
enclaive
Solution Brief
enclaive Managed vHSM
Key und Workload Identity Management
für attraktive Managed Services

enclaive

Executive Summary

Geschützte Secrets sind das Fundament sicherer IT-Architekturen – und werden es bleiben. Die Cloud stellt hier eine besondere Herausforderung dar: Klassische Hardware Security Module (HSM) sind für Service Provider kostspielig und schlecht skalierbar, während die etablierten Key Management Systeme (KMS) der Hyperscaler die Souveränität ihrer Kunden beeinträchtigen.

Traditionelle Verschlüsselung ist zudem nicht in der Lage, Daten während der Verarbeitung („in use“) zu schützen. Gerade in Cloud-Umgebungen entsteht dadurch eine kritische Sicherheitslücke, über die sich Cyberkriminelle oder staatliche Akteure Zugriff auf sensible Kundendaten oder – im Worst Case – auf die gesamte Infrastruktur des Service Providers verschaffen können.

Das virtual High Security Module (vHSM) von enclaive löst diese Herausforderungen, indem es die Sicherheit klassischer HSMs mit der Flexibilität der Cloud kombiniert. Das vHSM basiert dabei auf Confidential Computing, der Verschlüsselung in allen drei Dimensionen (at rest, in transit, in use) in isolierten Hardware-Enklaven. Damit bietet das vHSM nicht nur ein neues Niveau an Schlüsselsicherheit – nicht einmal privilegierte Admins oder Cloud- und Service Provider haben Zugriff –, sondern auch den Zugang zu einem der aktuell spannendsten Security-Märkte.

Als Cloud-native, multi-mandantenfähige Lösung eröffnet das vHSM MSPs und MSSPs die Möglichkeit, hochsichere und skalierbare Managed Services kosteneffizient bereitzustellen – inklusive eines neuen Sicherheitsansatzes und agiler Kryptografie auf Post-Quanten-Niveau.

In diesem Solution Brief erfahren MSPs und MSSPs mehr über die technische Funktionsweise des vHSM, welche Features es bietet und wie sie diese gezielt nutzen können, um ihr Portfolio zu differenzieren und nachhaltige Umsatzpotenziale in neuen Märkten zu erschließen.

enclaive

70 %
weniger Betriebskosten durch vHSM vs. klassisches HSM.

Von offizieller Seite als Technologiebaustein empfohlen (BSI C5, gematik, DORA §9)

Lediglich
2-3 %
zusätzliche Rechenleistung für 3D-Verschlüsselung

~50 %
CAGR für den Confidential-Computing-Markt in den nächsten 5 bis 10 Jahren

Gartner zählt Confidential Computing zu den
Top 10 Strategic Technology Trends 2026

enclaive

Herausforderungen

Immer mehr Unternehmen setzen auf die Expertise von MSPs und MSSPs, um die komplexen regulatorischen und sicherheitstechnischen Anforderungen in der Cloud zu erfüllen. Für Sie als Service Provider gilt es dabei, sich im wachsenden MS(S)P-Markt zu behaupten – und von den Angeboten der Konkurrenz und denen der großen Hyperscaler abzusetzen.

