# Andrew Jamieson

VP, Distinguished Standards Architect

PCI Security Standards Council






# Piecing Together The Future of Payment Security


20
YEARS OF SECURING
PAYMENT DATA
PCI
Security
Standards Council




Why?



## PCI Data Security Standard (PCI DSS)

The PCI DSS defines security requirements to protect environments where payment account data is stored, processed, or transmitted. PCI DSS provides a baseline of technical and operational requirements designed to protect payment account data.



## Point-to-Point Encryption (P2PE)

The PCI P2PE Standard defines security requirements for P2PE Solutions, P2PE Components, and P2PE Applications to protect payment account data via encryption from the point it is captured in the merchant's payment device to the point it is decrypted in a solution provider's or component provider's environment.



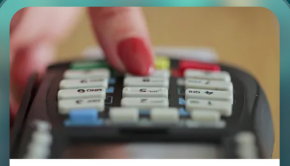
## Secure Software

The PCI Secure Software Standard defines security requirements for software vendors and developers to ensure that payment software is securely designed and managed, and the integrity of payment transactions and the confidentiality of payment data that is stored, processed, or transmitted in association with payment transactions is protected.



## Secure Software Lifecycle (Secure SLC)

The Secure Software Lifecycle (SLC) Standard defines security requirements for software vendors and developers to ensure security is integrated throughout the entire software lifecycle and that software is secure by design and able to withstand attack.



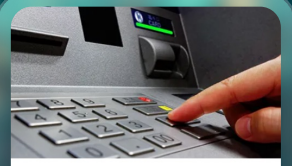
## PTS Point of Interaction (POI)

The PIN Transaction Security (PTS) Point of Interaction (POI) Standard defines security requirements for the characteristics and management of devices used to protect cardholder PINs (personal identification numbers), account data, and other sensitive payment card data at the point of interaction.



## Token Service Provider (TSP)

The Token Service Provider (TSP) Standard defines security requirements for Token Service Providers (TSPs) that generate and issue EMV payment tokens, as defined under the EMV® Payment Tokenisation Specification Technical Framework.



## PIN Security

The PIN Security Standard defines security requirements for the secure management, processing, and transmission of personal identification number (PIN) data during online and offline payment card transaction processing at ATMs and attended and unattended point-of-sale (POS) terminals.



## Card Production and Provisioning - Logical

This Standard defines the logical security requirements for the development, manufacture, transport, and personalization of payment cards and their components.

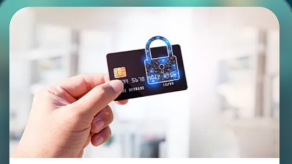
The Card Production and Provisioning Logical Security Requirements are complementary to the Card Production and Provisioning Physical Security Requirements.



## Card Production and Provisioning - Physical

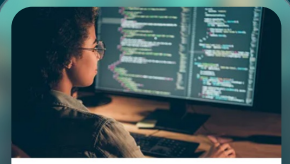
This standard defines the physical security requirements for card production and provisioning functions.

The Card Production and Provisioning Physical Security Requirements are complementary to the Card Production and Provisioning Logical Security Requirements.



## PCI 3DS Core

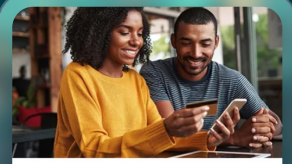
The PCI 3-D Secure (3DS) Core Security Standard defines security requirements to protect environments where specific 3DS functions are performed, to enable secure consumer authentication for e-commerce and m-commerce purchases.



## PCI 3DS SDK

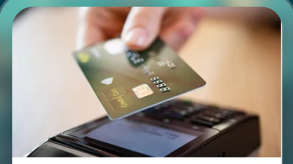
This standard offers security requirements, assessment procedures, and guidance for 3DS Software Development Kits (SDK), as defined in the EMV® 3-D Secure SDK Specification, to help prevent unauthorized card-not-present (CNP) transactions and to protect merchants from CNP exposure to fraud.

**The PCI Security Standards Council (PCI SSC) announced the formal sunset period for the PCI 3-D Secure (3DS) Software Development Kit (SDK) Standard from 1 May – 31 October, 2026. See the bulletin for more information.**



## Mobile Payments on COTS (MPoC)

PCI Mobile Payments on COTS (MPoC) builds on the existing PCI Software-based PIN Entry on COTS (SPoC) and PCI Contactless Payments on COTS (CPoC) Standards which individually address the security requirements for solutions that enable merchants to accept cardholder PINs or contactless payments, using a smartphone or other commercial off-the-shelf (COTS) mobile device.



## Contactless Payments on COTS (CPoC)

This standard offers security requirements for solutions that enable a merchant's commercial off-the-shelf (COTS) device (for example, phone or tablet) to accept contactless payments without the need for an external contactless reader by leveraging the native NFC capabilities inherent to a COTS device.

**The PCI Security Standards Council (PCI SSC) announced the formal sunset period for the PCI Contactless Payments on COTS (CPoC) Standard from 1 May – 31 October, 2026. See the bulletin for more information.**



## Software-based PIN Entry on COTS (SPoC)

This standard offers security requirements for secure mobile payment acceptance solutions that enable transactions with PIN entry on a merchant commercial off-the-shelf (COTS) device (e.g., smartphone or tablet).

