
enclaive
CONFIDENTIAL COMPUTING MADE SIMPLE
Run any workload on the safest cloud ecosystem
Get Started
CONFIDENTIAL COMPUTING CONSORTIUM

CUSTOMER CHALLENGES

Security concerns

- Storing sensitive data in the cloud raises concerns about unauthorized access and data breaches due to single points of attack.

Compliance concerns

- Meeting regulatory requirements for data protection can be challenging in a shared environment, especially when managed by third-parties.

Vendor Lock-In

- Organizations may become dependent on a specific cloud service provider's technologies, making it difficult to switch providers.

{ Mission }

WELCOME TO ENCLAIVE

We help customers to protect data, application and business logic by providing digital safes – so called enclaves – around any workload anywhere.

Product vHSM

{Portfolio}

OUR vHSM_

// Hardware Rooted

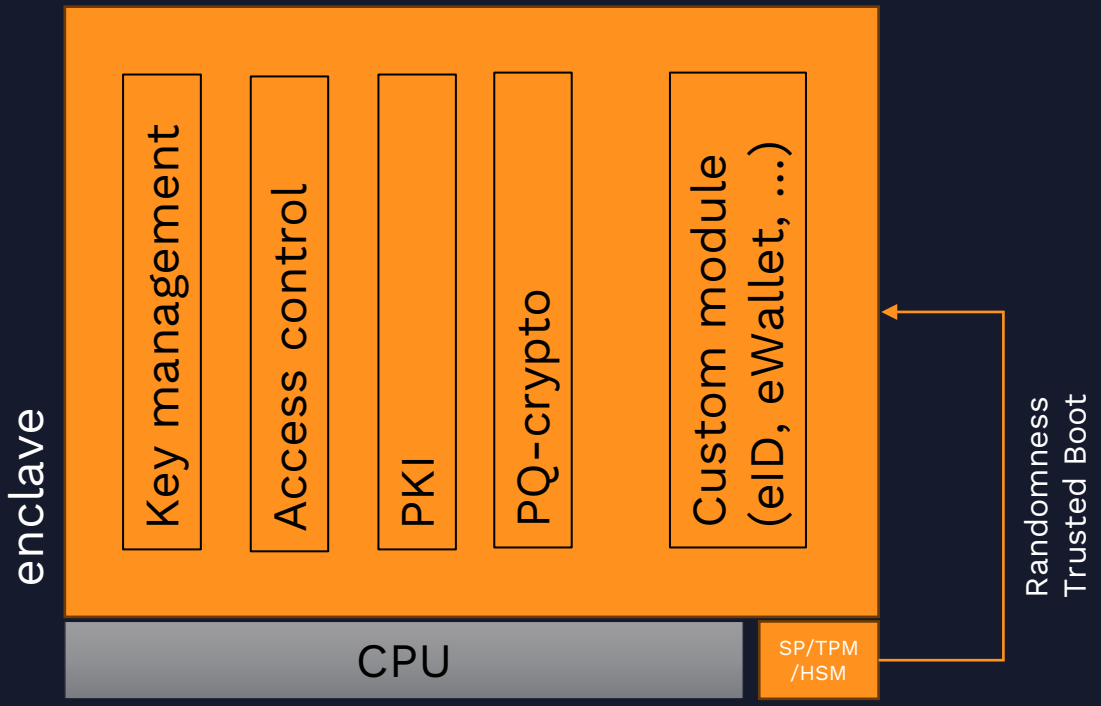
Trust based on hardware element (SP, TPM or HSM)

// Software Enclaved

Services are run-time memory encrypted

// Sealed

Persistant storage is sealed by HW to run only in ENCLAVE



No Vendor Lock

Runs on any infrastructure

Trust Anchor

SP, TPM or HSM

Crypto Agile

Choose your crypto (e.g. PQ/Isogeny)

High Performance

Up to 192 cores, 8 TB RAM

High Availability

Fault-tolerant clustering

Trusted Domains

Multi-tenancy on single / clustered vHSM

Supporting the Capabilities needed to run and control Digital Businesses

Key Distribution:

- Securely distributes keys over untrusted networks protection against eavesdropping & man-in-the-middle attacks.

Key Generation & Storage:

- Generating truly random keys and securely storing them for distributed and cloud-based environments.

Key Backup and Recovery:

- Enabling secure backup and recovery of the keys to grant business resilience.

Compliance and Auditing:

- Underpinning the requirements excerpted by industry and regulatory standards and ongoing compliance monitoring requirements.

Key Rotation:

- Rotating the keys without any disruption in operations ensuring high availability .

Key Revocation:

- Preventing the misuse of compromised keys, ready for large distributed and multi cloud systems.

Access Control:

- Integrated into your IAG and ready for workload identity management supported by NITRIDE.

Scaling:

- Build to scale seamlessly as keys and confidential computing become the cornerstone of the future compute.

{Comparison}

HSM vs vHSM_

6 reasons to choose vHSM_

1. Budget friendly as underlying HW is commodity
2. Customizable as overlying SW is an enclave
3. Usage/maintenance as simple as with a VM/K8s cluster
4. Bring your own app (e.g. PKI, eID, eWallet, cryptoWallet)
5. Cloud ready (store disc encryption keys, container credentials, k8s certs)
6. Scales dynamically when you need it

CUSTOMER REFERENCES

Meedio - Danish software firm specializing in medicine and oncology

Challenges:

- Transitioning from a **non-compliant**, vulnerable infrastructure to a **secure, confidential** cloud environment.
- **Securing sensitive medical and oncological data** against potential breaches and unauthorized access.

Solution (vHSM):

- enclaive's vHSM solution integrated HSM services, KMS, IAM, and secrets management, all certified to **high security standards**.
- **Unified key management system** enabled independent control of cloud encryption keys, crucial for data security and compliance.

Results:

- Enhanced data protection and integrity, ensuring secure management of sensitive health data and compliance with stringent regulatory standards.
- **Scalable and cost-effective** security measures allowed Meedio to adapt flexibly to evolving security needs, safeguarding their investment.

EXECUTIVE SUMMARY

vHSM shields your keys for all your data, signatures, communications ensuring the confidentiality, integrity, and authenticity of sensitive information!

- Centralizing Key Management across the complete digital estate gives you the control .
- Enables the management of ANY key within your control on the infrastructure of your choice
  - **No change to code**
  - **No change to DevOps**
  - **No change to infrastructure**
  - **No performance penalty (+2% CPU cycles)**
- Support all current an future challenges
  - **Move IT to cloud and become financially agile through CAPEX-to-OPEX shift**
  - **Reduce internal IT workload with IaaS/SaaS/PaaS in contrast to expensive self-hosted services**
  - **Protect business IPs (e.g. code, data, docs) in environments managed by third parties (e.g. external devs, cloud service provider, customer's infrastructure)**
  - **Shield IT from bad actors, vulnerabilities, weak isolation of virtualization and save on security expenses**
  - **Avoid fines and liability lawsuits for data leaks/GDPR violations**
  - **Untap business cases and industry segments that have been avoiding cloud/SaaS, or where regulations put a high burden (e.g. CRITIS, finance, insurance, public, defense)**

{Contact}

CONTACT US_

Phone
+49 30 233292970

E-mail
contact@enclaive.io

Address
Chausseestr. 40
10115 Berlin


enclaive
CONFIDENTIAL COMPUTING
MADE SIMPLE
Get Started
THANK YOU