
enclaive
Solution Brief
enclaive Managed vHSM
Key and Workload Identity Management
for Advanced Managed Services

enclaive

Executive Summary

Protected secrets are, and will remain, the bedrock of any robust IT architecture. However, the transition to the cloud introduces a critical dilemma: traditional Hardware Security Modules (HSMs) are often prohibitively expensive and lack the scalability required by modern service providers. Conversely, the native Key Management Systems (KMS) offered by hyperscalers often force customers to compromise on digital sovereignty.

Plus, standard encryption methods fail to protect data while it is being processed ("in use"). In cloud environments, this creates a significant vulnerability that cybercriminals or state actors can exploit to access sensitive customer data – or, worst-case scenario, compromise the service provider's entire infrastructure.

The enclaive virtual High Security Module (vHSM) bridges this gap by combining the unparalleled security of traditional HSMs with the agility of the cloud. Powered by Confidential Computing, the vHSM ensures "3D Encryption" – protecting data at rest, in transit, and in use within isolated hardware enclaves. This architecture delivers a new standard of key security – not even privileged administrators, cloud providers, or service providers have access –, and opens up opportunities in one of the fastest growing security markets.

Designed as a cloud-native, multi-tenant solution, the vHSM empowers MSPs and MSSPs to deliver highly secure, scalable managed services cost-effectively. It introduces a paradigm shift in security, featuring agile, post-quantum cryptography to future-proof client environments.

This document provides MSPs and MSSPs with an overview about the vHSM's functionality and core features. Learn how to leverage this technology to differentiate your portfolio, enter high-security markets, and drive sustainable revenue growth.

enclaive

70%
lower operating costs with vHSM compared to traditional HSM

Recommended by official bodies (BSI C5, gematik, DORA §9)

Only
2-3%
additional overhead for 3D Encryption

~50%
CAGR for the confidential computing market over the next 5 to 10 years

Gartner lists Confidential Computing as one of the
10 Strategic Technology Trends 2026

enclaive

Challenges

More and more companies are relying on the expertise of MSPs and MSSPs to meet complex regulatory and security requirements in the cloud. As a service provider, your challenge is to maintain your edge in a growing market – and to differentiate your offerings from both the competition and the major hyperscalers.

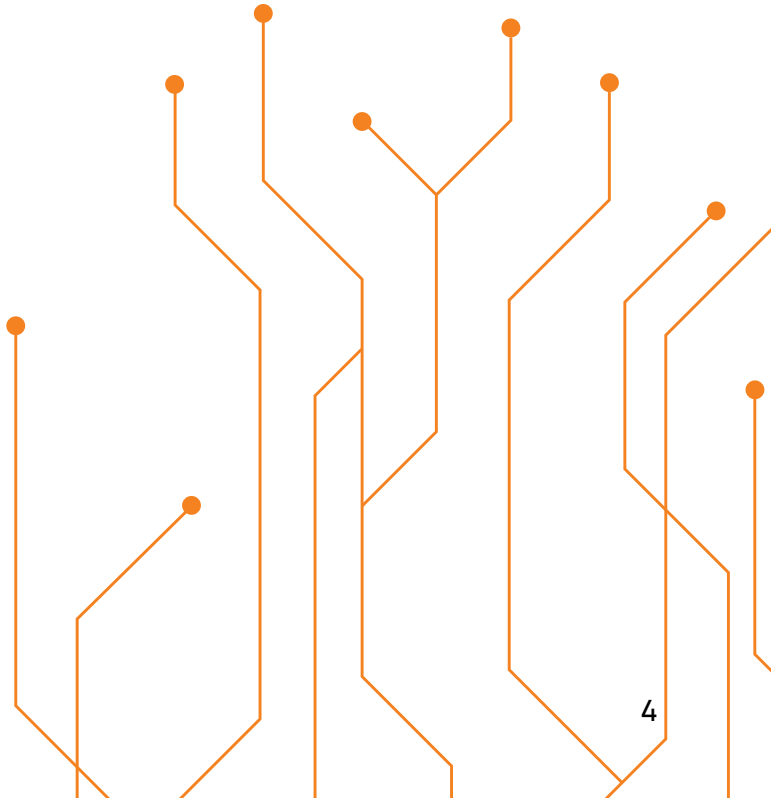
Cryptography as a Strategic Service Pillar