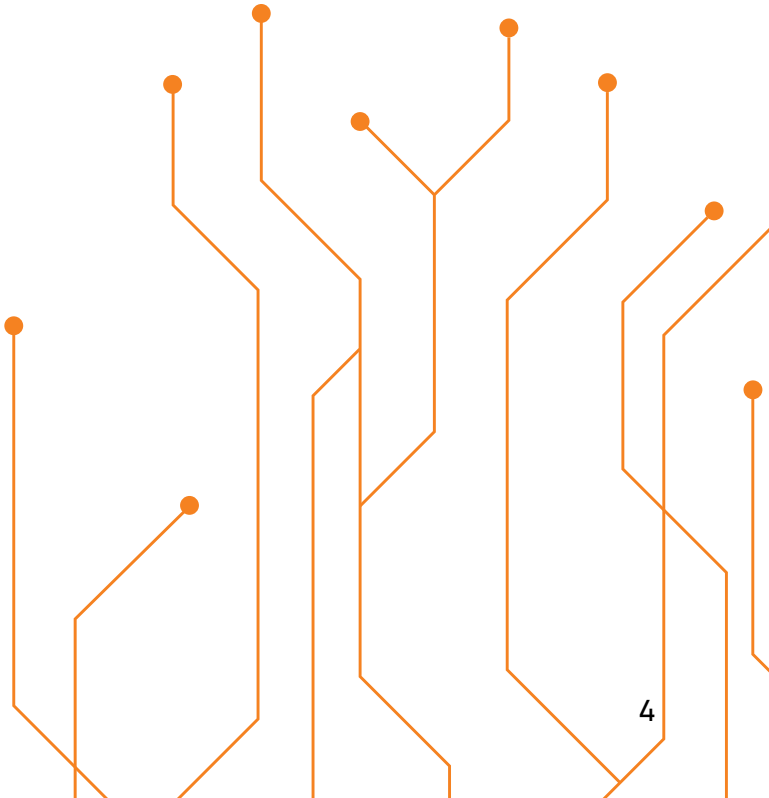
Kryptografie wird zum strategischen Service-Baustein

Wie Sie Ihren Kunden echten Mehrwert bei Sicherheit, Souveränität und Compliance bieten können? Durch starke Kryptografie und ein geschütztes Key und Secrets Management – denn Schlüssel, Zertifikate und Identitäten bilden die Vertrauensbasis für Anwendungen und digitale Geschäftsprozesse. Für Service Provider, die die hohen Anforderungen der Kunden und des Gesetzgebers hier erfüllen können, bietet dies enormes Potenzial. Mit gängigen Ansätzen lässt sich jedoch nur wenig erreichen:

- **Klassische HSMs** erfüllen zwar höchste Sicherheitsanforderungen, sind jedoch kaum skalierbar. Hohe Investitionskosten, komplexer Betrieb und geringe Flexibilität machen sie wirtschaftlich unattraktiv für standardisierte Managed-Services-Modelle.
- **Cloud-KMS- und Hyperscaler-HSM-Angebote** sind bequem, verlagern die Kontrolle über Schlüssel jedoch faktisch zum Cloud Provider. Für Kunden bedeutet das eingeschränkte Souveränität und potenzielle Compliance-Risiken, für MS(S)Ps fehlende Differenzierung und zunehmende Abhängigkeit vom Hyperscaler.
- **Software-basierte Secrets-Tresore** lassen sich zwar schnell integrieren, schützen Daten aber nicht während der Verarbeitung und stoßen insbesondere in regulierten Branchen an Compliance-Grenzen – genau dort, wo langfristige, margenstarke Kundenbeziehungen entstehen.

Unabhängig von der konkreten Technologie stellen Kunden heute zunehmend eine grundsätzliche Frage: Wie vereinfachen wir unser Secrets Management und stellen gleichzeitig die absolute Vertraulichkeit unserer Schlüssel sicher?

Klassische Sicherheitsmodelle liefern darauf keine überzeugende Antwort.



enclaive

Die Lösung

enclaive adressiert diese Herausforderungen grundlegend neu mit seinem virtual High Security Module (vHSM). Das vHSM verbindet das Sicherheitsniveau traditioneller HSMs mit der Flexibilität und Wirtschaftlichkeit der Cloud. Technologisch basiert das Cloud-native vHSM auf Confidential Computing, um kryptografische Prozesse in hardware-isolierten CPU-Enklaven auszuführen.

Jede Enklave bildet eine eigene Vertrauensdomäne, deren Integrität über Trusted Boot und Remote Attestation kryptografisch belegbar ist. Erst nach erfolgreicher Validierung werden Schlüssel und Funktionen freigegeben. Damit wird Vertrauen nicht angenommen, sondern nachweisbar – ein zentraler Baustein für moderne Zero-Trust-Architekturen und Compliance-Audits.

Als Krypto-Engine wird das vHSM zudem zum Türöffner, um Anwendungen, Datenbanken und KI-Workloads „confidential“ zu verschlüsseln.

