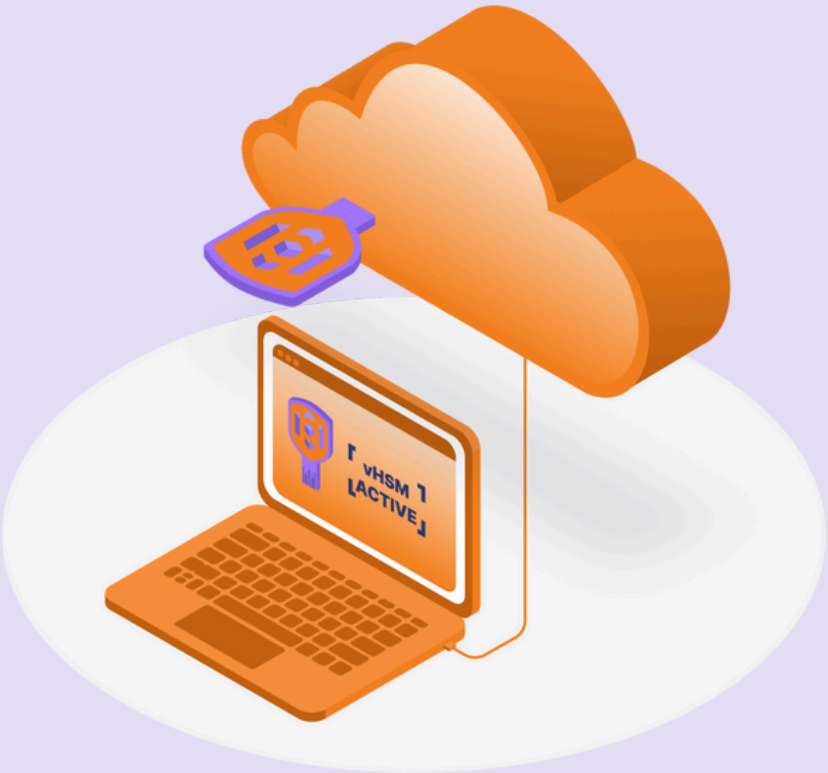
enclaive virtual HSM

Virtual Hardware Security Module (vHSM)

Sebastian Gajek
Andreas Walbrodt

enclaive GmbH



enclaive

ABSTRAKT

Hardware Security Modules (HSMs) sind dedizierte Systeme, die entscheidend für die Stärkung der digitalen Sicherheit sind. Sie bieten eine manipulationssichere Umgebung für das Verwalten kryptographischer Schlüssel und das Durchführen sicherer Operationen. Im Gegensatz zu Softwarelösungen setzen HSMs auf physische Hardware und bieten einen erhöhten Schutz vor spezifischen Cyber-Bedrohungen. Mit zunehmender Bedeutung der Verschlüsselung spielen HSMs eine entscheidende Rolle bei der Sicherung sensibler Informationen und der Gewährleistung der Integrität kryptografischer Prozesse. HSMs werden zum Beispiel im Bankensektor verwendet, um PIN-Authentifikation im Server-Backend abzugleichen, oder um digitale Quittungen im Supermarkt zu erstellen.

Virtualisierung ist eine grundlegende Technologie, die die Erstellung virtueller Instanzen von Rechenressourcen ermöglicht und es ermöglicht, mehrere Betriebssysteme und Anwendungen auf einem einzigen physischen Server auszuführen. Cloud-Computing basiert auf Virtualisierung, um einen bedarfsgesteuerten Zugang zu einem gemeinsamen Pool von Rechenressourcen zu ermöglichen und skalierbare und flexible Dienste über das Internet bereitzustellen.

Die Integration eines HSMs in die Cloud stellt aufgrund der physischen Natur von HSMs, die für On-Premises-Bereitstellungen konzipiert sind, eine Herausforderung dar. Die strengen Sicherheitsmaßnahmen und manipulationssicheren Funktionen von HSMs, die für ihre Funktionalität entscheidend sind, machen eine nahtlose Integration in die dynamische und virtualisierte Umgebung der Cloud praktisch unmöglich

.

