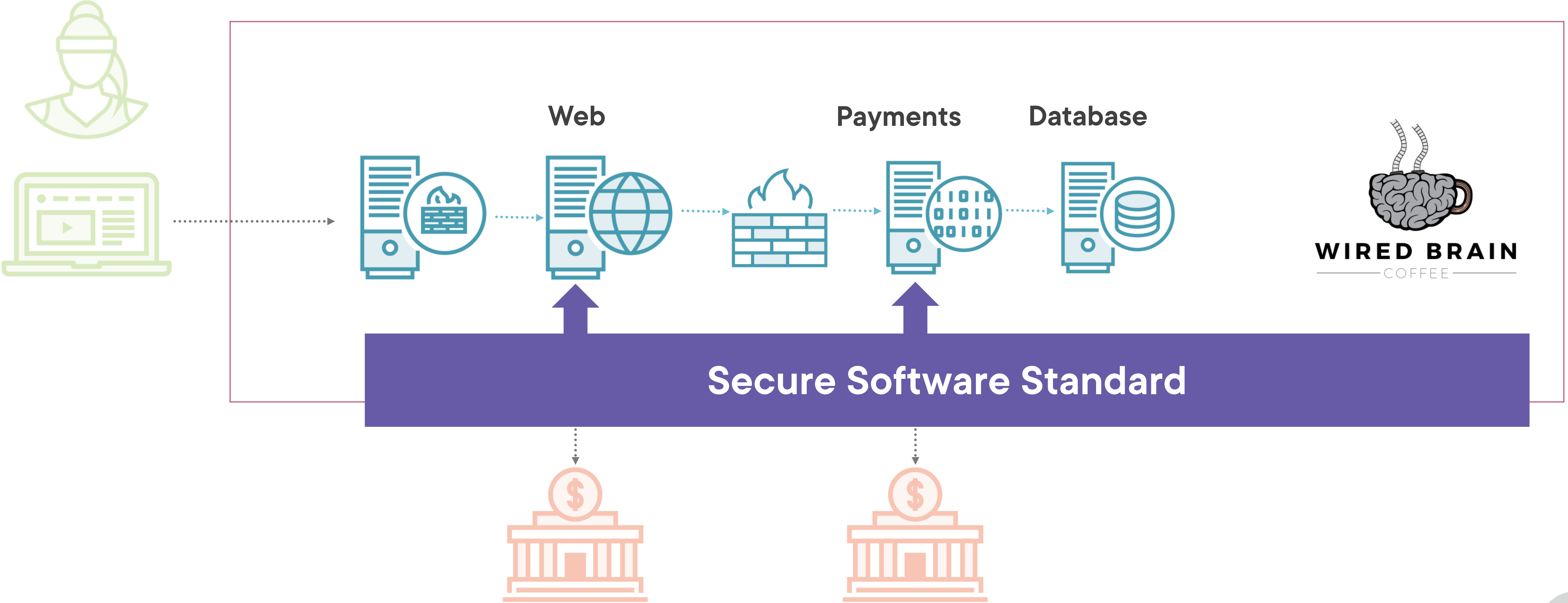
Which Standards Apply?



Which Standards Apply?

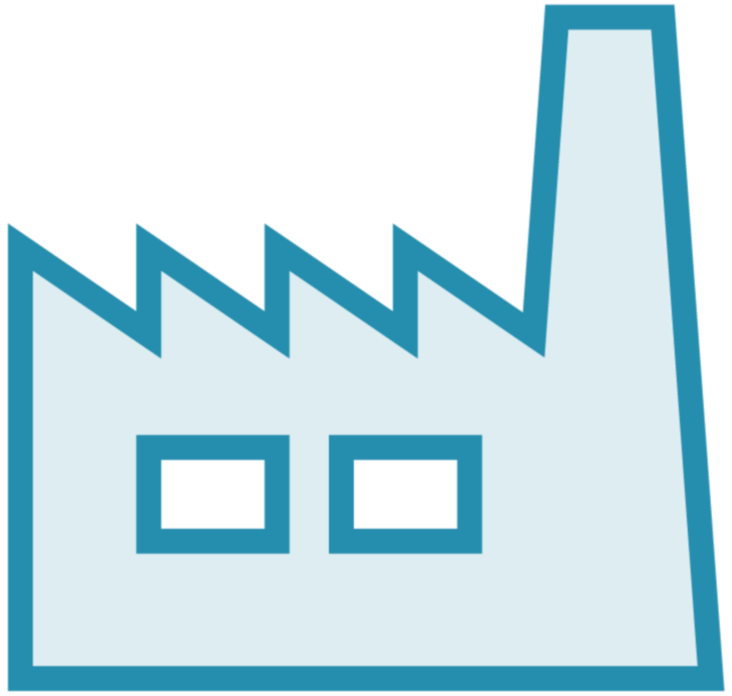


Which Standards Apply?



Secure Software Standard

Secure Software Framework



Secure Software Lifecycle

For companies
that develop software

Secure Software Standard

For commercial software products
that touch payment card data

Standards to Protect PINs

PTS Point of Interaction (PTS POI)

PIN

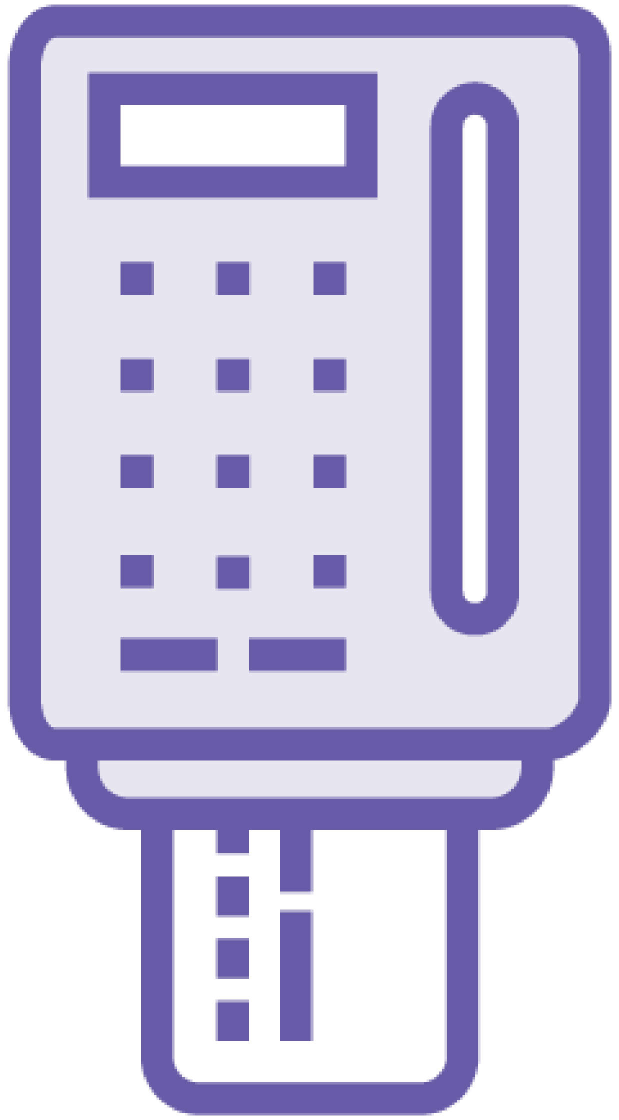
PTS Hardware Security Module (PTS HSM)

Standards to Protect PINs

PTS Point of Interaction (PTS POI)