How can you provide your customers with genuine added value in terms of security, sovereignty, and compliance? Through robust cryptography and secure key and secrets management – because keys, certificates, and identities form the foundation of trust for applications and digital business processes. For service providers capable of meeting the stringent demands of both customers and regulators, this presents enormous potential. However, traditional approaches often fall short:

- **Legacy HSMs** meet the highest security standards but are notoriously difficult to scale. High capital expenditure (CapEx), complex operations, and a lack of flexibility make them economically unattractive for standardised managed service models.
- **Cloud KMS and Hyperscaler HSM** offerings are convenient, but effectively shift control over the keys to the cloud provider. For customers, this means comromised sovereignty and potential compliance risks; for MS(S)Ps, it leads to a lack of differentiation and increasing dependency on the hyperscaler.
- **Software-based secret vaults** are quick to integrate but fail to protect data during processing. They often hit compliance ceilings in regulated industries – the very sectors where long-term, high-margin customer relationships are built.

- Regardless of the specific technology, customers today are increasingly asking a fundamental question: How can we simplify our secrets management while ensuring the absolute confidentiality of our keys?

Traditional security models fail to provide a convincing answer.



enclaive

The Solution

enclaive addresses these challenges with a fundamentally new approach: the virtual High Security Module (vHSM). The vHSM combines the security level of traditional HSMs with the flexibility and cost-effectiveness of the cloud. From a technical standpoint, the cloud-native vHSM is based on Confidential Computing, executing cryptographic processes within hardware-isolated CPU enclaves.

Each enclave forms its own trust domain, the integrity of which is cryptographically verified via Trusted Boot and Remote Attestation: Keys and functions are only released after successful validation. In this model, trust is not assumed – it is proven. This makes it a core component for modern Zero Trust architectures and compliance audits. As a dedicated crypto engine, the vHSM also serves as an enabler to make applications, databases, and AI workloads "confidential."

Confidential Computing: Next-Gen Encryption and a New Revenue Stream for Service Providers

Traditional encryption protects data at rest and in transit, but not during processing. Confidential Computing closes this gap by encrypting sensitive workloads within hardware-based, isolated Trusted Execution Environments (TEEs) – also known as enclaves. This ensures that data remains protected "in use," inaccessible even to privileged insiders, cloud providers, or service providers.

As one of the fastest-growing segments in the security market, Confidential Computing is particularly lucrative for service providers: the CAGR for the next 5–10 years is estimated at approximately 50%. Gartner predicts that by 2029, 75% of all public cloud workloads will be protected "in use." Furthermore, the technology is explicitly recommended by the BSI (German Federal Office for Information Security) in its current C5 catalog for sensitive cloud workloads. The performance overhead for Confidential Computing is typically in the low single digits, making it negligible for most operations.

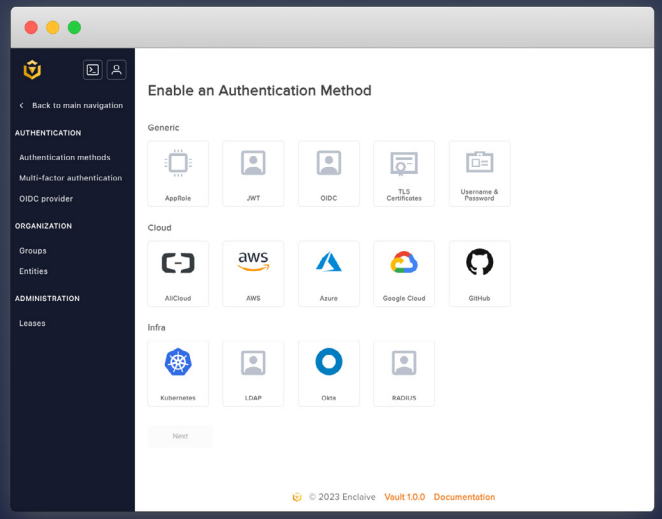
Technical Requirements: Intel TDX / AMD SEV-SNP and Linux 6.11.

enclaive

enclaive delivers the full functional scope of the vHSM through two core solutions: Vault and Nitride.