Confidential Computing – neuartige Verschlüsselung und Geschäftsfeld für Service Provider

Klassische Verschlüsselung schützt Daten im Ruhezustand und bei der Übertragung, aber nicht während der Verarbeitung. Confidential Computing schließt diese Lücke, indem sensible Workloads in hardwarebasierten, isolierten Trusted Execution Environments (TEEs) – auch Enklaven genannt – direkt auf der CPU verschlüsselt sind. Daten sind so auch „in use“ geschützt und selbst für privilegierte Insider sowie Cloud- und Service Provider nicht zugänglich.

Als einer der wachstumsstärksten Security-Märkte ist Confidential Computing für Service Provider besonders interessant: Der CAGR für die nächsten 5-10 Jahre liegt bei etwa 50 %. Gartner prognostiziert, dass bis 2029 75 % aller Workloads in der Public Cloud auch „in use“ geschützt sein werden. Die Technologie wird zudem vom BSI im aktuellen C5-Katalog ausdrücklich für sensible Cloud-Workloads empfohlen.

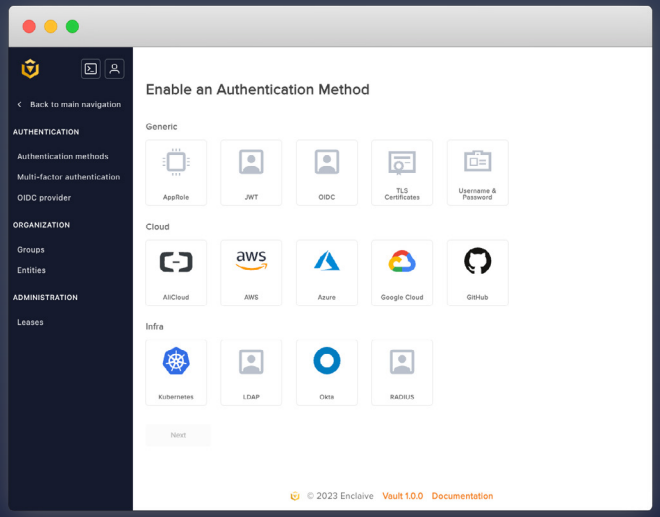
Der zusätzliche Rechenaufwand für Confidential Computing liegt in der Regel im niedrigen einstelligen Prozentbereich, ist also vernachlässigbar. Technische Voraussetzungen: Intel TDX / AMD SEV-SNP und Linux 6.11.

enclaive

Den Funktionsumfang des vHSM bildet enclaive in den beiden Lösungen Vault und Nitride ab.

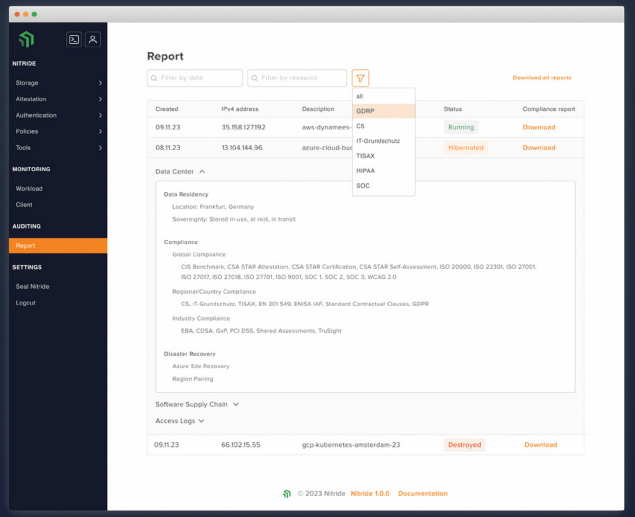
Vault

Vault ermöglicht Cloud-übergreifendes Key Management nach dem Hold-Your-Own-Key-Prinzip. Anwender behalten jederzeit die Kontrolle über ihre kryptografischen Schlüssel und stellen sicher, dass nur sie die Enklaven entschlüsseln können. Vault erleichtert das Zugriffsmanagement, indem es verschiedene Authentifizierungsmethoden erkennt, von Benutzername/Passwort bis hin zu SSO, fein abgestufte Zugriffsrechte ermöglicht und externe IAM-Plattformen integriert.