PIN

PTS Hardware Security Module (PTS HSM)



Tamper resistance

Security of encryption keys

Looked after from manufacture to merchant

These have been attacked by criminals to get card data and PINs

Standards to Protect PINs

PTS Point of Interaction (PTS POI)

PIN

PTS Hardware Security Module (PTS HSM)

Standards to Protect PINs

PTS Point of Interaction (PTS POI)

PIN

PTS Hardware Security Module (PTS HSM)

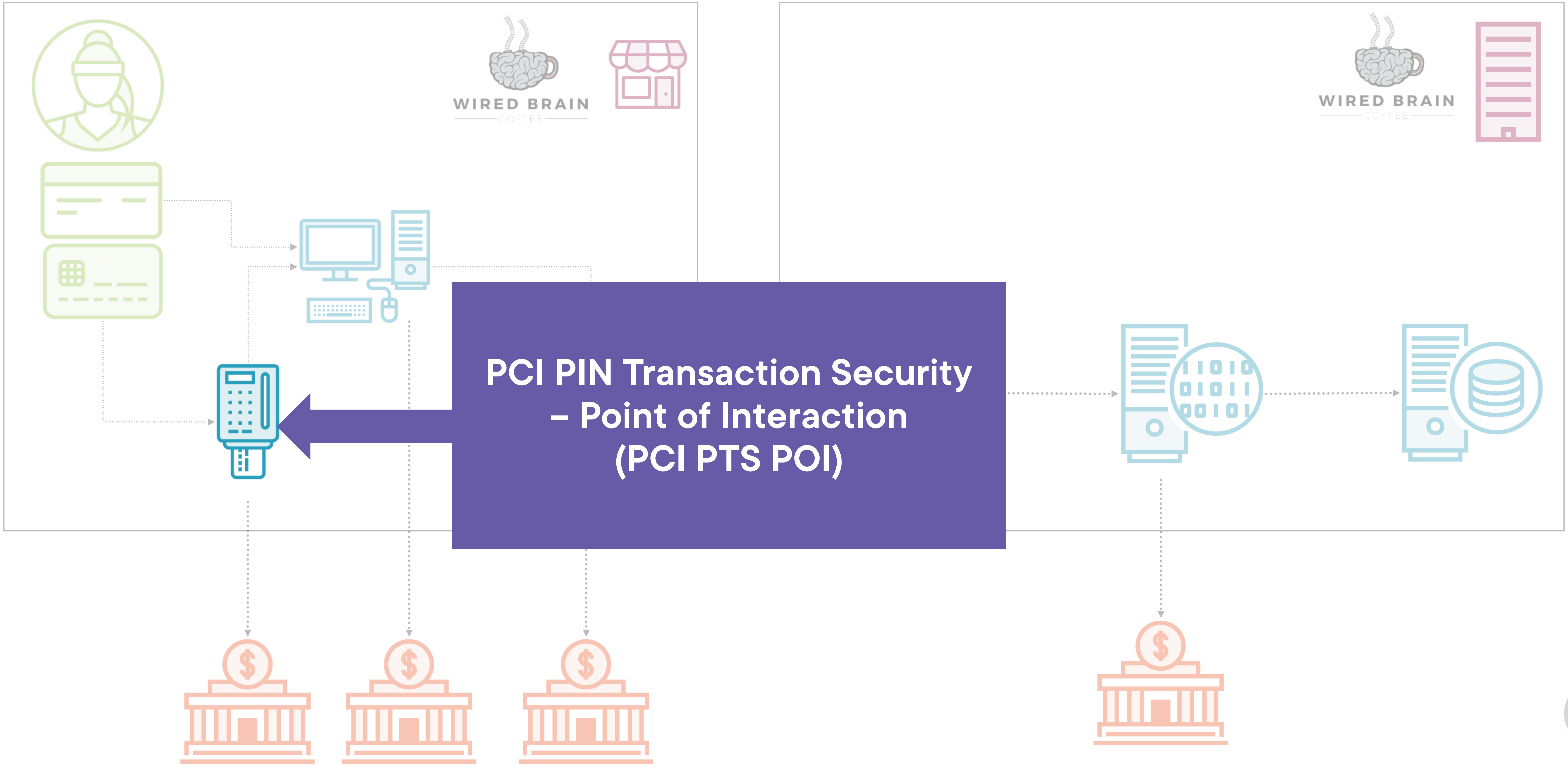
Standards to Protect PINs

PTS Point of Interaction (PTS POI)

PIN

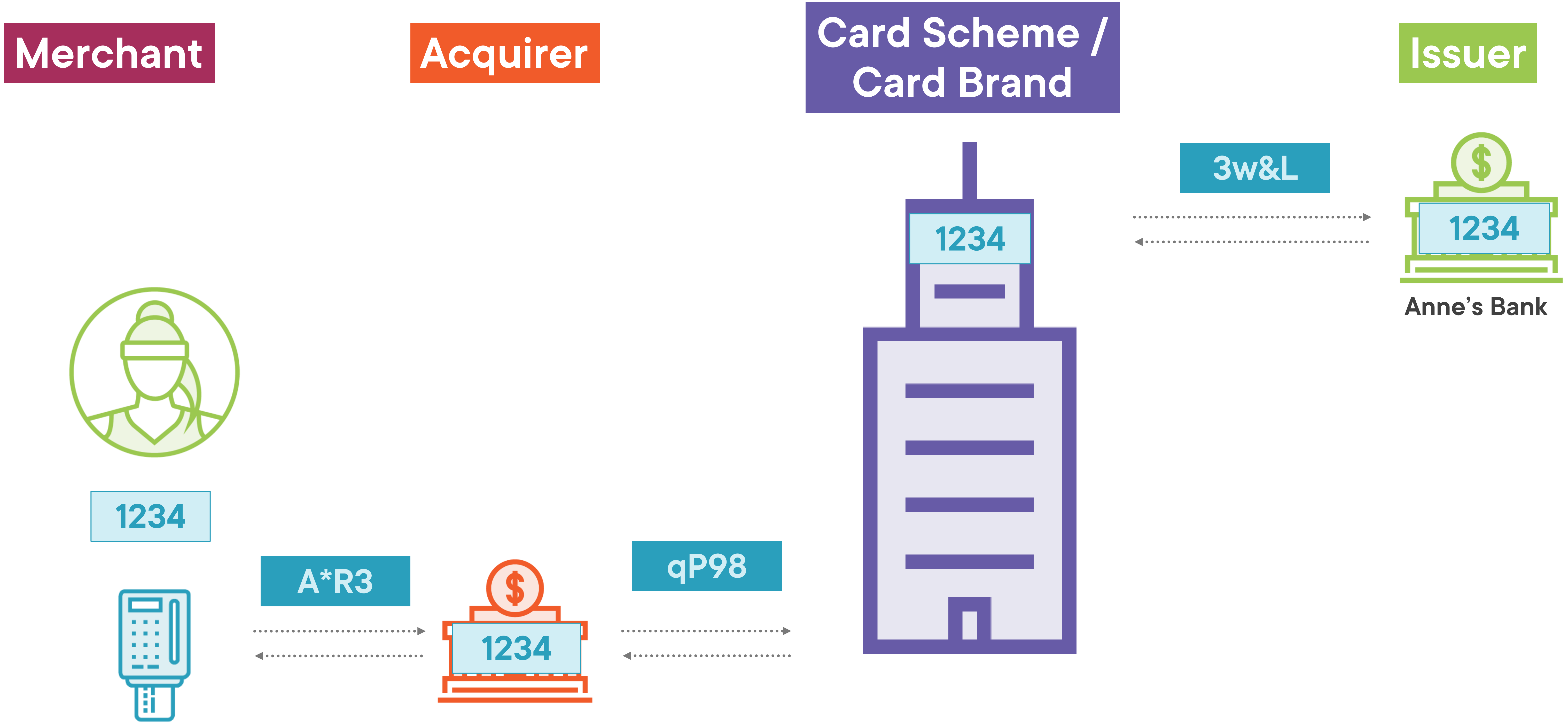
PTS Hardware Security Module (PTS HSM)