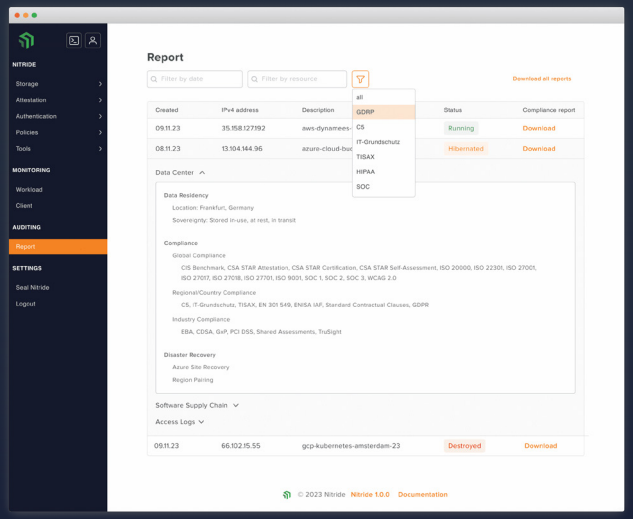
Vault

Vault enables cross-cloud key management based on the Hold-Your-Own-Key (HYOK) principle. Users retain full control over their cryptographic keys at all times, ensuring that only they can decrypt their enclaves. Vault simplifies access management by recognizing various authentication methods – from standard credentials to SSO – while providing granular access rights and seamless integration with external IAM platforms.