Die Einführung von virtuellen Hardware Security Modules (vHSMs) markiert eine bahnbrechende Entwicklung über traditionelle HSMs hinaus, da sie nahtlos in virtualisierten Umgebungen arbeiten und beispiellose Flexibilität und Skalierbarkeit bieten. Durch die Nutzung von Confidential Computing vereinen wir Sicherheit auf Hardware-Ebene mit skalierbarer Virtualisierung und führen die HSM-Funktionalitäten in einer durchgehend verschlüsselten Ausführungsumgebung aus. Dieser innovative Ansatz ersetzt die altbewährte Silizium-Schutzschicht durch softwarebasierte Verschlüsselung zur Laufzeit und ebnet so den Weg für die Ausführung von Schlüsselverwaltung selbst in zuvor als nicht vertrauenswürdig eingestuften Umgebungen, wie der Cloud.

DIE IDEE

Sicheres Key Management ist von entscheidender Bedeutung, weil es die Grundlage für eine robuste und vertrauenswürdige Sicherheitsinfrastruktur bildet. Cyberkriminelle suchen ständig nach Möglichkeiten, an kritische Daten zu gelangen. Ein gut durchdachtes Key Management ist eine wirksame Verteidigungslinie. Sicheres Key Management trägt dazu bei, die Integrität, Vertraulichkeit und Verfügbarkeit von Daten zu gewährleisten, was für Organisationen in einer zunehmend vernetzten und digitalisierten Welt von entscheidender Bedeutung ist. Aus diesem Grund wird Schlüsselmanagement gerne durch Hardware Security Module (HSMs) bereitgestellt, welche aufgrund ihrer speziellen physischen Sicherheit wie Tresore fungieren. Die Sicherheitsannahme ist, dass die Schlüssel geheim bleiben, auch wenn der Software-Stack korrumpiert wurde.

HSMs sind nicht ideal für gemanagte Infrastrukturen wie die Cloud, da ihre physische Natur und traditionelle Implementierung auf On-Premises-Bereitstellungen ausgerichtet sind. Man kann nicht seine eigene “Box” in ein von Dritten gemanagtes Rechenzentrum bringen.

Durch den Einsatz von Confidential Computing [1] besteht die Möglichkeit, das Key Management in einer Enklave zu betreiben. Eine Enklave fungiert dabei wie ein sicherer Tresor, der die Ausführung einer virtuellen Maschine ermöglicht, die während der Laufzeit im Speicher verschlüsselt bleibt. Diese Enklavierung wird mit Hilfe eines Security Prozessors (SP) auf der CPU realisiert, der einem "Mini"-HSM ähnelt. Alle modernen Server-CPUs von Intel [2], AMD [3] und ARM [4] sind standardmäßig mit einem solchen Security Prozessor ausgestattet. Da die Verschlüsselung direkt auf der CPU erfolgt, beträgt der Performance-Overhead lediglich 2-3% zusätzliche CPU-Zyklen (effektiv der Overhead einer optimierten AES-Verschlüsselung), was für Cloud-Anwendungen keinen nennenswerten Nachteil darstellt.

Unsere grundlegende Idee besteht darin, die Key Management Funktionen des Hardware Security Modules in einer Enklave zu virtualisieren. Anstatt auf kostspielige, dedizierte Hardware zu setzen, setzen wir auf Standard-Hardware, gängige Verschlüsselungsmethoden und übliche Virtualisierungstechniken. Anders ausgedrückt, reduzieren wir die Funktionen des HSMs auf die des Security Prozessors und kompensieren die verbleibende Funktionalität durch verschlüsselte Virtualisierung.

DER NUTZEN

Ein virtualisiertes Hardware Security Module (vHSM) bietet mehrere Vorteile gegenüber herkömmlichen, physischen HSMs, insbesondere in den dynamischen Umgebungen der Cloud und modernen Rechenzentren.

vHSMs können leicht in virtuellen Umgebungen bereitgestellt und skaliert werden. Im Gegensatz zu physischen HSMs ermöglicht die Virtualisierung eine flexible Anpassung an die Anforderungen, sodass Ressourcen je nach Bedarf hinzugefügt oder entfernt werden können.