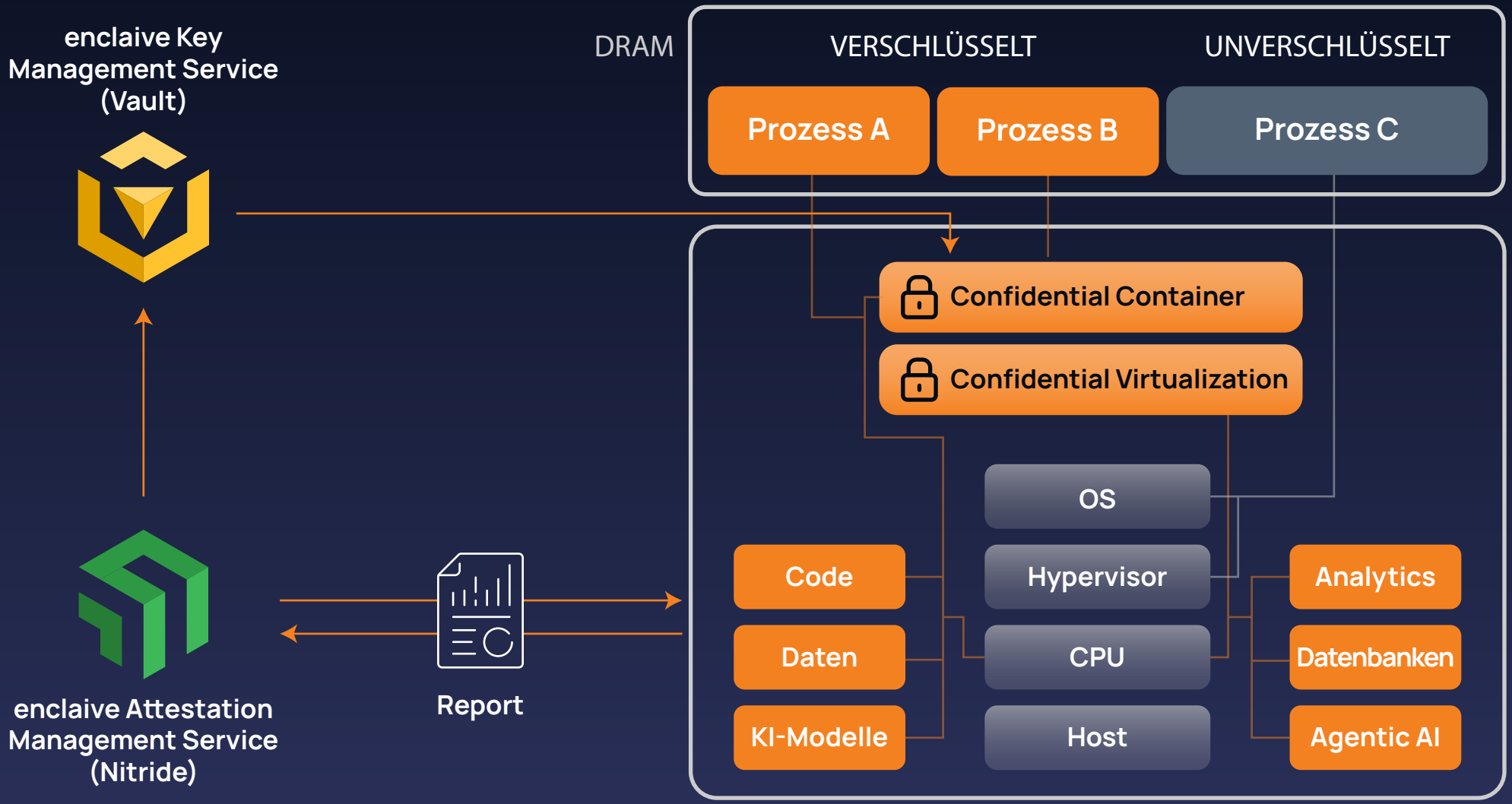


Nitride

Nitride stattet Workloads und Nutzer mit eindeutigen Identitäten und granularen Zugriffsrechten aus. Über kryptografische Attestation wird dabei sichergestellt, dass die Enklaven nur mit verifizierten, vertrauenswürdigen Komponenten booten. So erhalten Anwender nachweisbare Integrität für Ihre vertraulichen Workloads – und mit dem Report-Feature lassen sich Compliance und Audit-Anforderungen mühelos erfüllen.