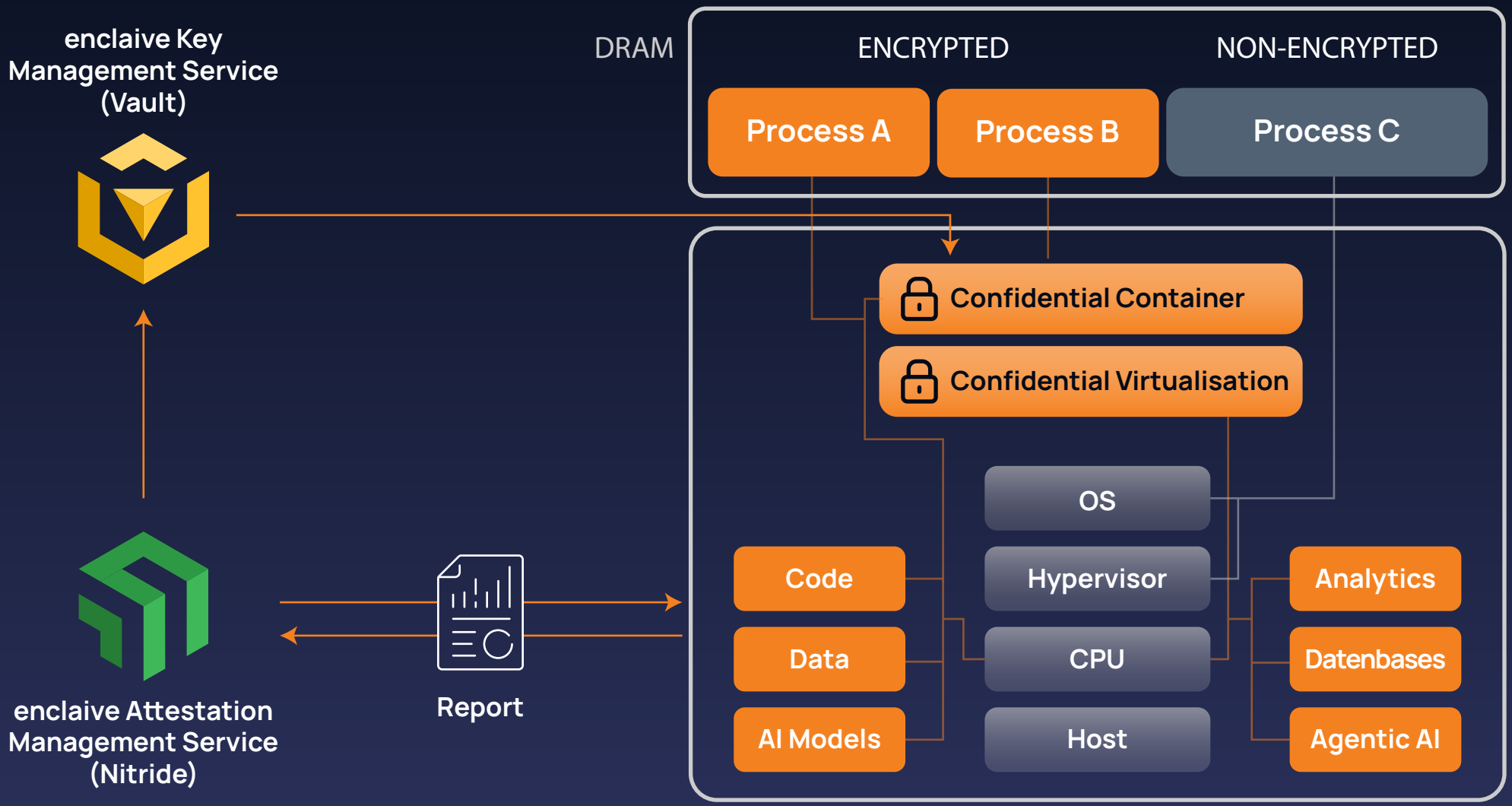


Nitride

Nitride provides workloads and users with unique identities and granular access permissions. Through cryptographic attestation, it ensures that enclaves only boot using verified, trusted components. This provides users with verifiable integrity for their confidential workloads, while the integrated reporting feature makes meeting compliance and audit requirements effortless.



enclaive

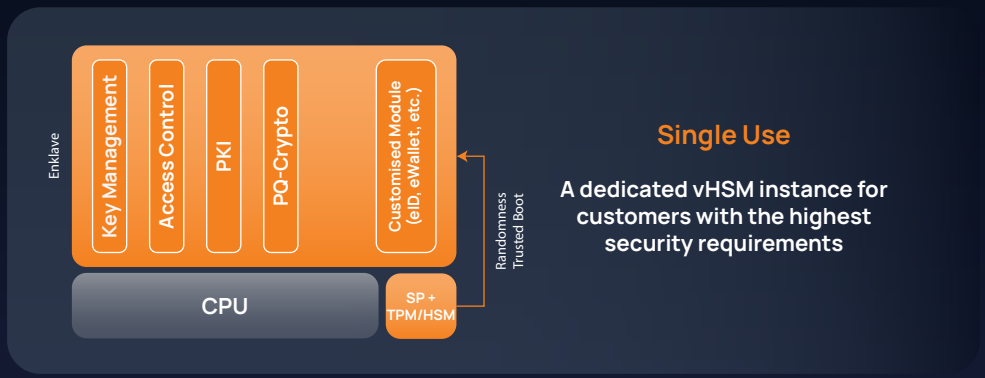

enclaive Key Management Service (Vault)
DRAM
ENCRYPTED
NON-ENCRYPTED
Process A
Process B
Process C
Confidential Container
Confidential Virtualisation
OS
Code
Hypervisor
Analytics
Data
CPU
Datenbases
AI Models
Host
Agentic AI
Report
enclaive Attestation Management Service (Nitride)

enclaive

The vHSM as a Managed Service

As a cloud-native and multi-cloud ready solution, the vHSM is a highly flexible, low-maintenance crypto engine that service providers can easily integrate into their portfolios. Instead of managing physical hardware, MSPs and MSSPs operate the vHSM in the cloud, taking responsibility for availability, scaling, updates, and monitoring.

Depending on the customer's security requirements, service providers can offer the vHSM via dedicated VMs (via enclaive Buckypaper) or redundant Kubernetes clusters (enclaive Dyneemes). In every model, the customers retain complete control over their policies and keys (Bring and Hold Your Own Key).



Single Use

A dedicated vHSM instance for customers with the highest security requirements

Trusted Domains

Multi-client hosting within a single vHSM instance – balancing high security with optimal resource utilisation

Cluster

High availability through redundant clustering

enclaive

The features of the vHSM offer managed service providers ideal conditions:

Implementation and Operations

- **Multi-tenancy:** Every customer receives their own isolated enclave for secrets management. This is ideal for multi-tenant platforms, SaaS providers, and shared services.
- **Seamless Integration and Modularity:** As an open-source-based solution with standardised APIs (PKCS#11, KMIP, REST), the vHSM integrates anywhere without code changes and can be extended with custom functions as needed.
- **External Root of Trust Integration:** To harden the vHSM's cryptographic performance, physical HSMs can be integrated as a Root of Trust.
- **Software Flexibility:** The vHSM scales automatically, features self-healing for failed instances, and adapts to new cryptographic standards via simple software updates.