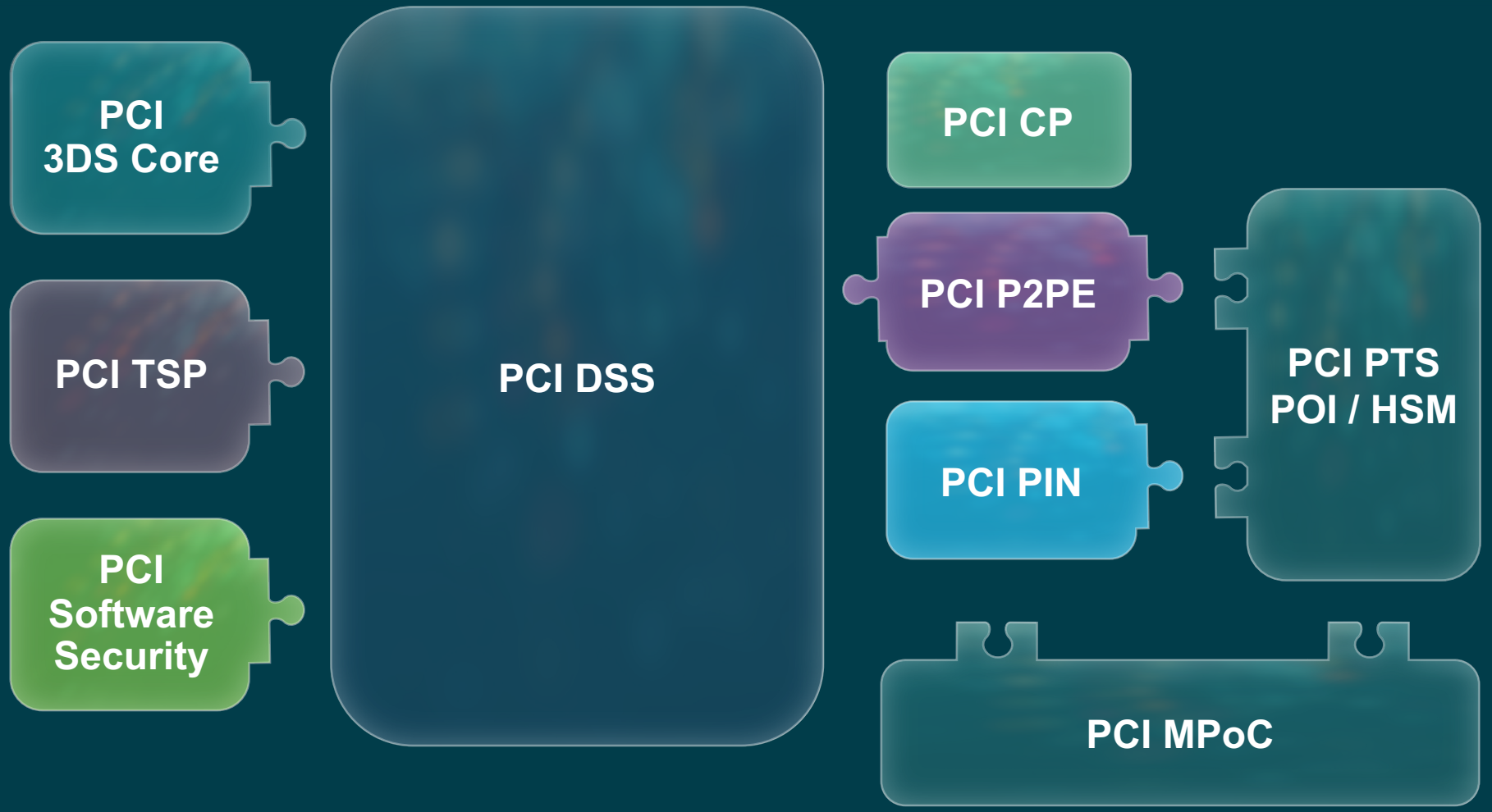
**The PCI Security Standards Council (PCI SSC) announced the formal sunset period for the PCI Software-based PIN Entry on COTS (SPoC) Standard from 1 May – 31 October, 2026. See the bulletin for more information.**



## PTS Hardware Security Module (HSM)

The PIN Transaction Security (PTS) Hardware Security Module (HSM) Standard defines security requirements for characteristics and management of hardware security modules throughout their lifecycle, to ensure confidentiality and data integrity during activities such as financial transactions and payment card personalization.

# The PCI SSC Standards Jigsaw




Why?

## Mission

To enhance global payment account data security by developing standards and supporting services that drive education, awareness, and effective implementation by stakeholders.

## Strategic Pillars



Increase Industry Participation knowledge



Evolve Security Standards and Validation



Secure Emerging Payment Channels



Increase Standards Alignment and Consistency

## Architecture Principles

Security | Flexibility | Consistency | Global | Reliance

## Mission

**To enhance global payment account data security** by developing standards and supporting services that drive education, awareness, and effective implementation by stakeholders.

## Strategic Pillars



Increase Industry Participation knowledge



Evolve Security Standards and Validation



Secure Emerging Payment Channels



Increase Standards Alignment and Consistency

## Architecture Principles

Security | Flexibility | Consistency | Global | Reliance

# The Goal is the Why

Secure
Account Data

# A goal without a plan is just a wish

– Antoine de Saint-Exupery

# Supporting the Goal is the Plan

Secure
Account Data

# Supporting the Goal is the Plan



# Supporting the Goal is the Plan



# Supporting the Goal is the Plan



# The beginning is the most important part of any work

– Plato

# The Elements of Payments

# The Elements of Payments

Thing to store account data



# The Elements of Payments

Thing to accept account data




Thing to store account data



# The Elements of Payments

Thing to secure transmission of account data



Thing to accept account data




Thing to store account data



# The Elements of Payments

Thing to secure processing / storage of account data



Thing to secure transmission of account data



Thing to accept account data




Thing to store account data



# The Elements of Payments

Secure cryptography

Thing to secure processing / storage of account data



Thing to secure transmission of account data



Thing to accept account data




Thing to store account data





# The Elements of Payments

Secure software & hardware

Secure cryptography

Thing to secure processing / storage of account data



Thing to secure transmission of account data



Thing to accept account data



Thing to store account data



# The Elements of Payments

Secure software & hardware

Secure cryptography

Thing to secure processing / storage of account data

Thing to secure transmission of account data

Thing to accept account data

Thing to store account data









Payment Key Management

Payment Environment
(physical and logical)

Payment Solution
(end to end security)

Payment Acceptance Product (MPoC App, POI)

Payment Instrument
(card or token)

Payment Software
(product and process)

Payment hardware
(devices)

# The Elements of Payments

Secure software & hardware

Secure cryptography

Thing to secure processing / storage of account data

Thing to secure transmission of account data

Thing to accept account data

Thing to store account data

Payment Key Management

Payment Environment (physical and logical)