Virtualisierte Lösungen reduzieren die Notwendigkeit teurer physischer Hardware und ermöglichen eine effizientere Nutzung von Ressourcen. Durch die Möglichkeit, virtuelle HSM-Instanzen zu erstellen, können Unternehmen Kosten sparen und ihre Sicherheitsinfrastruktur optimieren.

vHSMs ermöglichen eine schnelle Bereitstellung im Vergleich zu physischen HSMs. Dies ist besonders wichtig in Cloud-Umgebungen, in denen die Agilität und die Fähigkeit, schnell auf sich ändernde Anforderungen zu reagieren, entscheidend sind.

Virtualisierte HSMs lassen sich nahtlos in virtualisierte IT-Infrastrukturen und Cloud-Plattformen integrieren. Diese Integration erleichtert die Implementierung von Sicherheitslösungen und gewährleistet die Interoperabilität mit anderen virtuellen Ressourcen (z.B. Kubernetes Cluster).

vHSMs ermöglichen die dynamische Anpassung an sich ändernde Anforderungen und Lastspitzen. Durch die Virtualisierung können Unternehmen ihre Sicherheitsinfrastruktur effizienter anpassen, ohne auf starre physische Strukturen angewiesen zu sein.

Virtualisierte HSMs können zentralisiert verwaltet werden, was die Verwaltung und Überwachung von Sicherheitsrichtlinien erleichtert. Dies führt zu einer effizienteren Verwaltung und stärkt die Sicherheitspostur der Organisation.

Virtualisierte HSMs bieten den Vorteil der Kryptoagilität, da algorithmische Änderungen gemäß BSI/NIST-Standards durch einfache Software-Updates umgesetzt werden können, ohne dass ein Austausch der physischen Hardware erforderlich ist. Dies ermöglicht eine kosteneffiziente Anpassung an aktuelle Sicherheitsstandards und erhöht die Agilität der Sicherheitsinfrastruktur in einer sich ständig weiterentwickelnden Bedrohungslandschaft.

DIE (GRUNDZÜGE DER) UMSETZUNG

Die Herausforderung, die physischen Vertrauenseigenschaften des Hardware Security Modules (HSMs) durch Verschlüsselung abzubilden, gestaltet sich aufgrund der eingeschränkten Funktionen des Secure Processors (SP) und der flexiblen Anforderungen virtualisierter Infrastrukturen als äußerst anspruchsvoll. Unser vorrangiges Ziel bestand darin, unsere Key Management Applikation Vault zu virtualisieren, um sicherzustellen, dass die Anwendung während der Ausführung verschlüsselt ist und ausschließlich von der CPU (unter Verwendung des SP) ausgeführt werden kann.

Um dieses Ziel im Einklang mit den definierten Anforderungen zu erreichen, haben wir uns von innovativen Techniken der IT-Sicherheits-Grundlagenforschung inspirieren lassen. Hierbei setzen wir auf eine umfassende Strategie, die Memory Encryption, Disk Encryption und sichere TLS-Kommunikation kombiniert. Zudem integrieren wir eine neuartige Confidential Boot Technik, die zwar dem Trusted Boot ähnelt, jedoch nicht auf einem Trusted Platform Module (TPM) basiert, sondern auf dem Secure Processor verankert ist. Dieser Ansatz gewährleistet die Integrität der Trusted Code Base innerhalb der verschlüsselten virtuellen Maschine.

In Abbildung 1 ist eine Architektur mit den grundlegenden Komponenten dargestellt. Wir haben eine UEFI-Firmware (FW-CB) entwickelt, die die Fähigkeit zum Confidential Boot besitzt, sowie einen Linux-Kernel, der die persistente Festplattenverschlüsselung durch den Secure Processor (SP) durchführt (Kernel mit Disc Encryption Layer).

Die Ausführung des virtualisierten Hardware Security Modules (vHSM) erfolgt gemäß folgender Schritte: (1a) Der SP allokiert einen speziellen, "enklavierten" Speicherbereich, von dem die CPU weiß, dass er verschlüsselt ist und nur mithilfe des SPs ausgeführt werden kann. Der SP generiert einen einmaligen AES-Schlüssel für die Verschlüsselung dieses Speicherbereichs, der außerhalb der CPU nicht zugänglich ist. In dieser Enklave wird die virtuelle Maschine ausgeführt. Als erster Die Ausführung des virtualisierten Hardware Security Modules (vHSM) erfolgt gemäß folgender Schritte: (1a) Der SP allokiert einen speziellen, "enklavierten" Speicherbereich, von dem die CPU weiß, dass er verschlüsselt ist und nur mithilfe des SPs ausgeführt werden kann. Der SP generiert einen einmaligen AES-Schlüssel für die Verschlüsselung dieses Speicherbereichs, der außerhalb der CPU nicht zugänglich ist. In dieser Enklave wird die virtuelle Maschine ausgeführt. Als erster Schritt wird FW-CB in die Enklave geladen, wobei der SP die Firmware attestiert und somit die Integrität des folgenden Confidential Boot Prozesses sicherstellt. (1b)