Security and Sovereignty

- **Enclave Isolation:** Confidential Computing adds a new layer of protection to a hardened key and secrets management. Not even the infrastructure provider has access to keys or certificates, strengthening both sovereignty and Zero Trust.
- **Post-Quantum Cryptography (PQC):** enclaive already utilises post-quantum secure algorithms to provide long-term security and protection against "harvest now, decrypt later" attacks.
- **Remote Attestation:** Cryptographic verification that the enclave and its contents remain unaltered. Verifiable workload integrity becomes a vital compliance asset.
- **Workload Identity & Access Management:** Perfect for Zero Trust architectures. Users and workloads are granted only the minimum necessary permissions (Least Privilege) to access the enclaves.

enclaive

How the vHSM Drives Your Business

New Revenue Streams

- **Recurring Revenue via vHSM-based Services:** Offer "Compliance-as-a-Service" to meet requirements for BSI, eIDAS, GDPR, KRITIS, DORA, or healthcare (gematik), complete with tamper-proof audit-trails. Keys remain strictly within EU-compliant boundaries
- **Service Upgrades:** Position the vHSM as a premium add-on, offering enhanced "Data in Use" protection and cloud flexibility
- **Strategic Partnerships:** Seamless integration with industry leaders like Red Hat, SUSE, Hashicorp, or Utimaco – perfect for bundling, e. g. with Managed Kubernetes
- **Upselling Potential:** Leverage single-tenant vHSMs or hardware Root of Trust integration as high-margin premium features

Low Operational Overhead

- **Cost Efficiency:** Eliminate hardware investment, installation, and maintenance. Use auto-scaling to optimise resource consumption and handle peak loads
- **Faster Time-to-Market:** Provision new customer vHSM instances in minutes
- **Multi-tenancy:** Streamline client administration through centralised key management for efficient multi-customer handling
- **Cloud-Native Design:** Benefit from inherent elasticity, high availability, and automated cryptographic updates
- **Easy Implementation:** Ensure high flexibility with multi-cloud readiness and seamless integration into existing infrastructures

Market Differentiation

- **A New Security Paradigm:** Protect "Data in Use" – something traditional architectures simply cannot do
- **Future-Proof Protection:** Post-quantum cryptography builds long-term customer trust
- **Sovereignty Guaranteed:** An independent, European alternative to hyperscaler HSMs –free from vendor lock-in and risks associated with the US CLOUD Act
- **White Labeling:** Customise and extend the open-source-based vHSM to offer proprietary, tailor-made solutions

enclaive

Added Value for Your Customers

Key Sovereignty in Managed Services: Customers control keys and policies; the operator has no access

Post-Quantum-secure Data in Use: A new level of confidentiality and cyber resilience

Verifiable Security Cryptographic proof that keys are processed exclusively in protected enclaves – perfect for audits

Confidential Computing Use Cases Secure lift-and-shift migrations, confidential collaboration, and secure AI interactions

Conclusion

A platform for advanced managed services

With the enclaive Managed vHSM, service providers gain a central crypto engine to build and refine high-value, scalable, and high-margin services. The combination of hardware-backed security, cloud-native architecture, and the strict separation of operations from key sovereignty creates a robust foundation of trust – without the economic and operational burden of traditional HSM models.

The vHSM allows service providers to clearly differentiate themselves from hyperscalers and competitors while offering customers tangible security and compliance benefits. For MSPs and MSSPs, cryptography evolves from a necessary infrastructure component into a strategic service enabler.

enclaive

Launch your vHSM business today!

Expand your portfolio with managed services that combine security, sovereignty, and scalability. Position yourself as a provider of modern, trusted security services and unlock new revenue in regulated and mission-critical markets.

How enclaive supports you:

- Continuous vHSM development, including free updates
- Kickoff workshops and support for pilot projects
- Co-marketing and co-selling opportunities
- Attractive partner and pricing models

Contact
sales@enclaive.io

For more information, visit
enclaive.io