PTS POI at an F2F Merchant



PCI PIN Transaction Security – Point of Interaction (PCI PTS POI)

PIN Security in Practice



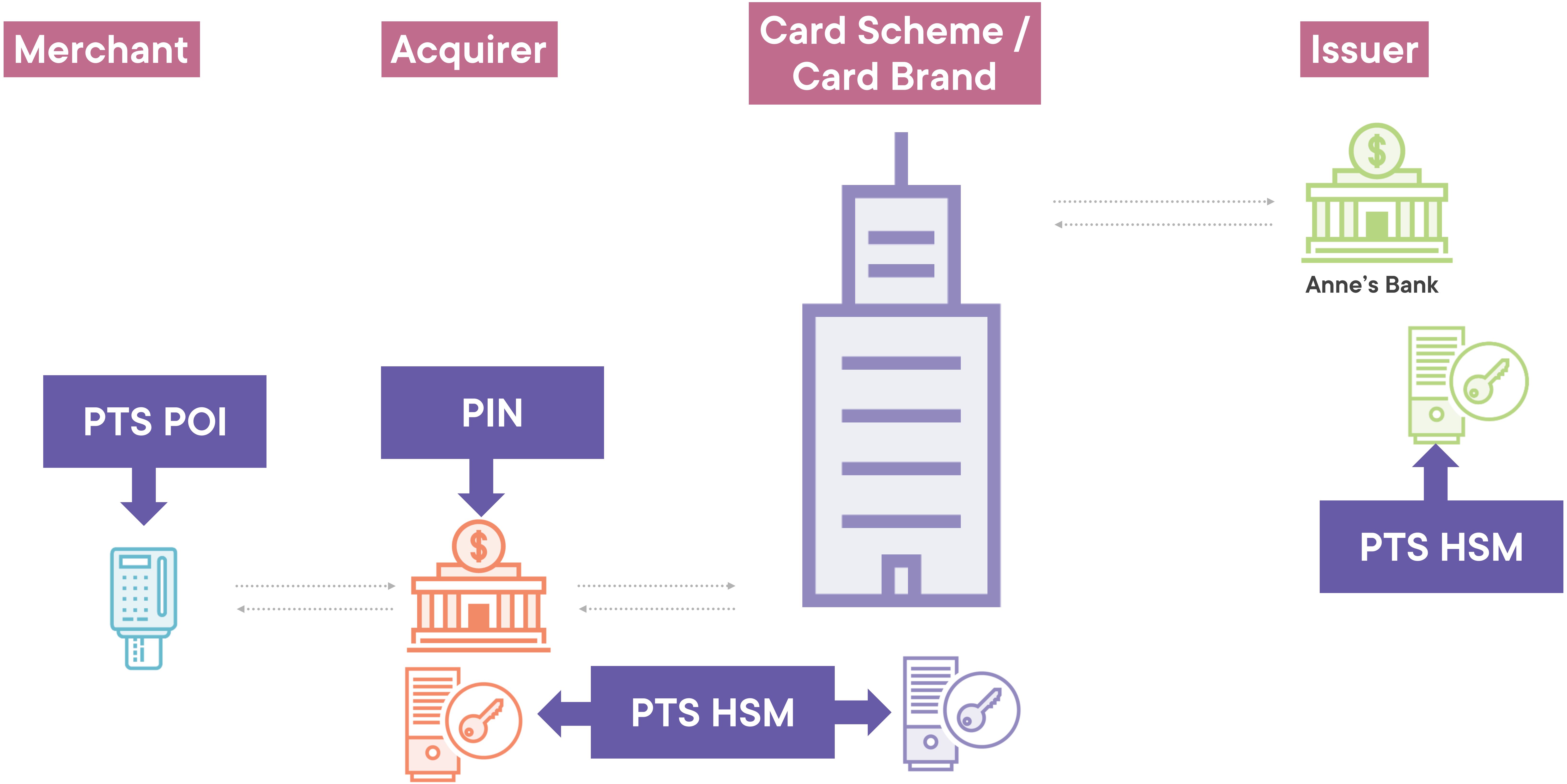
Merchant

Acquirer

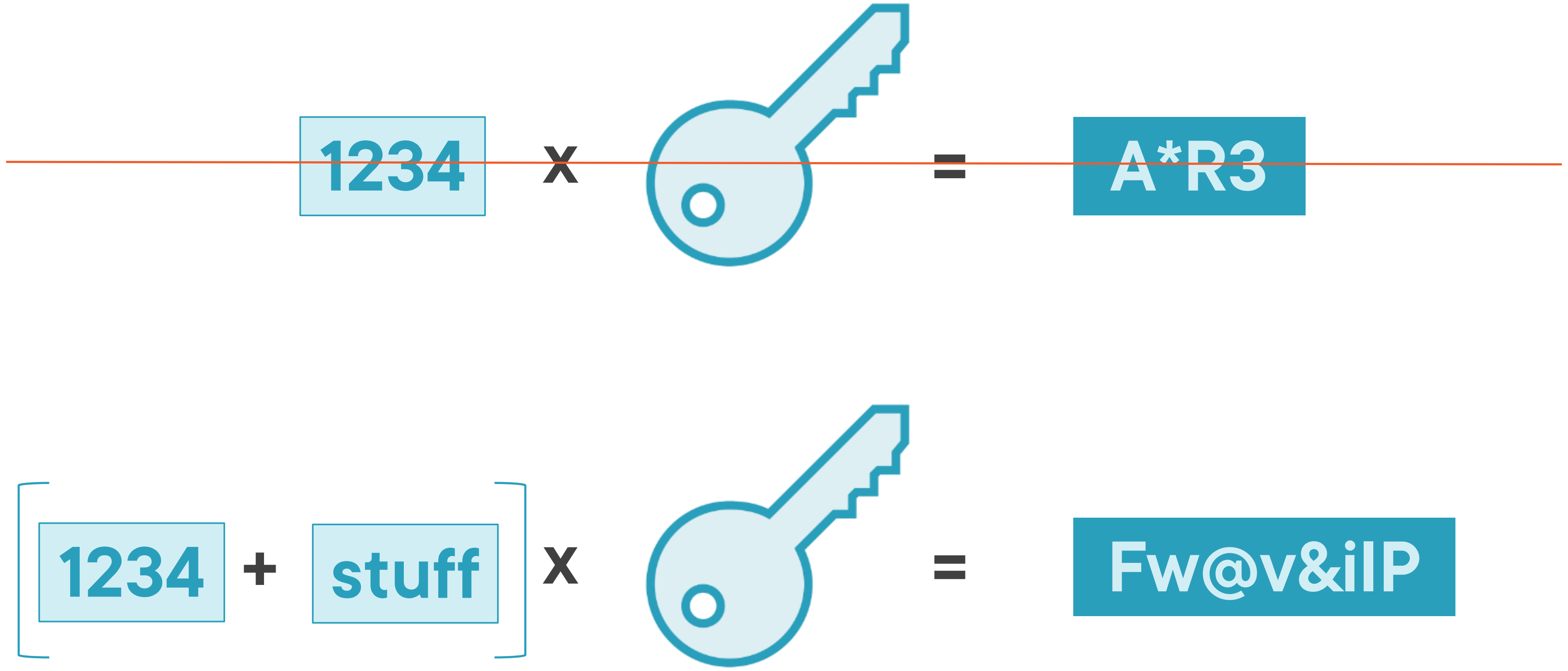
Card Scheme / Card Brand

Issuer

PIN Security in Practice



Simplification



~~1234 x = A*R3~~

[1234 + stuff] x = Fw@v&ilP

This is a PIN Block

Payment Solutions
Point-to-point Encryption, SPoC and CPoC

PCI Point-to-Point Encryption Standard (P2PE)