Als zweiter Schritt wird der modifizierte Kernel in den enklavierten Speicherbereich geladen, nachdem die Authentizität des Kernel-Binary vom FW-CB überprüft wurde. (2a) Aufgrund der erfolgreichen Attestierung leitet der SP einen an die Plattform gebundenen "Sealing Key" ab. (2b) Mit Hilfe dieses Sealing Keys wird die persistente Speicherung entschlüsselt. Auf diese Weise kann die Vault-Applikation in die Enklave geladen, durch den Disk Encryption Layer entschlüsselt und in der enklavierten Umgebung ausgeführt werden. Dies umfasst nicht nur den Applikationscode, sondern auch die Geheimnisse des Vaults. Modifikationen am Applikationscode werden während der Entschlüsselung durch das sicher gegen Chosen Ciphertext Attack geschützte AES-GCM-Verfahren erkannt. (2c) Neue Geheimnisse werden persistent mit Hilfe des Sealing Keys verschlüsselt.

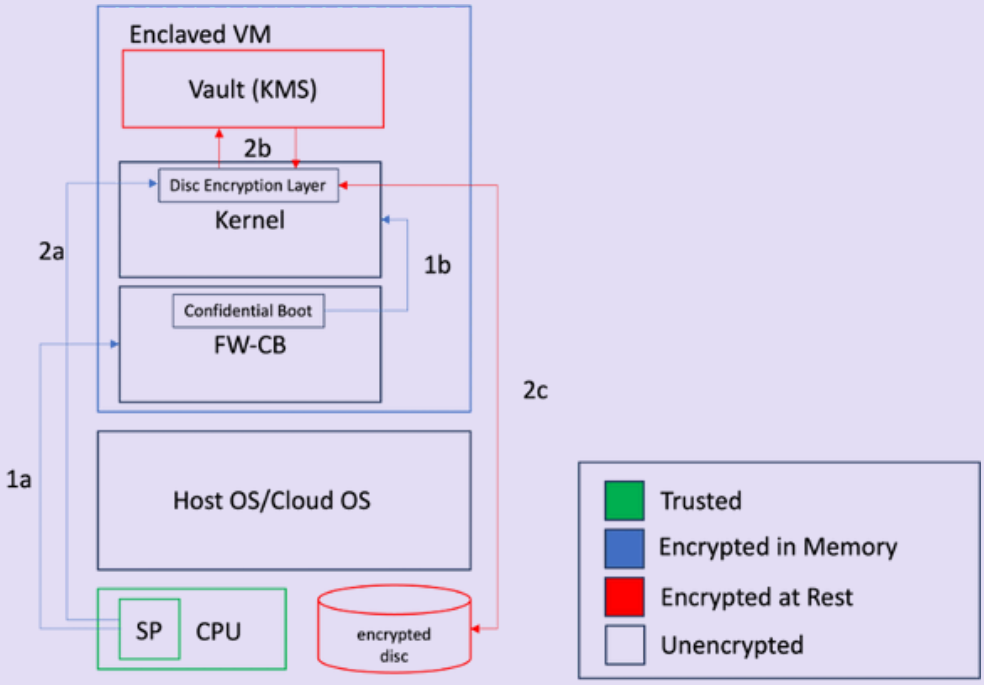


Abbildung 1: vHSM Architektur (vereinfacht)

Anmerkung: In der Cloud-Umgebung wird der Aspekt der Live-Migration von virtuellen Maschinen sowohl für Ausfallsicherheit als auch für Hochverfügbarkeit als äußerst bedeutend erachtet. Die Live-Migration von VMs wird durch den Einsatz des Secure Processors ermöglicht, während die Hochverfügbarkeit durch redundante Spiegelungen der Vault-Applikation gewährleistet wird. Aufgrund von Platzbeschränkungen werden hier keine detaillierten Informationen bereitgestellt.

