PCI Security Standards Council®

2025 EUROPE COMMUNITY MEETING

2025 EUROPE COMMUNITY MEETING

Leveraging Confidential Computing for Sensitive Operation in the Cloud

PCI Security Standards Council

Bruno Besson

CTO Pay Business Line

THALES / Cyber Security & Digital Identity

THALES

Cyril Solé

Principal Engineer Pay Business Line

THALES / Cyber Security & Digital Identity

THALES

PCI Security Standards Council

This is THALES

Empower Customers to face their decisive moments with confidence

PAY BL provides digital and physical payment methods to more than 3000 financial institutions

THALES D1 is our SaS fast-growing platform to support Launch of modern card program, covering 60+ countries and 180+ active users.

An Introduction to Confidential Computing

Confidential computing is a security and **privacy-enhancing** computational technique focused on **protecting data in use**

By performing computation in a **hardware-based**, **attested e**nvironment

Environment are typically Trusted Execution Environment (TEE) provided by processor manufacturers

Confidential Computing in the Trust Chain

Hardware Security Module (HSM)

Providing state of the art encryption capacity.

Providing native encryption in use by implementing functions

Confidential Computing

Moderate elasticity

Environment considered as trusted

Cloud Computing (VM)

Highly elasticity

Environment considers as untrusted

Cloud-based Confidential Computing

All major cloud providers propose a confidential computing offer.

AWS present a disruptive approach by leveraging its own Hypervisor as a **hardware-based**, **attested** environment

AWS defines confidential computing as the use of **specialized hardware** and associated **firmware** to protect customer code and data during **processing** from outside access

https://aws.amazon.com/blogs/security/confidential-computing-an-aws-perspective/

SaaS Offering

Stakes and Challenges

PCI Security Standards Council

Thales D1 Key principles

Easy to Integrate

- Simplified integration
- Speed-up time-to-market

Highly Scalable

- Mission critical use cases
- Serving worldwide customers
- Adapted to peak season

Compliant

- PCI-DSS, ISO27001 compliant
- Country specific regulation

Challenges and Limits

Systematic use of the HSM

- For all categories of sensitive data
- Regardless of the data classification

Limited elasticity

- It is possible to add HSM
- Non adapted to seasonal pics

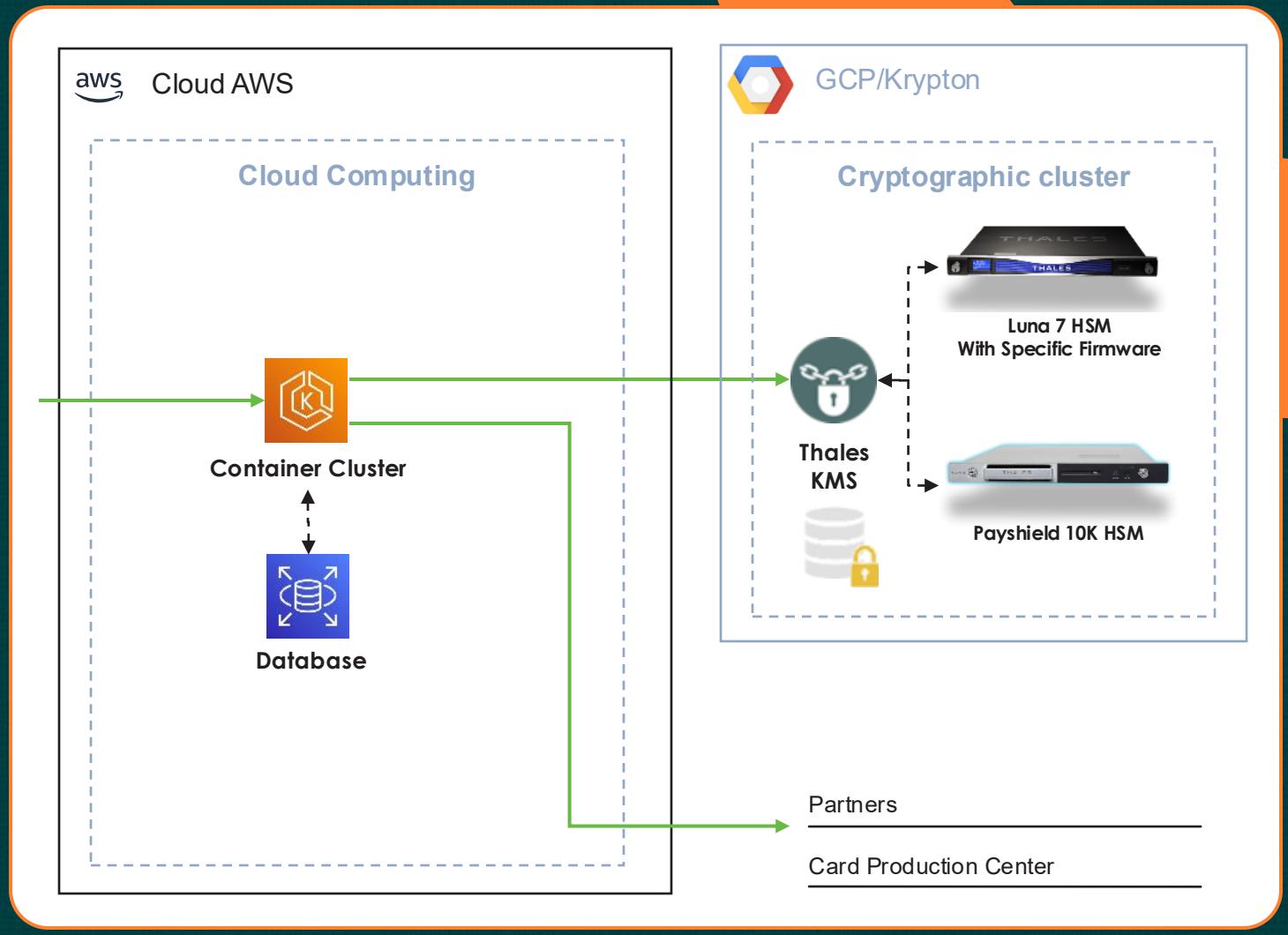
Objective & Study

- Improve our SaaS offer with confidential computing to increase encryption in use in the cloud
- Our study investigated a straightforward use case, well-suited for enclave-based in-use encryption: **securely displaying card information**