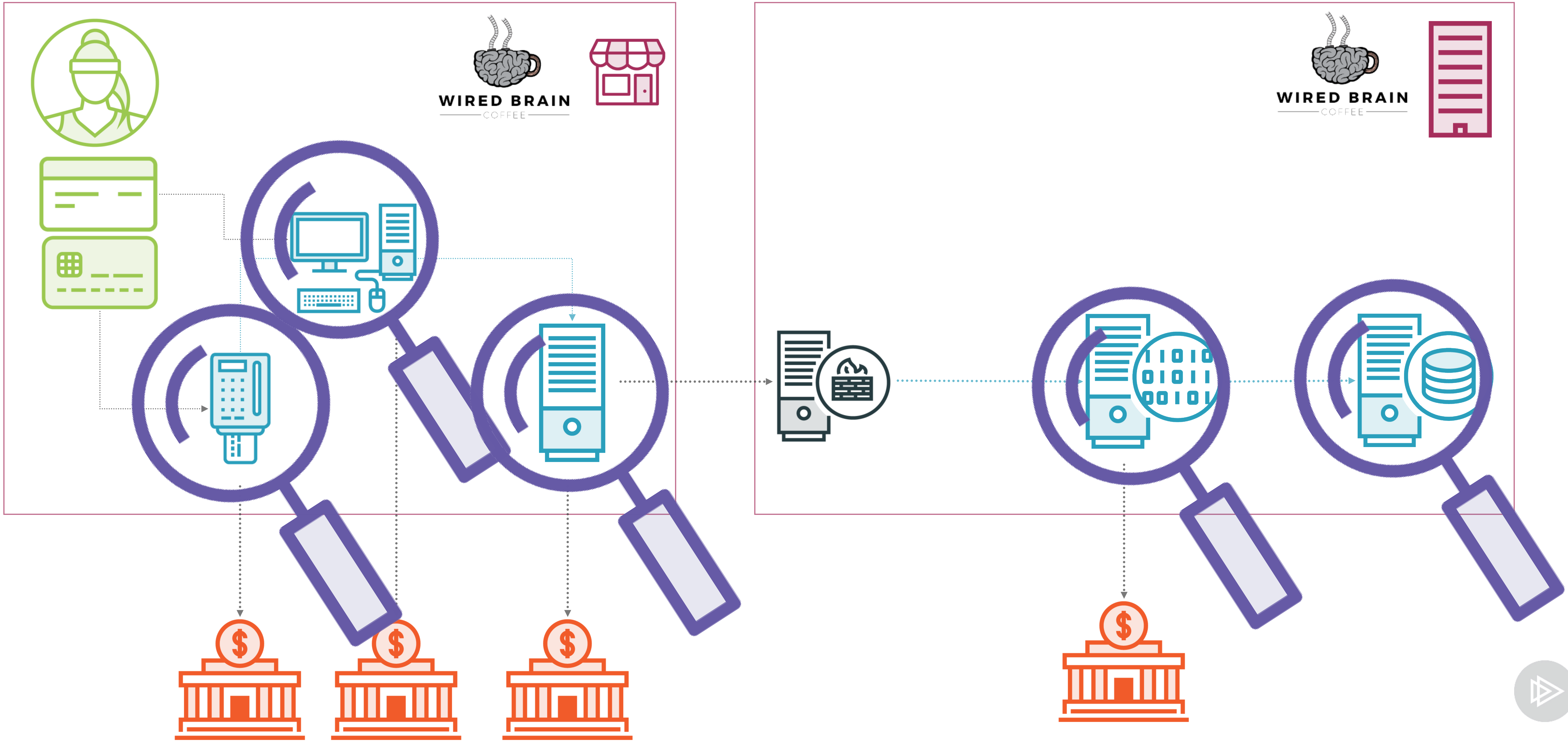
How to encrypt Primary Account Numbers in POI devices and decrypt it in a service provider (or acquirer)

Key management (like PTS)