enclaive

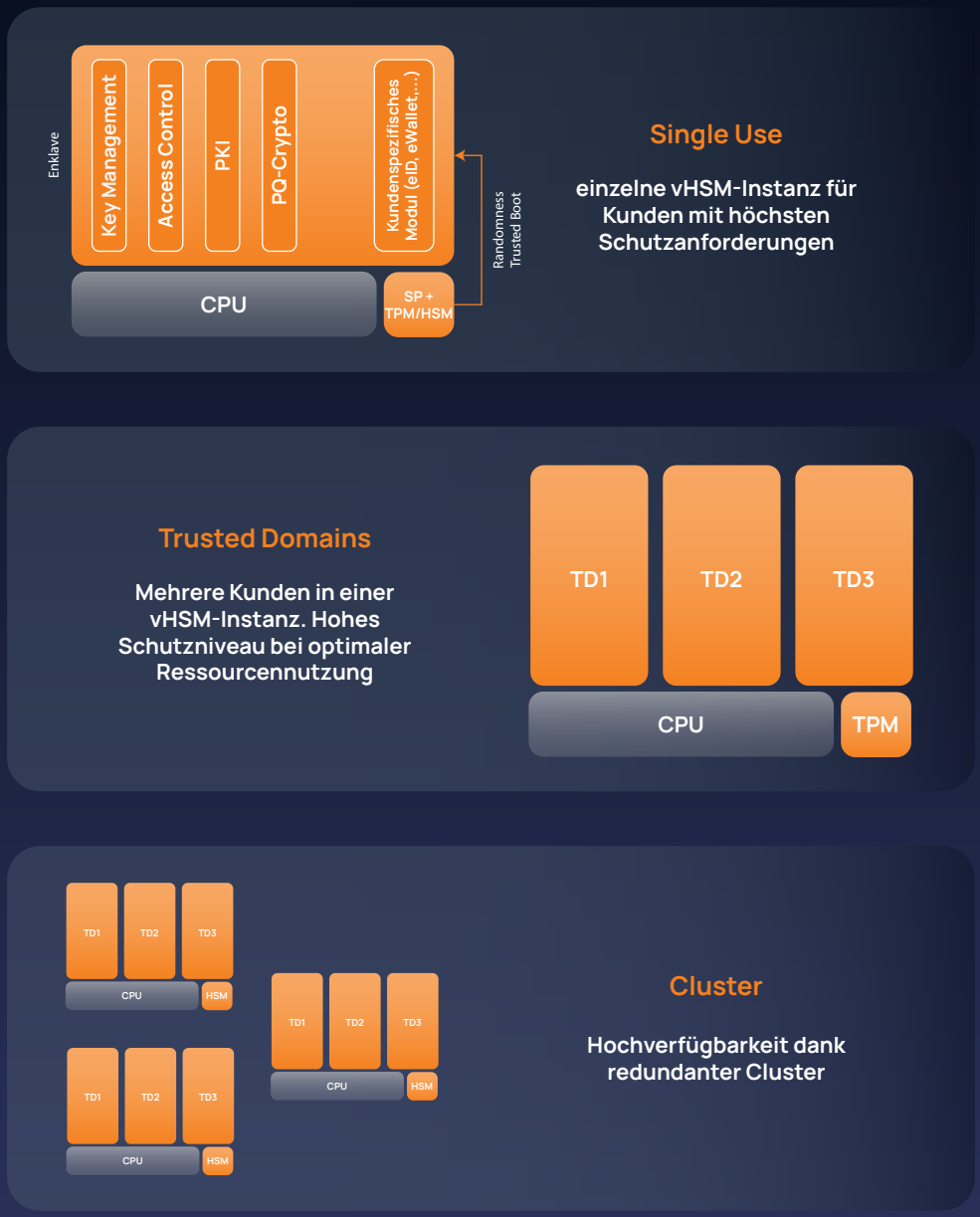

enclaive Key Management Service (Vault)
DRAM
VERSCHLÜSSELT
UNVERSCHLÜSSELT
Prozess A
Prozess B
Prozess C
Confidential Container
Confidential Virtualization
OS
Code
Hypervisor
Analytics
Daten
CPU
Datenbanken
KI-Modelle
Host
Agentic AI
Report
enclaive Attestation Management Service (Nitride)

enclaive

Das vHSM als Managed Service

Als Cloud-native und Multi-Cloud-fähige Lösung ist das vHSM eine hochgradig flexible und pflegeleichte Krypto-Engine, die Service Provider einfach in ihr Portfolio integrieren können. Statt physischer HSMs betreiben MSPs und MSSPs das vHSM in der Cloud und verantworten Verfügbarkeit, Skalierung, Updates und Monitoring.

Je nach Sicherheitsanforderung des Kunden können Service Provider das vHSM in dedizierten VMs (über enclaive Buckypaper) oder redundanten Kubernetes-Clustern (enclaive Dyneemes) anbieten. Der Kunde behält bei jedem Modell jederzeit die vollständige Kontrolle über seine Policies und Schlüssel (Bring and Hold Your Own Key).



enclaive

Diese Features des vHSM bietet Managed Service Providern ideale Voraussetzungen:

Implementierung und Betrieb

- **Multimandantenfähigkeit:** Jeder Kunde erhält eine eigene isolierte Enklave für sein Secrets Management. Perfekt für Multi-Tenant-Plattformen, SaaS-Anbieter und Shared Services.
- **Nahtlose Integration und Modularität:** Als Open-Source-basierte Lösung mit standardisierten APIs (PKCS#11, KMIP, REST) lässt sich das vHSM ohne Code-Änderungen überall integrieren und bei Bedarf um eigene Funktionen erweitern.
- **Einbindung externer Root of Trust:** Um die kryptografische Leistung des vHSM zu „vergolden“, lassen sich zudem klassische HSMs als Root of Trust integrieren.