Ecosystem Overview

Key components and layers

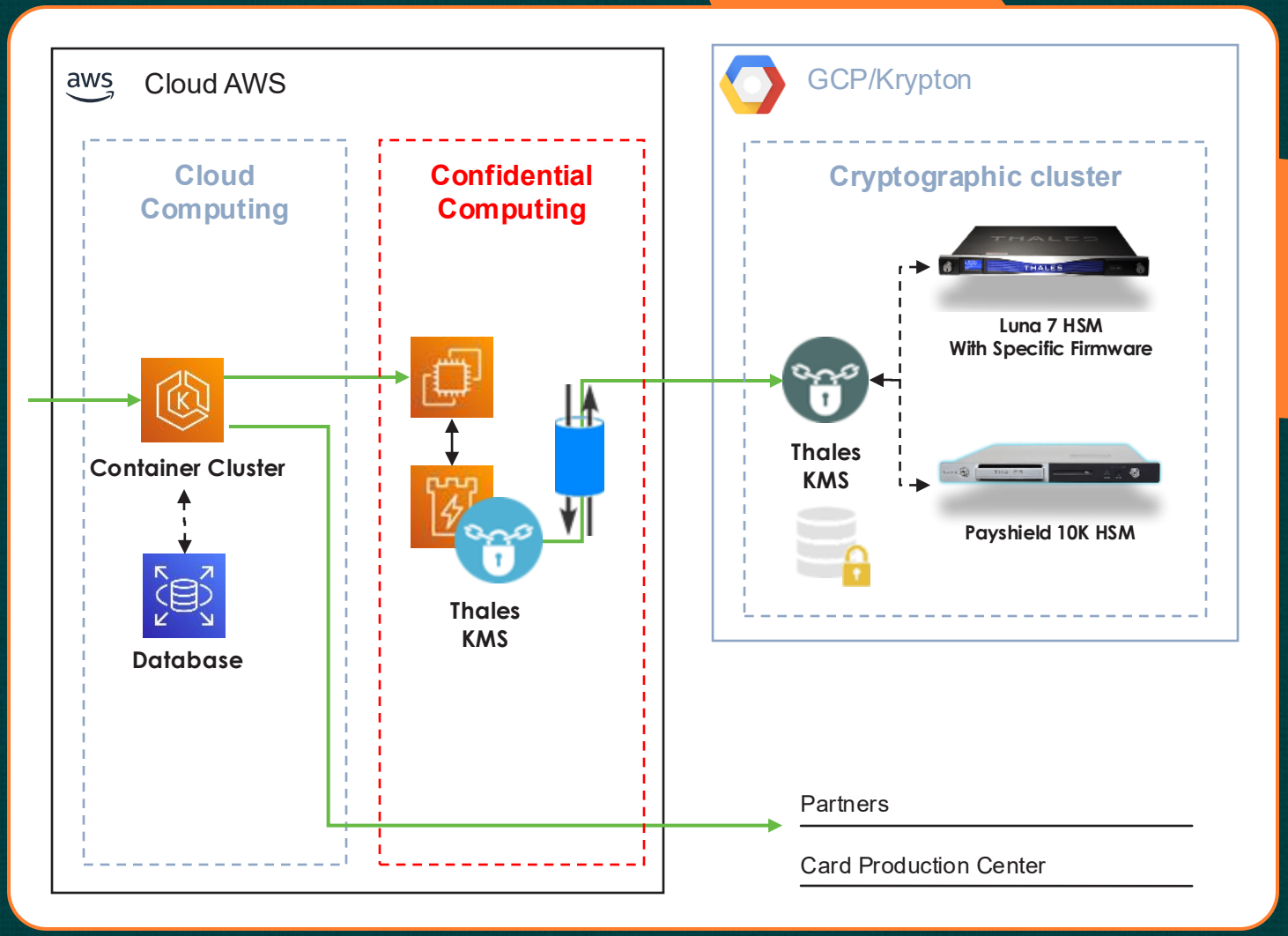
- A PCI/DSS certified solution already deployed in the AWS cloud
- A cryptographic cluster already deployed in the GCP cloud



Cloud Enclaves

Positioning and challenges in Cloud

- Introducing a confidential computing layer in our existing ecosystem



Study Results

Achievements and Opportunities

PCI Security Standards Council

Achievements

Confidential Computing : a way to enhanced our crypto features while retaining our core principles

- Reduce Latency
- Enhance Crypto Elasticity
- Keeps our strong key management
- Inline with our zero-trust approach

However...

Key Learnings

- Entry cost is significative
- Nitro technology is specific to AWS
- Confidential Computing environments, by design, enforce strong isolation boundaries that limit traditional monitoring and observability mechanisms
- One tips : Enclave-resident code should remain lightweight to simplify control and uphold the security mode

THALES

Thanks!

PCI Security Standards Council