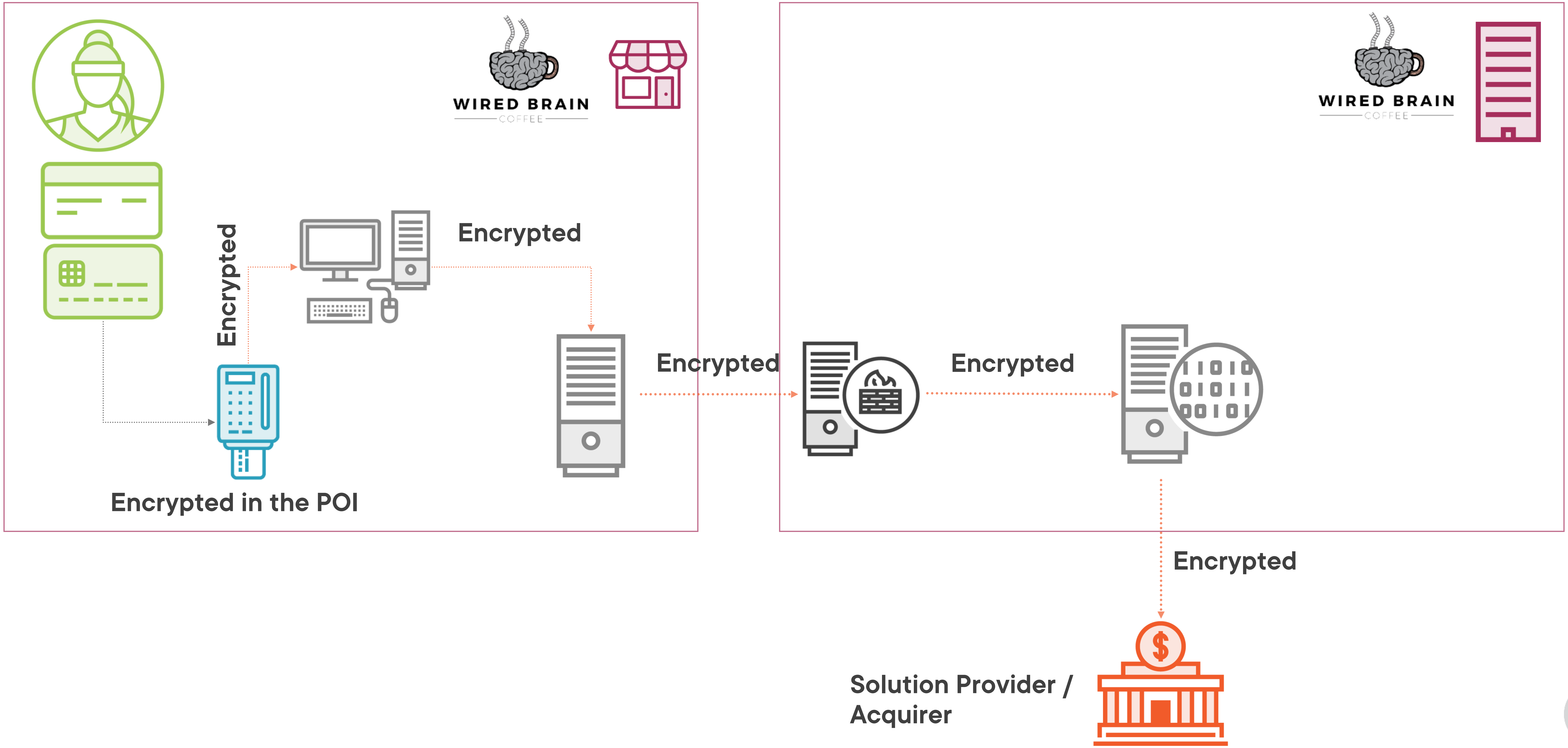
Security of decryption environment

How to look after the POI devices

Where to Find Authorization Data (Face-to-face)

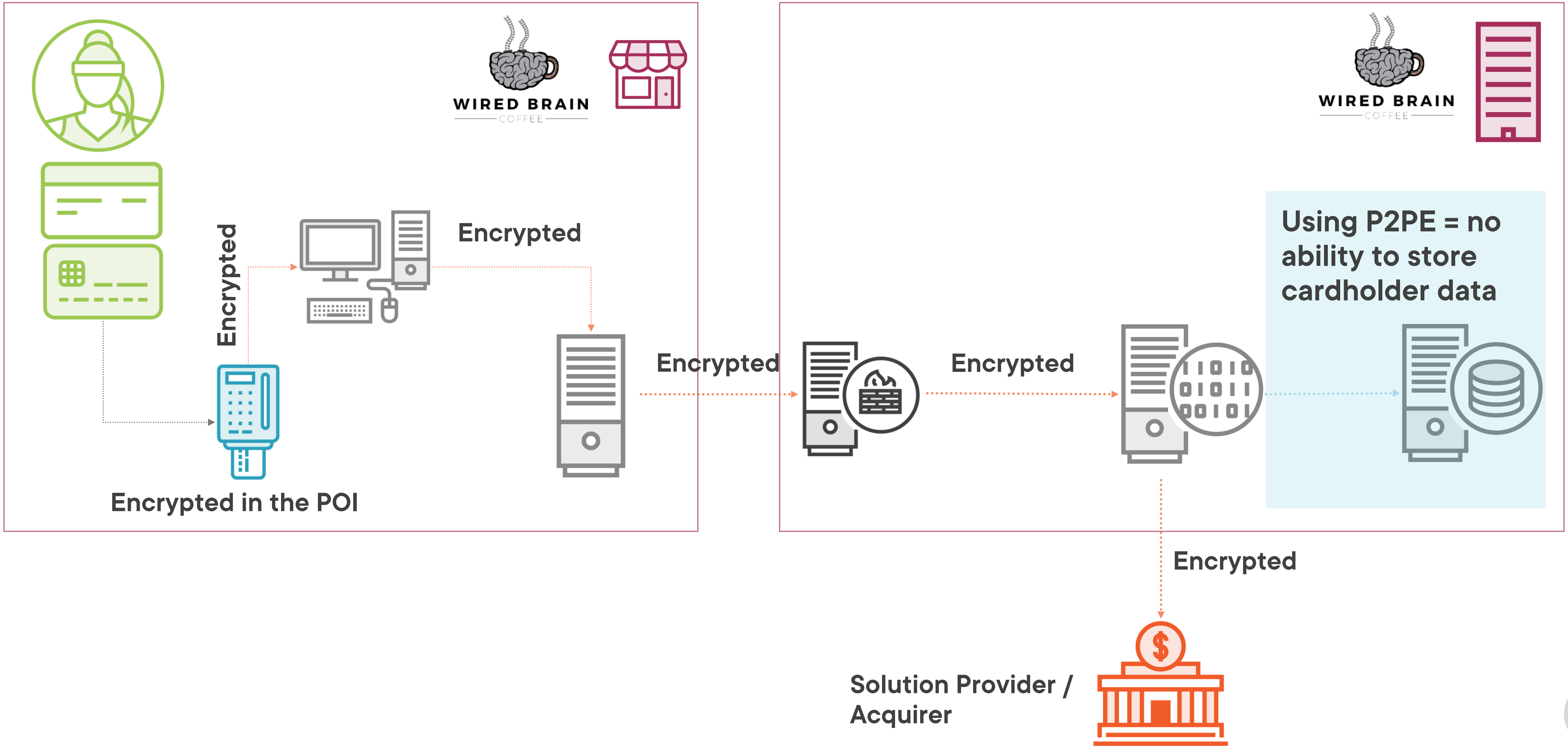


P2PE



WIRED BRAIN
COFFEE
Encrypted
Encrypted
Encrypted in the POI
Encrypted
WIRED BRAIN
COFFEE
Encrypted
Encrypted
Solution Provider /
Acquirer

P2PE



Encrypted

Encrypted

Encrypted in the POI

Encrypted

Encrypted

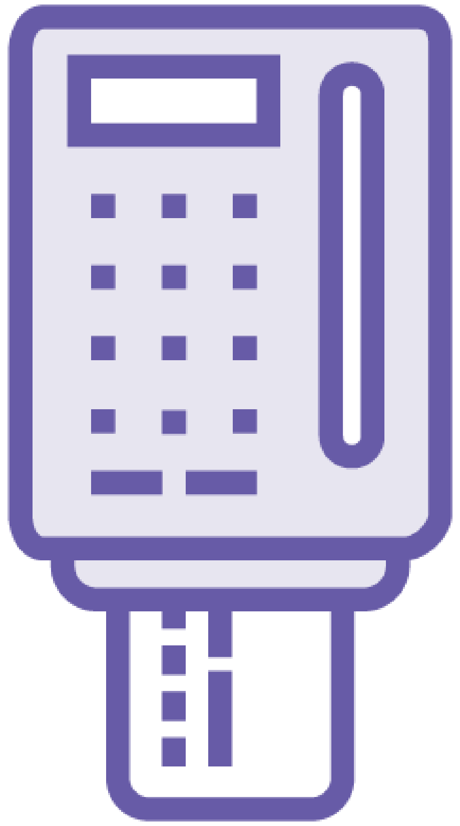
Using P2PE = no ability to store cardholder data

