Why You Shouldn’t Trust The Public Cloud For Cardholder Data, A Look At Confidential Computing

Microsoft did it, should you?

Ashok Misra

Principal Program Manager
Commerce Financial Services, Microsoft.

Microsoft

Brad Turner

Principal Security Assurance Architect
Commerce Financial Services, Microsoft

Microsoft

PCI Security Standards Council

Why migrate payment platforms to the cloud?

Aren’t payment platforms “high security environments” (HSE)?

Security Standards Council

Should I trust *any* cloud with my customer's confidential payment data and secrets?

Why did Microsoft move its own payment gateway?

PCI Security Standards Council

What sort of precautions should I take to move them and why is cryptography in the cloud safe?

Existing Encryption		Confidential Computing
Data at rest Encrypt inactive data when stored in blob storage, database, etc.	**Data in transit** Encrypt data that is flowing between untrusted public or private networks	**Data in use** Protect/encrypt data that is in use, while in RAM, and during computation

Protect against

Insider threat
privileged admins abusing rights

Hackers
exploiting bugs in the Hypervisor/OS

Third parties
accessing data without customer consent

Provides

The protection of data in use by performing computation in a hardware-based, attested Trusted Execution Environment (TEE).

Verifiable assurance for data integrity, code integrity, and data confidentiality.

PCI Security Standards Council

Evolving Regulations for Data Protection – Is PCI Next?

Compliance/Regulations	Date released	Region	Notes/Comments	Relevant section
Framework for Adoption of Cloud Services by SEBI Regulated Entities	March 2023	India	**Direct reference to confidential computing** "Data-in-use i.e., wherever data that is being used or processed in the cloud, **confidential computing solutions shall be implemented**."	Section 6.2.9
California Consumer Privacy Act (CCPA)	January 2020	California , USA	Need for reasonable security procedures and practices	Section 1798.81.5
General Data Protection Regulation (GDPR)	May 2018	European Union	• **Need for state-of-the-art security measures**. • Accountability for protection of data and showing compliance.	• Article 32 – Security of processing • Article 5(2) & Article 24 – Principle of accountability
Lei Geral de Proteção de Dados (LGPD)	August 2020	Brazil	**Need for state-of-the-art security measures**.	• Article 46 – Security and Secrecy of Data
Personal Information Protection and Electronic Documents Act (PIPEDA)	January 2021	Canada	Accountability for protection of data.	Schedule 1, Section 4.1.4
Personal Data Protection Act (PDPA)	January 2013	Singapore	Accountability for data protection	Section 11 & 12
Digital Operational Resilience Act (DORA)	December 2022	European Union	Financial entities shall design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to **maintain high standards of availability, authenticity, integrity and *confidentiality* of data, whether at rest, in use or in transit**.	• Article 9, protection and privacy • Digital Operational Resilience Act (DORA), Article 9 (digital-operational-resilience-act.com)

Confidential Computing Consortium

The Confidential Computing Consortium (CCC) brings together hardware vendors, **cloud providers**, and software developers to accelerate the adoption of Trusted Execution Environment (TEE) technologies and standards

A community focused on projects securing data in use and accelerating the adoption of confidential computing through open collaboration

Microsoft is a founding member, and chairs both the governing board and the Technical Advisory Council (TAC) of this open source community

Premier

Microsoft intel Red Hat arm Meta

HUAWEI ORACLE Google Alibaba Cloud

General

AMD ByteDance cosmian swisscom Anqlave

Baidu 百度 Fortanix OASIS LABS anjuna decentriq

NVIDIA KINDITE Tencent 腾讯 vmware

*Other names and brands may be claimed as the property of others.

PCI Security Standards Council

Summary

- Be cautious moving sensitive or confidential workloads to the cloud – consider how those compute workloads are protected from the cloud provider and other adjacent customer workloads.
- Consider how you shift adoption away from on-prem physical HSM to cloud-based HSM
- With the right investment in Confidential Computing, moving payment related services to the cloud can be secure.
- Work to include “Encryption in Use” scenarios as part of your security policies and standards for sensitive or confidential data.
- Expect regulatory requirements to evolve to include Confidential Computing requirements for sensitive or confidential data. The PCI space is especially fitting.


PCi
Security
Standards Council
®