Payment Solution (end to end security)

Payment Acceptance Product (MPoC App, POI)

Payment Instrument (card or token)

Payment Software (product and process)

Payment hardware (devices)

**Target Areas**

- Key Management Operations
- Environmental Security
- Payment Solution Security
- Payment Acceptance Product
- Payment Card/Instrument
- Software and Dev Process Security
- Physical Device Security

# Mission defines strategy, and strategy defines structure

– Peter Drucker

# Building Out the Structure



# Building Out the Structure



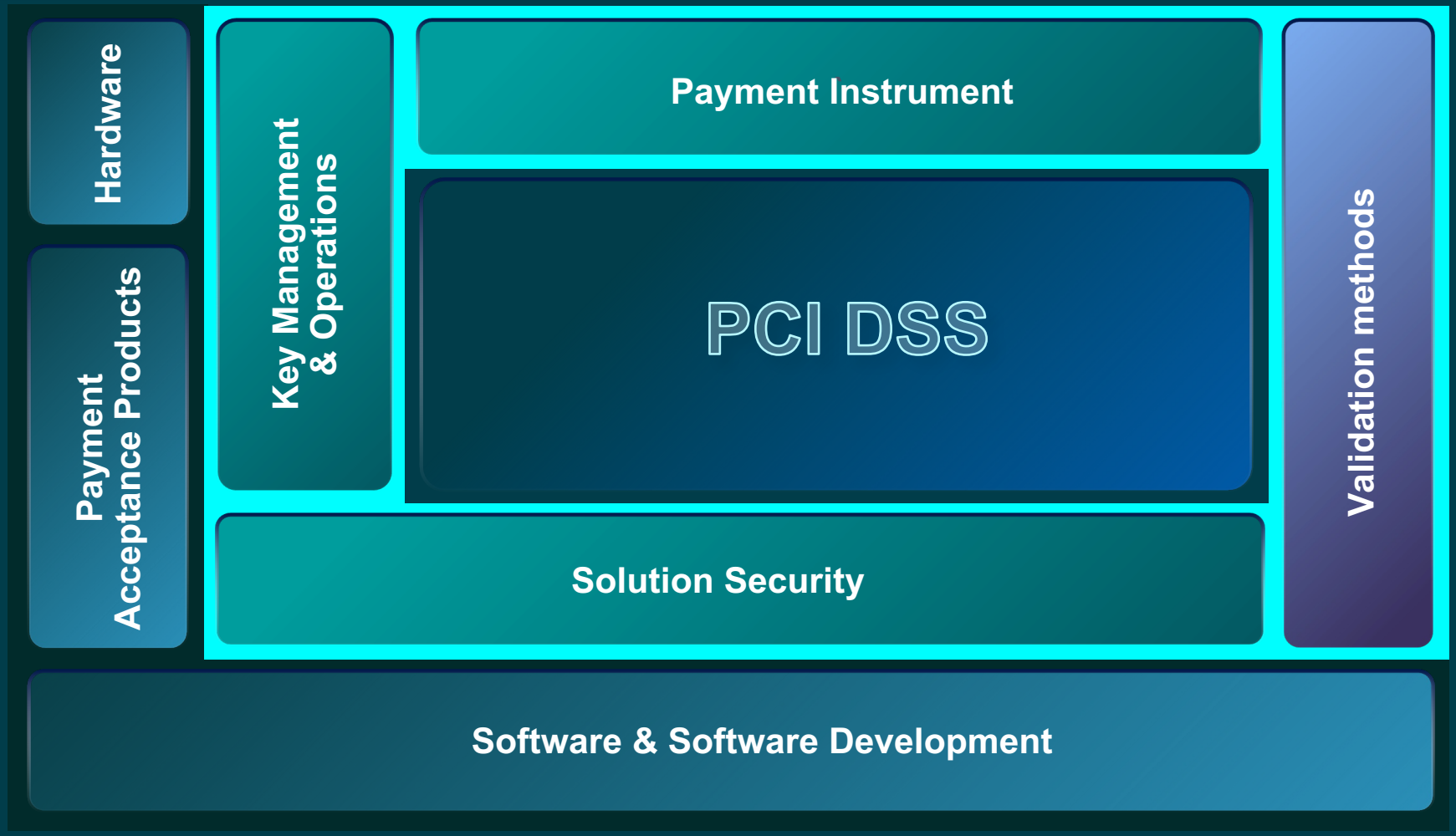
# Building Out the Structure



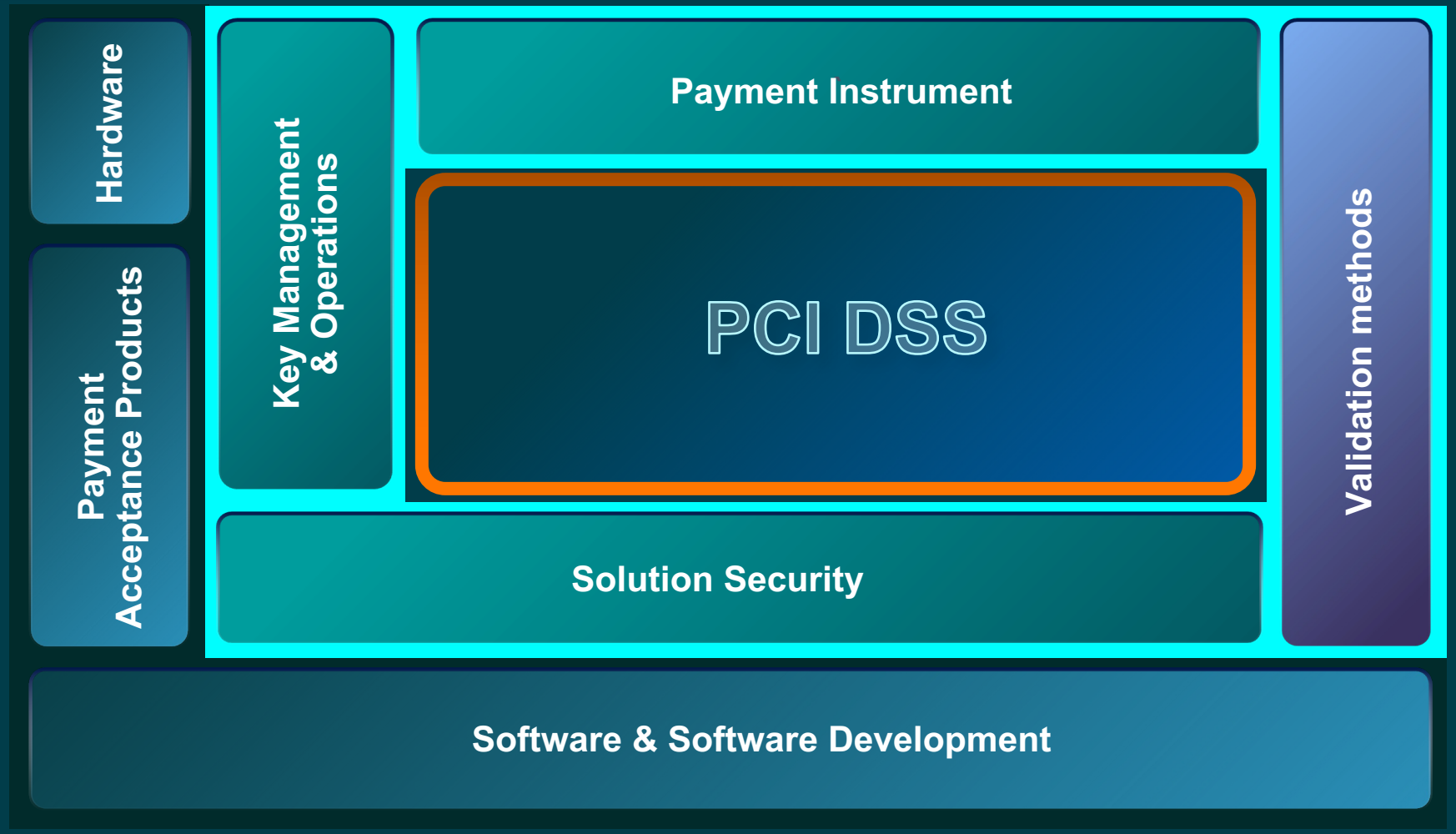
# Building Out the Structure



# Building Out the Structure



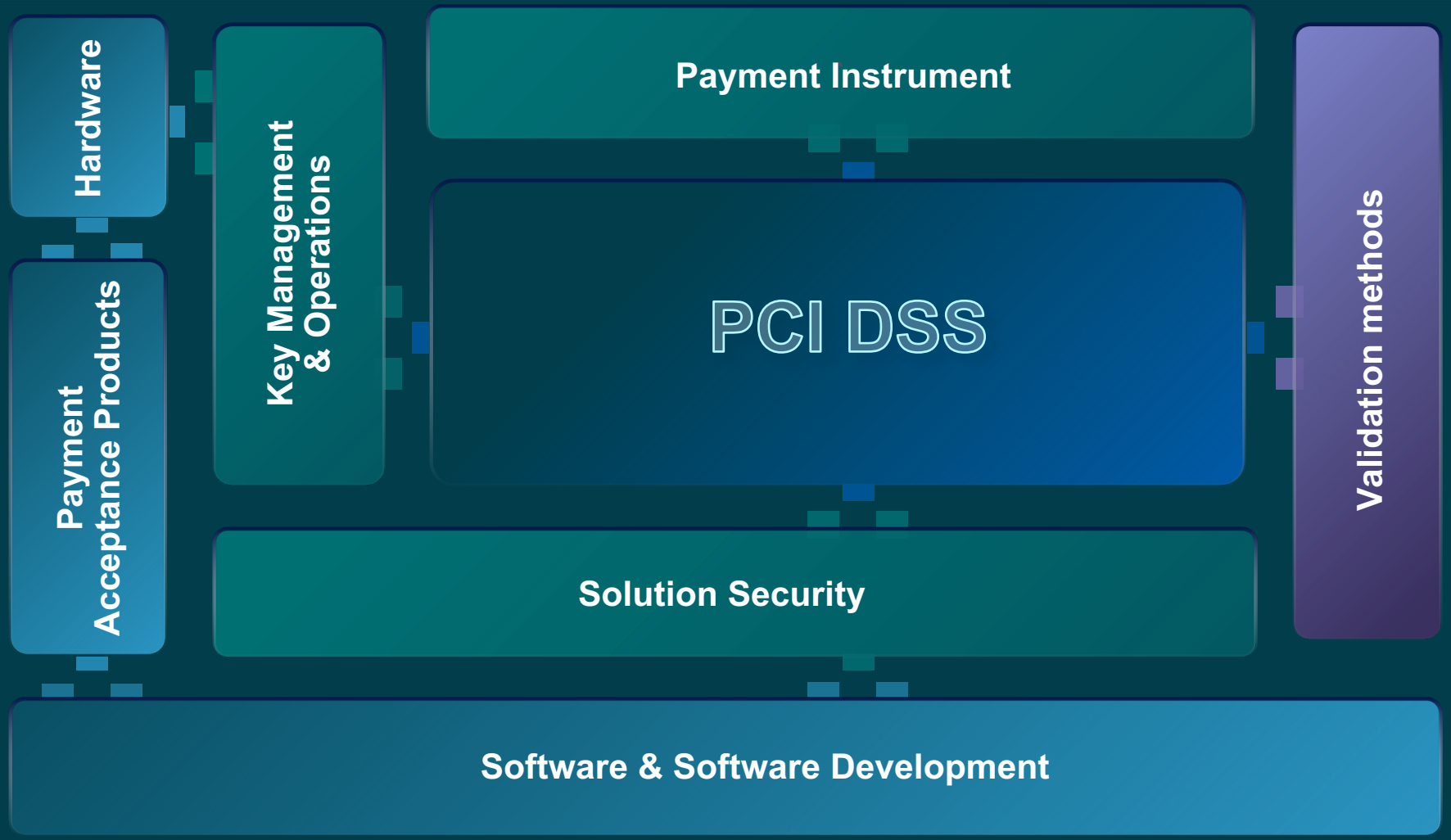