Encrypted

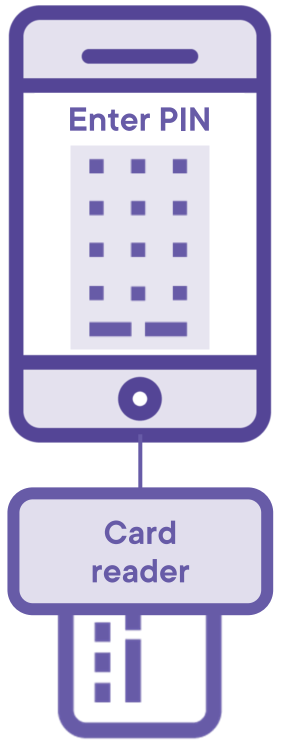
Solution Provider / Acquirer

Card Acceptance

P2PE



SPoC



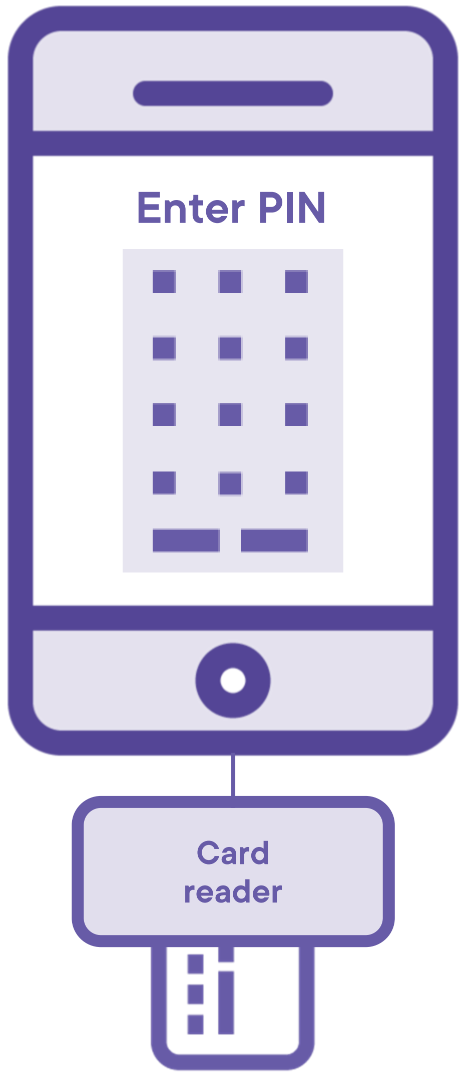
Software based PIN Entry on Commercial-off-the-shelf Devices (COTS)

CPoC

Tap to complete $10 transaction

Contactless Payments on Commercial-off-the-shelf Devices (COTS)

Software Based PIN Entry on COTS (SPoC)



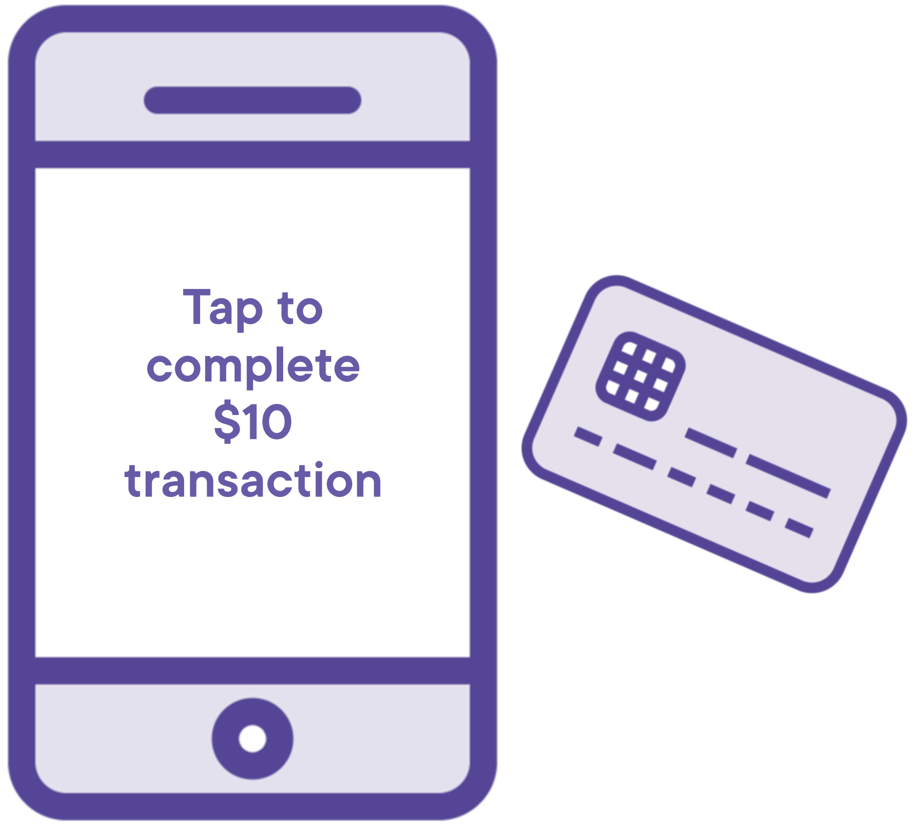
Smartphone/device +

Encrypting card reader (PTS POI validated)

Software on the smartphone
- **PIN entry**
- **Communications**

Solution provider
- **Security of their environment**
- **Security of the device**

Contactless Payments on COTS (CPoC)



Smartphone/device +

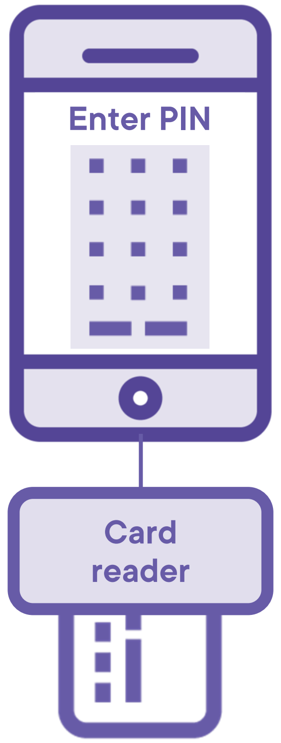
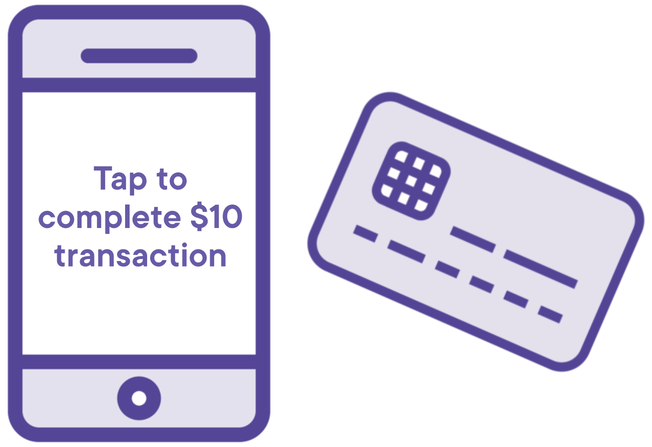
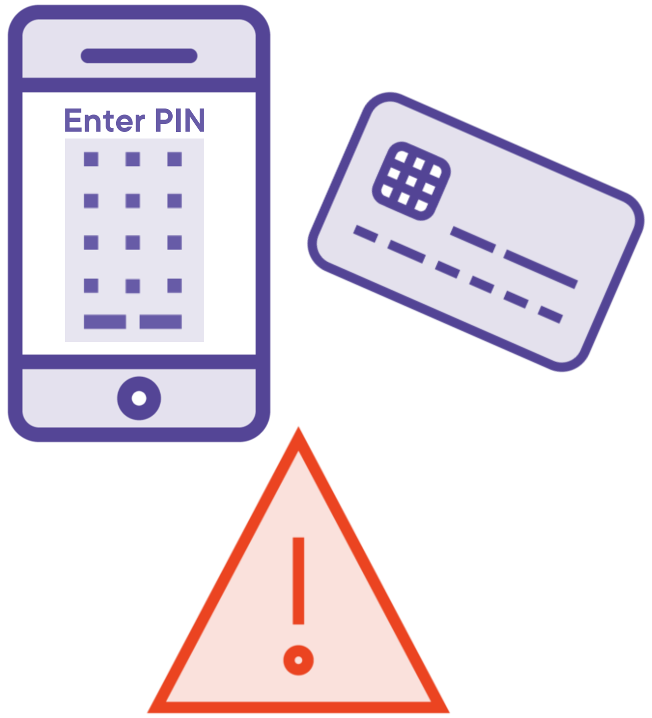
Software on the smartphone