- **Software-Flexibilität:** Das vHSM skaliert automatisch, ersetzt ausfallende Instanzen („self-healing“) und lässt sich durch simple Software-Updates an neue kryptografische Standards anpassen – Stichwort: PQC-Agilität.

Sicherheit und Souveränität

- **Enklaven-Isolierung:** Confidential Computing als neue Schutzschicht eines gehärteten Key und Secrets Managements. Selbst der Infrastructure-Provider hat keinen Zugriff auf Schlüssel und Zertifikate, was Souveränität und Zero Trust stärkt.
- **Post-Quanten-Kryptografie:** enclaive verwendet bereits Post-Quanten-sichere Algorithmen, die langfristige Sicherheit bieten und schon jetzt vor „Harvest now, decrypt later“-Angriffen schützen.
- **Remote Attestation:** Kryptografische Verifizierung, dass die Enklave und ihr Inhalt unverändert sind und nicht manipuliert wurden. Nachweisbare Workload-Integrität wird zum wichtigen Compliance-Asset.
- **Workload Identity & Access Management:** Ideal für Zero-Trust-Architekturen. Benutzer und Workloads erhalten nur das Mindestmaß an Zugriffsrechten (Least Privilege) auf die Enklaven.

enclaive

Wie das vHSM Ihr Business vorantreibt

Zusätzliche Umsatzmöglichkeiten

- **Recurring-Revenues durch neue vHSM-basierte Services:** Beispiel Compliance-as-a-Service: vHSM erfüllt Anforderungen von BSI, eIDAS, DSGVO, KRITIS, DORA oder gematik und ermöglicht revisionssichere Audit-Trails. Schlüssel bleiben dabei in EU-konformen Grenzen
- **Aufwertung bestehender Services:** vHSM als Premium Add-On. Verbessertes Schutzniveau (Confidential Computing) und Cloud-Flexibilität. Nahtlose Integration mit Branchenführern wie Red Hat, SUSE, Hashicorp oder Utimaco. Ideal für Bundles, etwa mit Managed Kubernetes.
- **Up-Selling-Potenzial:** Nutzen Sie Single-Tenant-vHSMs oder die Integration einer Hardware Root of Trust als Premium-Features