# Building Out the Structure



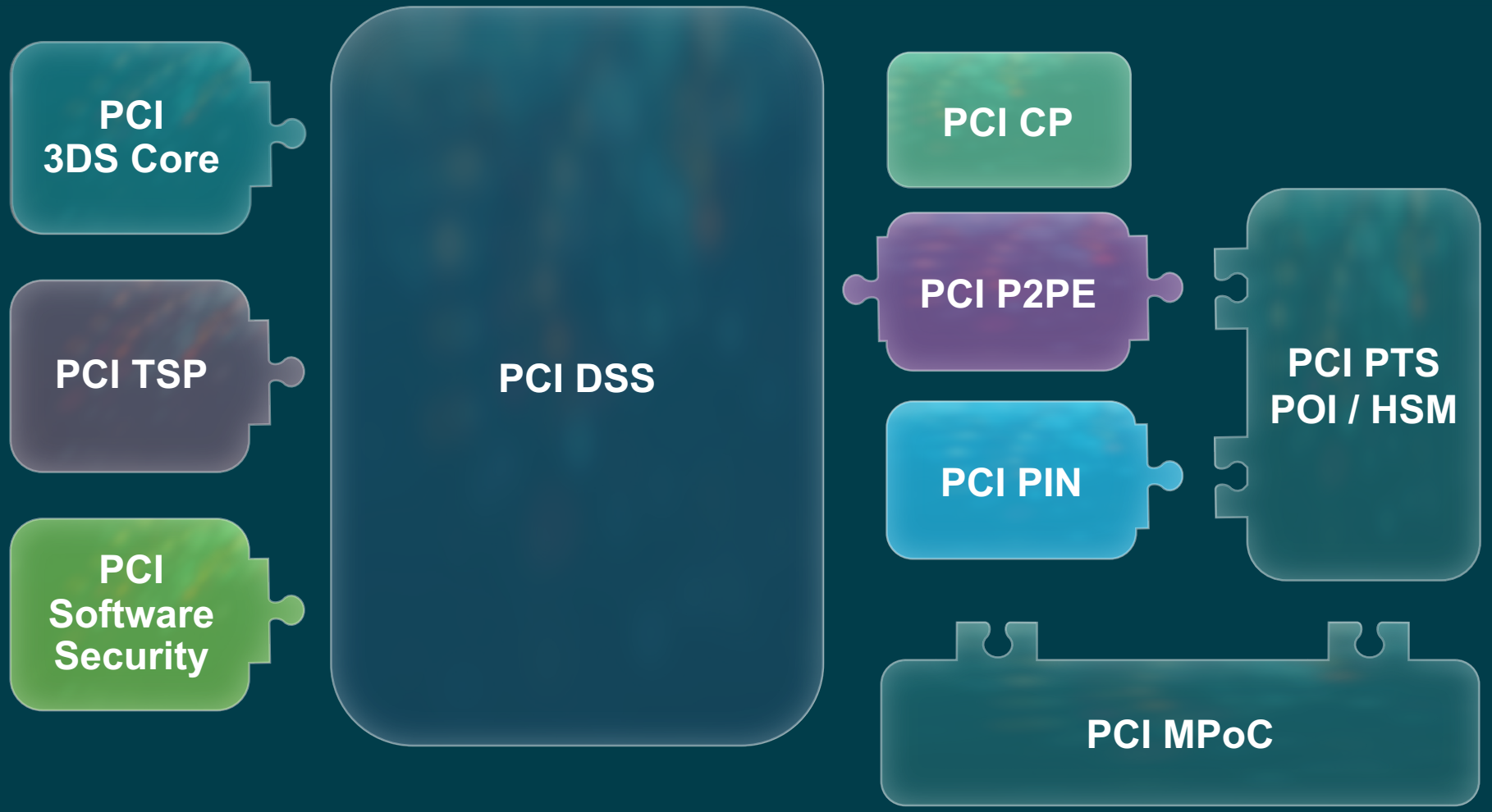
# Building Out the Structure



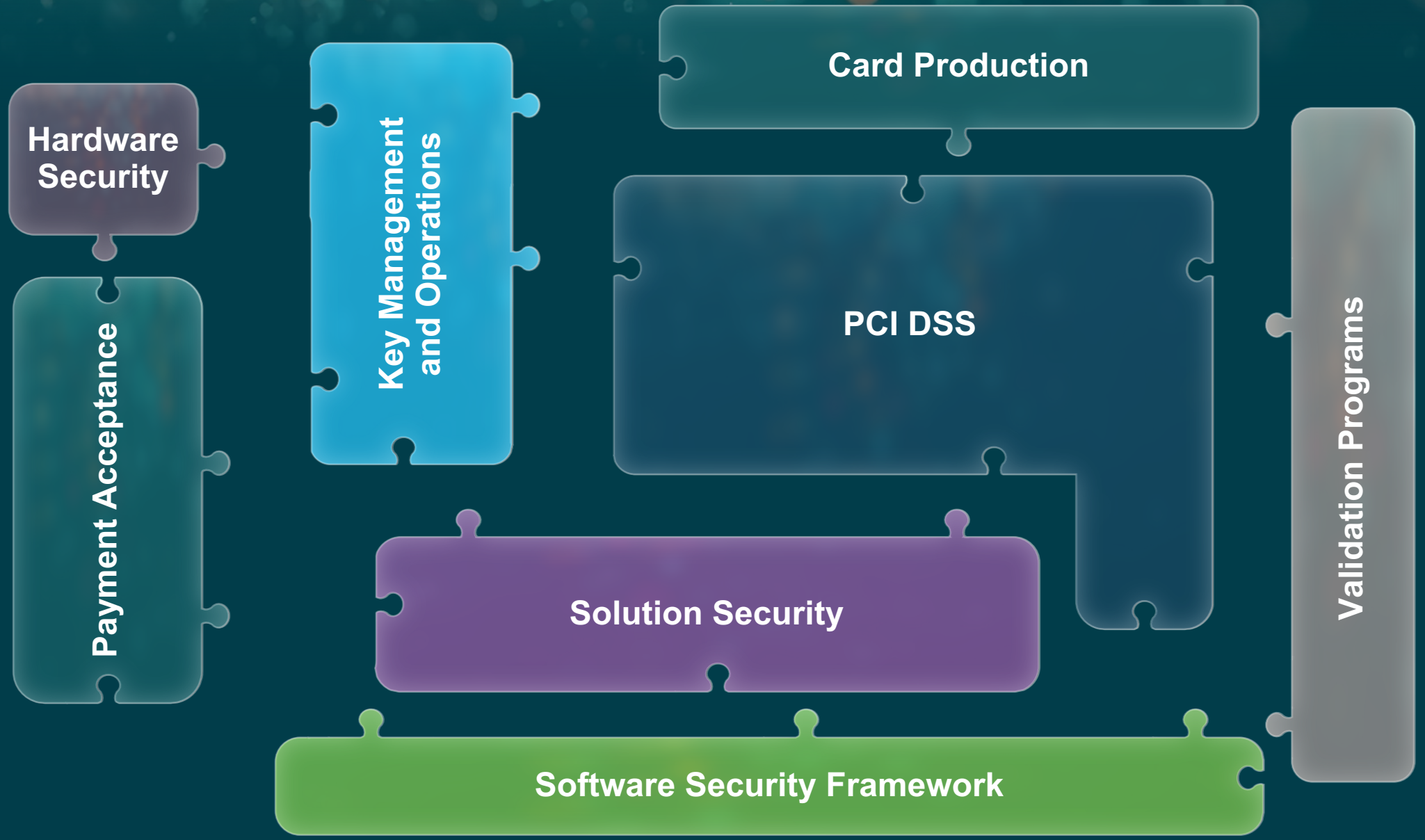
# Solving the PCI SSC Jigsaw



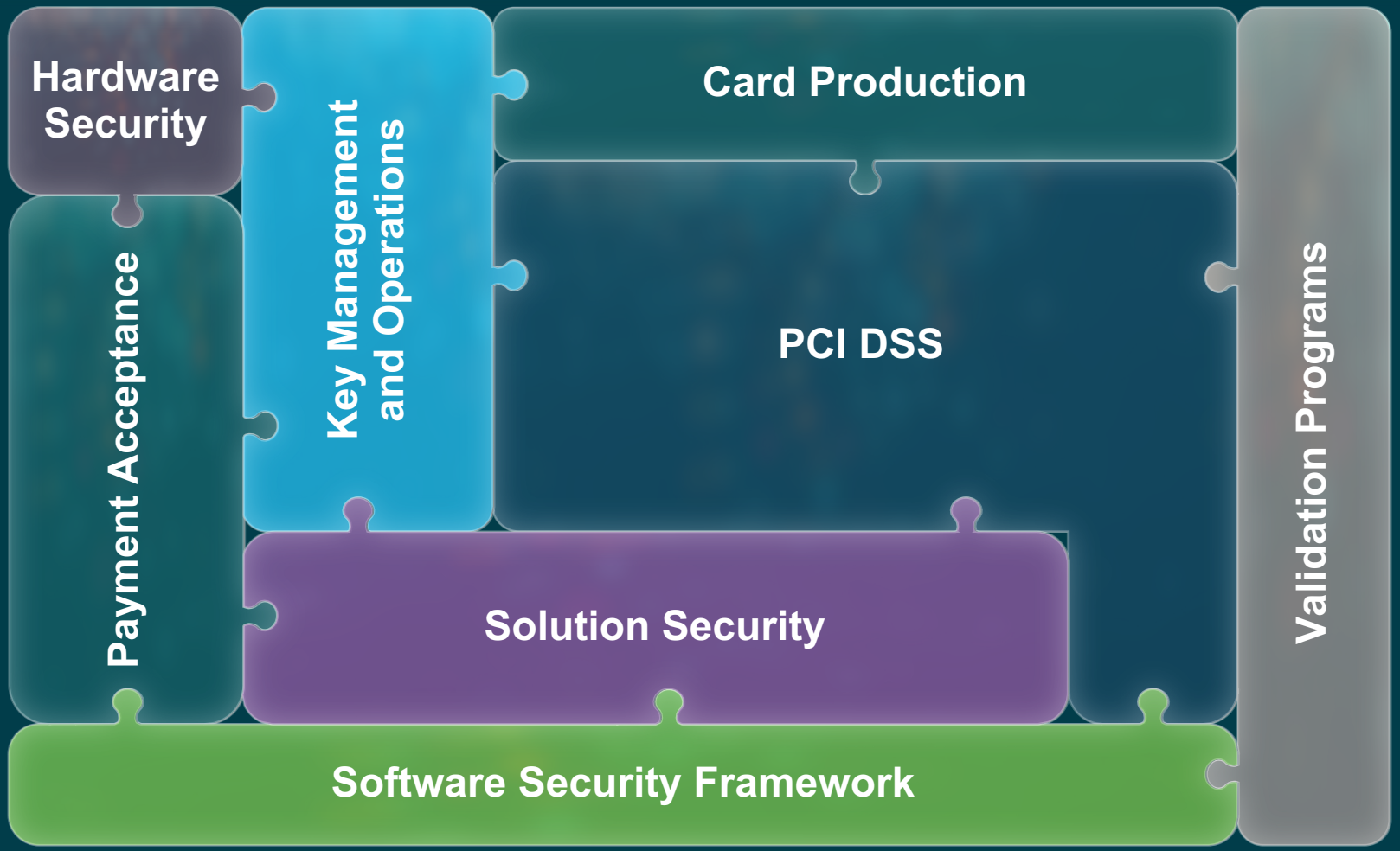