Solution provider

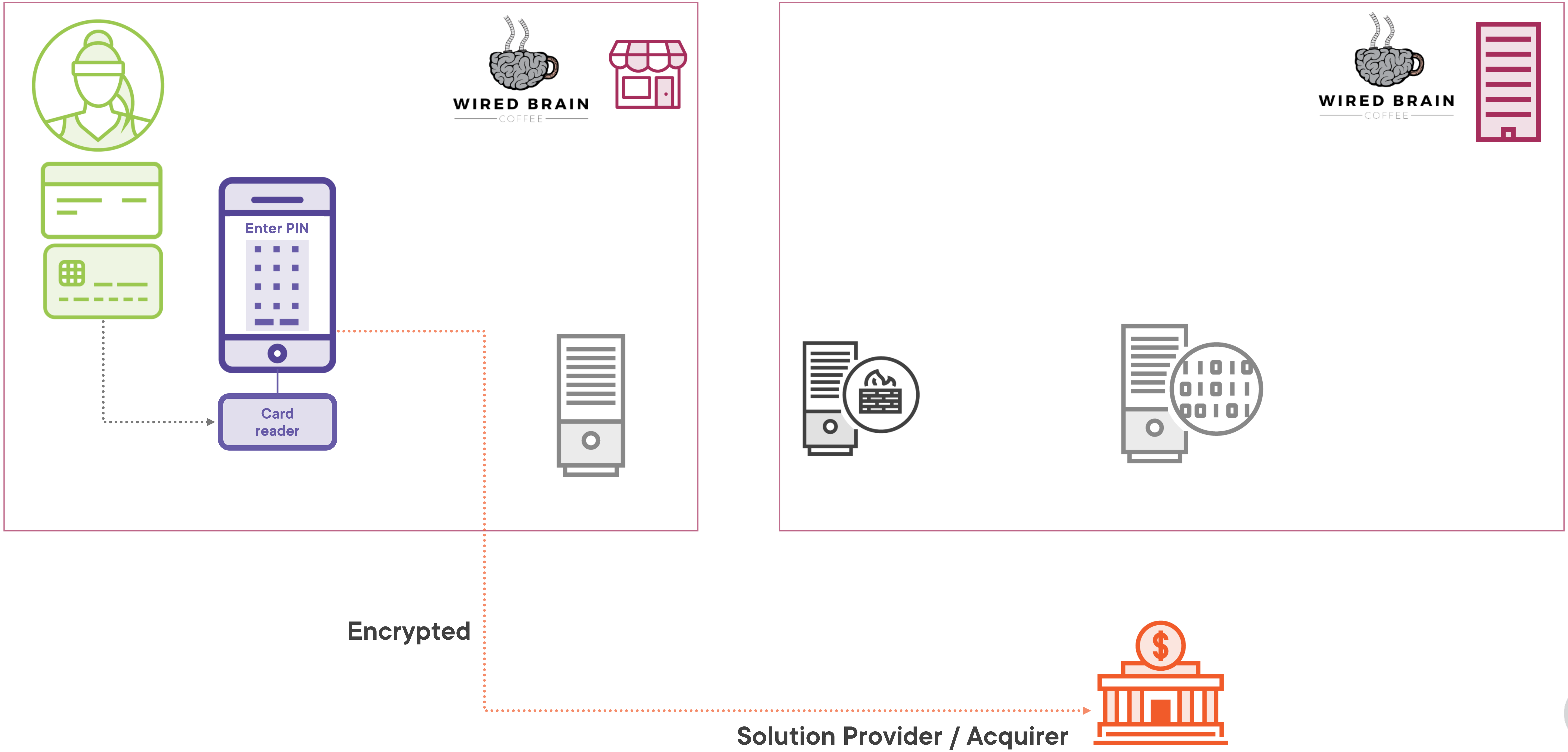
- **Security of their environment**
- **Security of the device**

Sidebar:
Device security and payment card data

Sidebar

	SPoC	**CPoC**	**????**
Data on the device			
Account data	**Encrypted**	**Unencrypted**	**Unencrypted**
PIN	**Unencrypted**	-	**Unencrypted**

SPoC and CPoC



Encrypted

Solution Provider / Acquirer

Standards for Financial Institutions

3DS Standards

3DS Core

Acquirer

3DS Server

Card Scheme / Card Brand

Directory Server

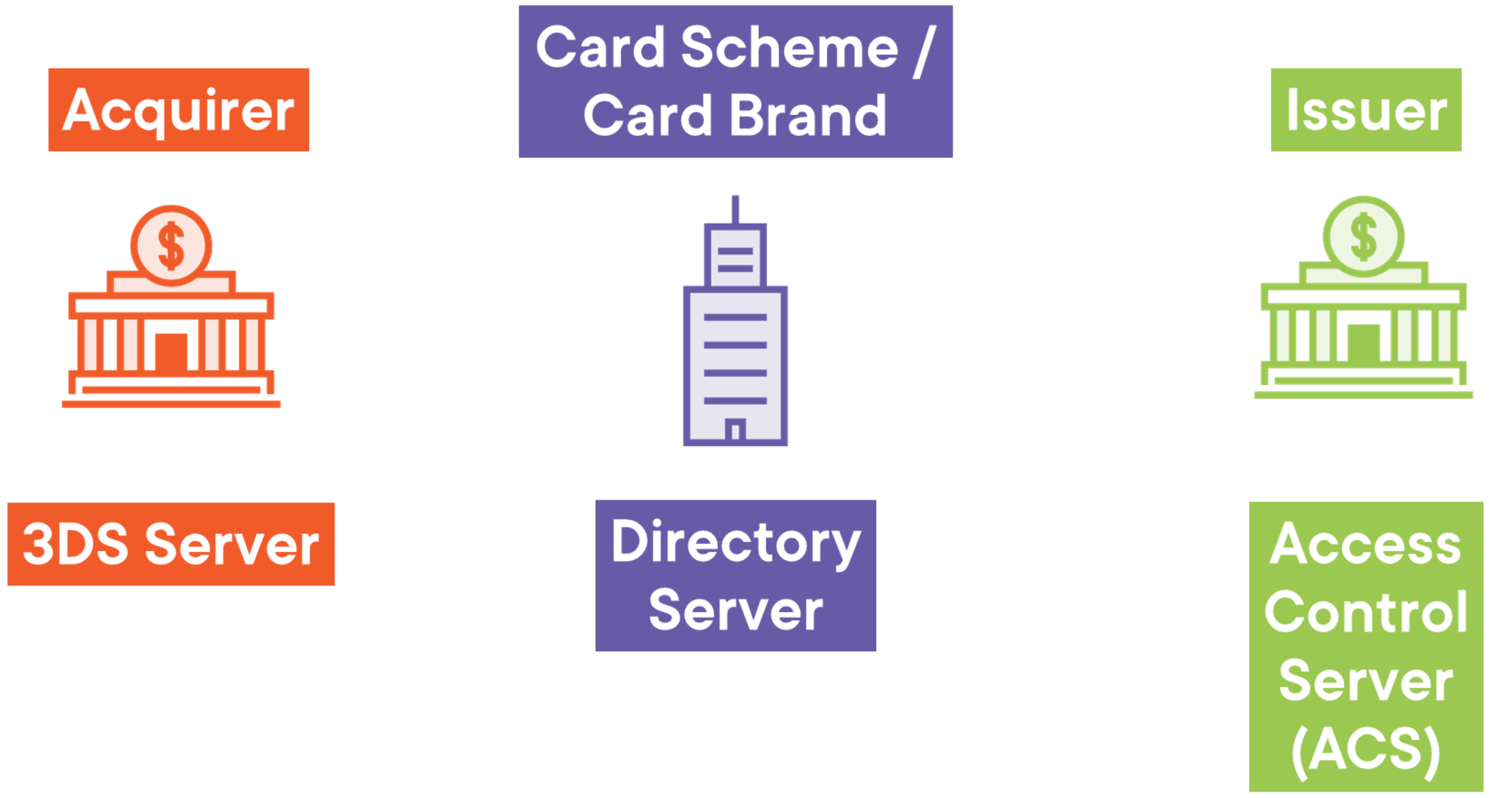
Issuer

Access Control Server (ACS)

