

Modernisation of Card Production & Provisioning Specification (PCI-CPP):

Evolution or Revolution?

Stephan Seefeld

R&D Architect

THALES

Nigel Barnes

Solutions Architect

IDEMIA

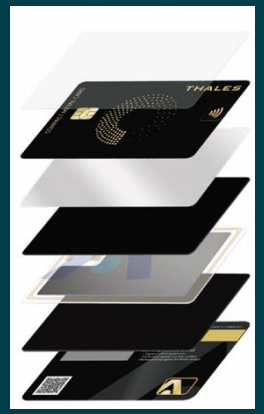




20 YEARS OF SECURING PAYMENT DATA

PCI Security Standards Council

How to Secure Card Production and Provisioning?





- Card Manufacturing
- Chip Embedding







- Personalization (Card, PIN, Letter, …)
- Packaging



- Data Preparation



Provisioner



- Mailing
- Delivery

Individual Scheme Controls	PCI consolidated requirements	RFC
1995	2013	2026

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

The Castle

How to protect a payment card manufacturing site?

In 1995, using $100 millions:

- Protect the perimeter.
- Fences, cameras, vaults, and armoured vehicles

Today, using $100 millions?

- Fences, cameras, vaults, and armoured vehicles ???

If not, what changed?



The Asset Moved

EMV arrived

In the old time

A raw card had a fraud value of $500

Today

A raw card had a fraud value of $0.50

Current reality:

Security has shifted from the physical card to cryptography

The question:

Does a blank EMV card body need to be transported like cash or precious metals?







The Threats Moved

Threats Nobody Was Thinking Of 30 Years Ago:

- Data misuse without physical card
- AI-assisted social engineering
- Software supply chain attacks





Controls Moved

Modern Security Approaches

- Zero Trust **instead of giant wall**
- AI supported threat analysis
- ...

And time doesn't stand still



The Future of PCI-CPP

It solved the risks for which it was originally designed for

Assets and risks and threats evolved

Protect the right assets, the right way



The Future of PCI-CPP

The PCI-CPP have been discussed since 2025, resulting in a RFC and the formation of a Tiger Team.

Future Activities

- Additional RFC cycles for further industry input

Key Areas Under Consideration

- Re-evaluate risks in light of current threats
- Align with PCI DSS and KMO frameworks
- Prioritizing CHD over blank card stock
- Incorporate cloud and remote-access



Reinvent the Wheel?

PCI-CPP should follow the principles established by other PCI standards



Principles

Guiding Principles for the PCI CPP proposal



Threat-Driven

- Focused on Business Assets
- And associated fraud risks



Objective-Based

- Define “what”
- Not “how”
- Testable reqs.



Harmonized

- Aligned with PCI standards
- Leverage DSS
- Leverage KMO



Scalable

- Risks not the same at 1k or 1M cards/mo
- Design controls to scale with production & risk



Modular

- Support multiple deployment models (on-prem, priv-cloud, cloud)
- Open to future form factors

20 YEARS OF SECURING PAYMENT DATA
PCI Security Standards Council

How to protect a payment card manufacturing site?

The future security of payment card manufacturing will not be built on thicker walls.

It will be built on smarter controls.