Geringer Kosten- und Betriebsaufwand

- **Kosteneffizienz:** Keine Hardware-Investition, -Installation und -Wartung oder Kapazitäten für Spitzenlasten. Stattdessen automatische Skalierung für optimierte Ressourcennutzung
- **Schnellere Time-To-Market:** Neues Kunden-vHSM ist in wenigen Minuten provisioniert
- **Multi-Mandantenfähigkeit:** Zentrales Schlüsselmanagement für effiziente Kundenverwaltung
- **Cloud-nativ:** Elastizität, Hochverfügbarkeit und Krypto-Updates
- **Einfache Implementierung:** Multi-Cloud-Readiness und nahtlose Integration

Differenzierung im Markt

- **Neuer Security-Ansatz:** Confidential Computing schützt auch Data in use, klassische Architekturen nicht
- **Zukunftssicherer Schutz:** Post-Quanten-Kryptografie erhöht Kundenvertrauen und begünstigt langfristige Zusammenarbeit
- **Souveränitäts-Garant:** Unabhängige, europäische Alternative zu Hyperscaler-HSMs – ohne Vendor-Lockin und Risiken durch den US CLOUD Act
- **Eigenentwicklungen / White Label vHSM:** Erweitern Sie das Open-Source-basierte vHSM bei Bedarf um neue Features und bieten Ihren Kunden maßgeschneiderte Lösungen

enclaive

Mehrwerte für Kunden

Schlüsselhoheit trotz Managed Service
Kunden kontrollieren Keys und Policies, der Betreiber hat keinen Zugriff

Post-Quanten-sicherer Schutz von „Data in Use“
Neues Level an Vertraulichkeit und Cyber-Resilienz

Überprüfbare Sicherheit
Kryptografischer Nachweis, dass Schlüssel ausschließlich in geschützten Enklaven verarbeitet werden. Perfekt für Audits

Confidential Computing Use Cases
Geschützte Lift-and-Shift-Migrationen, sichere Collaboration durch granulare Schlüsselverteilung, vertrauliche KI-Interaktionen

Fazit

Ein Fundament für differenzierte Managed Services

Mit dem enclaive Managed vHSM erhalten Service Provider eine zentrale Krypto-Engine, mit der sich hochwertige, skalierbare und margenstarke Services aufbauen und veredeln lassen. Die Kombination aus hardwaregestützter Sicherheit, cloud-nativer Architektur und klarer Trennung von Betrieb und Schlüsselhoheit schafft eine belastbare Vertrauensbasis – ohne den wirtschaftlichen und operativen Aufwand klassischer HSM-Modelle.

Das vHSM ermöglicht es Service Providern zudem, sich klar von Hyperscalern und anderen Mitbewerbern zu differenzieren und Kunden neue Security- und Compliance-Mehrwerte zu bieten. Für MSPs und MSSPs wird Kryptografie damit vom notwendigen Infrastrukturbaustein zum strategischen Service-Enabler.

enclaive

Starten Sie jetzt Ihr vHSM Business!

Erweitern Sie Ihr Portfolio um Managed Services, die Sicherheit, Souveränität und Skalierbarkeit vereinen. Positionieren Sie sich als Anbieter moderner, vertrauenswürdiger Security-Services und erschließen Sie neue Umsatzpotenziale in regulierten und sicherheitskritischen Märkten.

Wie enclaive Sie dabei unterstützt:

- Kontinuierliche Weiterentwicklung des vHSM inkl. kostenfreier Updates
- Kickoff-Workshops und Unterstützung bei Pilotprojekten
- Co-Marketing und Co-Selling
- Attraktive Partner- und Preismodelle

Kontakt
sales@enclaive.io

Mehr Informationen unter
enclaive.io