3DS Standards

3DS Core

- Baseline requirements – very much like PCI DSS
- 3DS security requirements



Acquirer

3DS Server

Card Scheme / Card Brand

Directory Server

Issuer

Access Control Server (ACS)

3DS Standards

3DS Software Development Kit

- SDK for app builders to use to incorporate 3DS payment flows

Requirements relate to

- The SDK itself
- Vulnerability reporting and management

Token Service Provider

Has PCI DSS as a baseline

Adds more stringent controls:

- Remote access
- Logical access
- Physical access
- Cryptographic key management

PCI Card Production Standard

Physical and logical standards

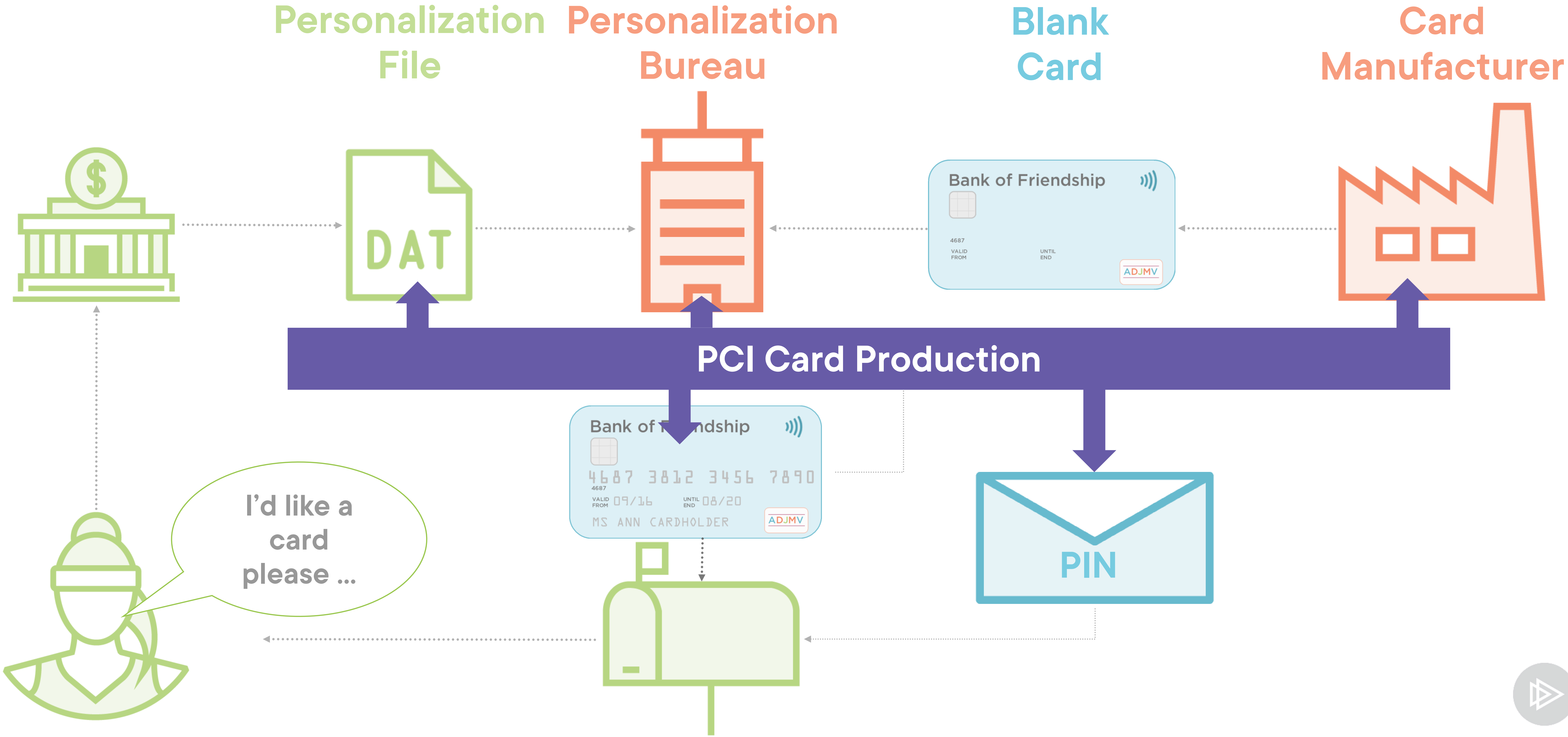
How to manufacture, personalize and distribute payment cards

How to send PINs to consumers

Two standards

- Physical security
- Logical security

Card Production Standards



Personalization File

Personalization Bureau

Blank Card

Card Manufacturer

PCI Card Production

I'd like a card please …

PIN

The PCI Standards Are Freely Available

Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures
Version 3.2
April 2016

Payment Card Industry (PCI)
Payment Application Data Security Standard

Requirements and Security Assessment Procedures
Version 3.2
May 2016

Payment Card Industry (PCI)
PIN Security Requirements

Version 2.0
December 2014

Payment Card Industry (PCI)
PIN Transaction Security (PTS)
Hardware Security Module (HSM)

Payment Card Industry (PCI)
PIN Transaction Security (PTS)
Point of Interaction (POI)

https://www.pcisecuritystandards.org/document_library

Payment Card Industry (PCI)
Point-to-Point Encryption

Solution Requirements and Testing Procedures
Version 2.0
June 2015

Payment Card Industry (PCI)
Card Production

Physical Security Requirements
Version 1.1
March 2015

Payment Card Industry (PCI)
Card Production

Logical Security Requirements
Version 1.1
March 2015

Insert Demo of PCI SSC Document Library

What Criminals Want

They steal this:	To:
Cards (±PINs)	Withdraw money from ATMS Buy goods
Magstripe (track) data (±PIN)	Make clone magstripe cards +PIN = ATMs -PIN = buy goods
Ecommerce data (PAN, Exp, ±CVV2)	Buy goods at other Ecommerce merchant that they can turn into cash
Chip Data Mag Stripe Image (MSI) (PAN, Exp)	Buy goods at other Ecommerce merchants that do not ask for CVV2 or use 3DS

Summary

Criminals steal data that they want to turn into money

PCI security standards protect data

- Data security (PCI DSS)
- Secure software standard
- PINs and PIN-processing devices
- Merchant solutions (P2PE, SPoC & CPoC)
- 3DS, TSP and Card Production

EMV standards devalue data so that stolen data is worthless

- Chip transactions
- 3 Domain Security
- Tokenization