# The PCI SSC Standards Jigsaw



# Solving the PCI SSC Jigsaw

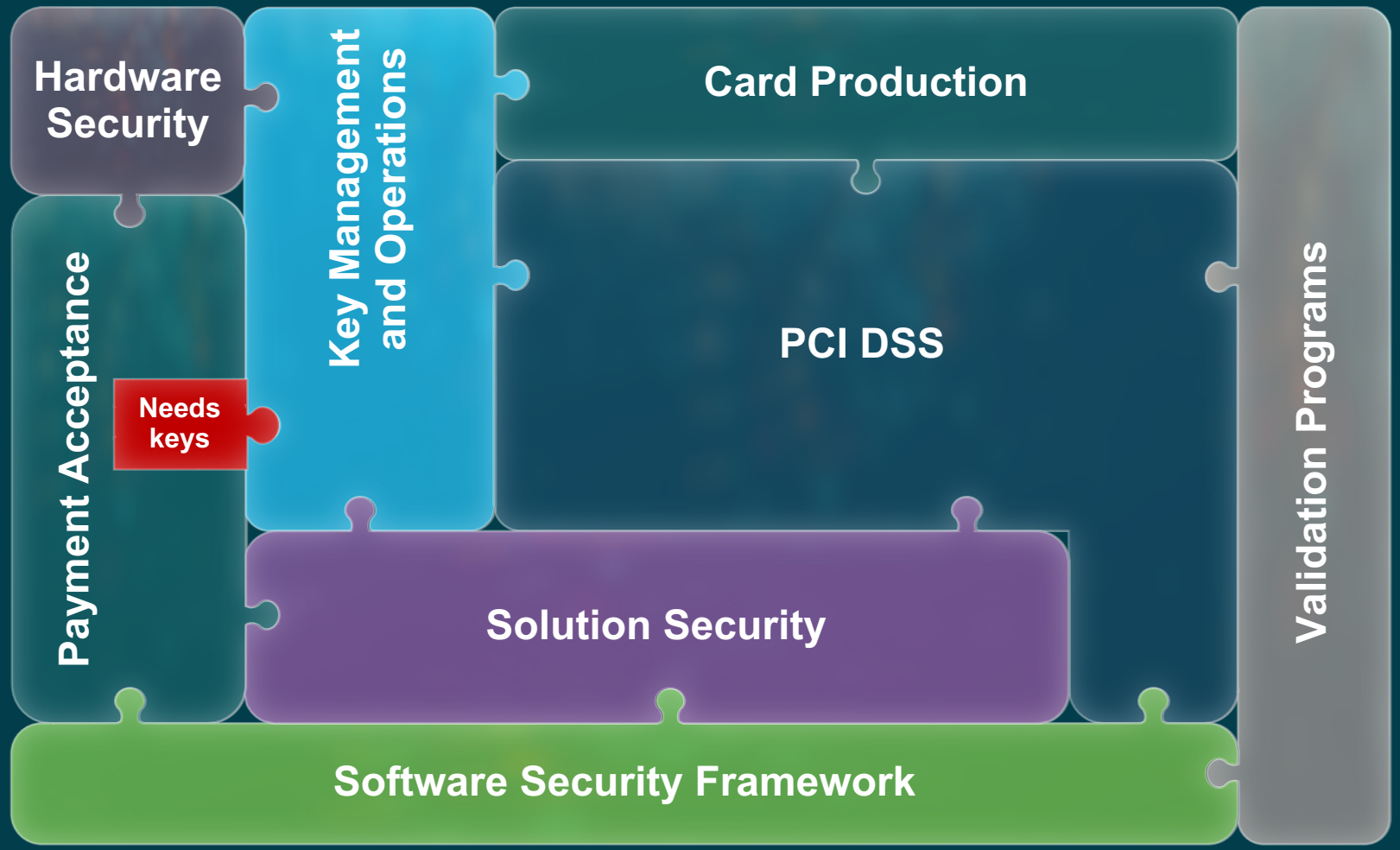


# Solving the PCI SSC Jigsaw

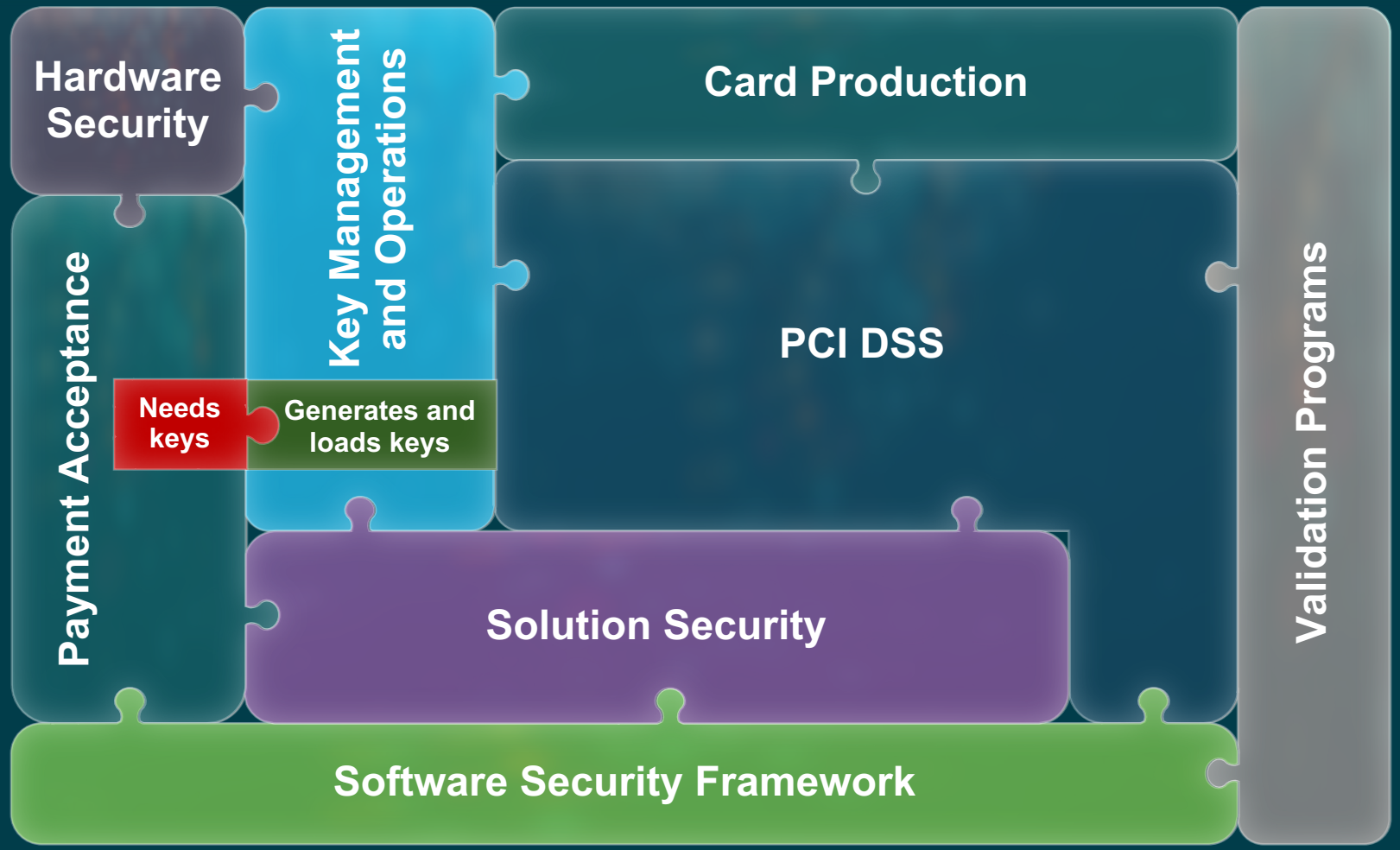



Why?

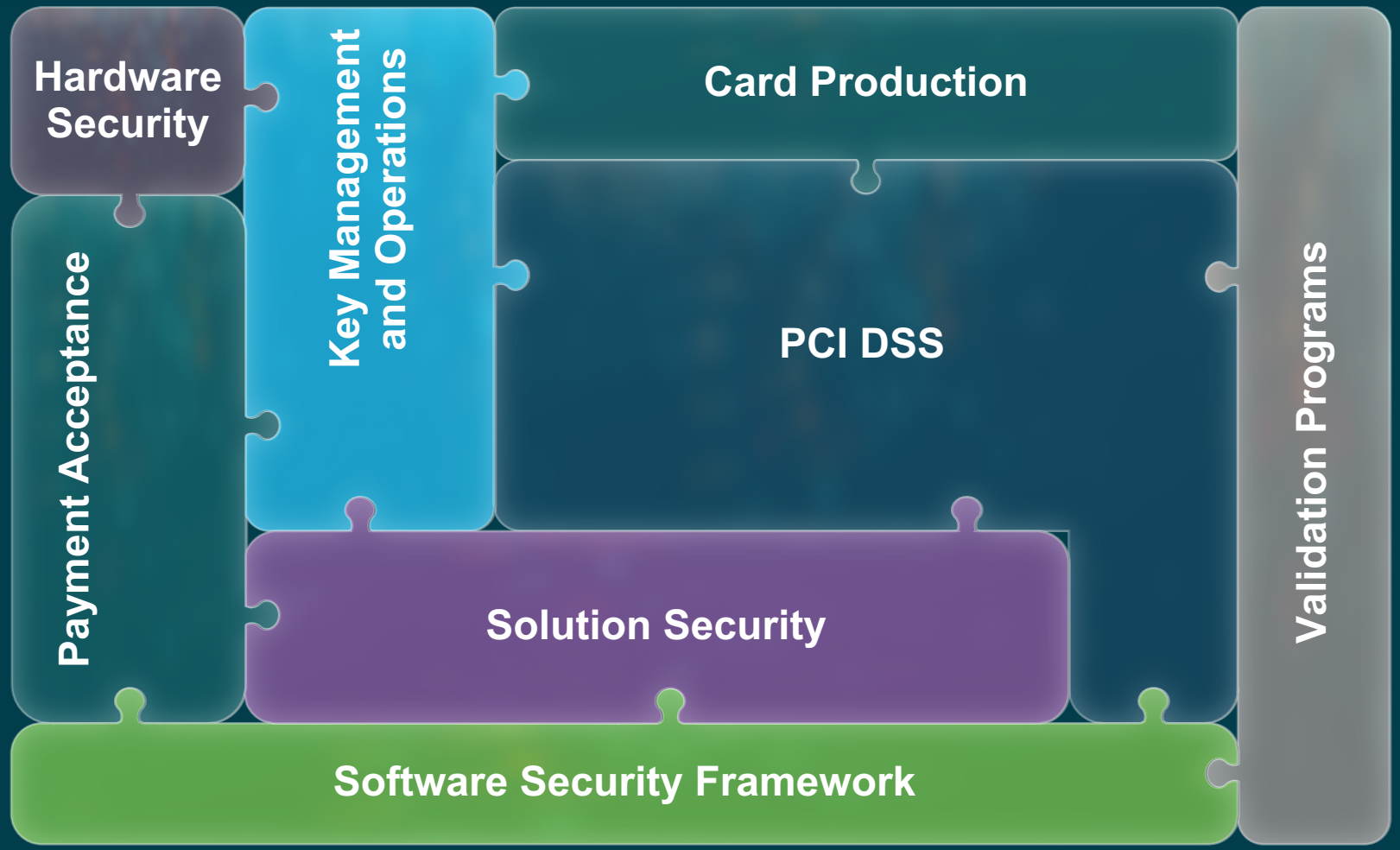
# Solving the PCI SSC Jigsaw



# Solving the PCI SSC Jigsaw



# Solving the PCI SSC Jigsaw



# Solving the PCI SSC Jigsaw




Why?


Plans are worthless
–Dwight D Eisenhower,
November 14 1957


Plans are worthless,
but planning is everything
–Dwight D Eisenhower,
November 14 1957


ELTA
CENTER