VERWANDTE PRODUKTE

In Europa gibt es mehrere traditionelle HSM-Hersteller und Produkte. Bekannte Namen sind Utimaco HSM [5] aus Deutschland (gegründet von Dr. Horst Görtz), Thales Luna [6] und Eviden Trustway [7] aus Frankreich. Diese HSM-Produkte wurden traditionell für On-Premise-Umgebungen entwickelt und existieren in verschiedenen Varianten, von USB-Sticks über Netzwerkkarten bis hin zu PCI-Steckkarten. In jüngster Zeit bieten die Hersteller auch Cloud-HSMs an, sodass Kunden ein gemanagtes HSM in einem Rechenzentrum erhalten können.

Die Hyperscaler wie Azure [8], AWS [9], Google [10] und andere Cloud-Anbieter stellen ebenfalls dedizierte HSMs in ihren Rechenzentren bereit. Alternativ bieten sie auch softwarebasierte Key Management Lösungen an, darunter Azure Vault [11], AWS KMS [12], Google Secret Key Management [13] und HashiCorp Vault [14]. Obwohl diese gemanagten Software-basierten Key Management Lösungen kostengünstiger sind als HSMs, sollten sie kritisch betrachtet werden. Die Schlüssel sind dem Cloud-Anbieter zugänglich, da die Verschlüsselung nur für die persistente Speicherung und Kommunikation eingesetzt wird. Allerdings bleiben die Schlüssel im Speicher unverschlüsselt. Diese Schwachstelle führte kürzlich bei Azure zu Problemen, als der Master-Key für das Active Directory durchgesickerte [15].

Im Zusammenhang mit Virtualisierung hat sich das Konzept virtueller Trusted Platform Modules (vTPMs) etabliert [16], die in Software die Funktionalität eines physischen TPMs emulieren. Auch hier ist die Sicherheit kritisch zu hinterfragen, da die Kernfunktionalität des vTPMs nicht in Hardware verankert ist, sondern vom Cloud Provider emuliert wird.

DIE WIRTSCHAFTLICHEN AUSSICHTEN

Die Zielgruppe für virtuelle Hardware Security Modules umfasst Unternehmen verschiedener Größen und Branchen, die ihre digitalen Assets in Cloud- und virtualisierten Umgebungen schützen müssen. Große Unternehmen, insbesondere solche mit komplexen IT-Infrastrukturen und umfangreichen Cloud-Implementierungen, profitieren von der Flexibilität und Skalierbarkeit virtueller HSMs, die es ihnen ermöglichen, schnell auf sich ändernde Sicherheitsanforderungen zu reagieren. Kleinere Unternehmen und Start-ups, die möglicherweise begrenzte Ressourcen für physische Hardwareinvestitionen haben, können ebenfalls von vHSMs profitieren. Die Kosteneffizienz und die Möglichkeit, Sicherheitsfunktionen bedarfsgerecht zu skalieren, machen virtuelle HSMs attraktiv. Branchen mit strengen Sicherheitsvorschriften und Compliance-Anforderungen, wie Finanzdienstleistungen, Gesundheitswesen und Regierungen, könnten vHSMs nutzen, um sicherzustellen, dass ihre kritischen Daten gemäß den höchsten Sicherheitsstandards geschützt sind.
In Bezug auf die Größe des Zielmarktes ist dieser beträchtlich, da die Digitalisierung in nahezu allen Branchen voranschreitet und die Verlagerung zu Cloud- und virtualisierten Umgebungen zunimmt. Der Markt für vHSMs könnte daher sowohl Großunternehmen als auch kleinere und mittlere Unternehmen ansprechen, die ihre Sicherheitsinfrastruktur modernisieren und an die Anforderungen der digitalen Ära anpassen möchten. Die genaue Größe des Marktes hängt von Faktoren wie der Akzeptanz virtualisierter Sicherheitslösungen, der Fortschritte in der Cloud-Adoption und der Sensibilität gegenüber Datenschutz- und Sicherheitsfragen ab.

Auf Grundlage der Vermarktungsstrategie, die sich auf die beiden Kernmärkte sowie den öffentlichen Dienst konzentriert (siehe “Die Vermittlungsstrategie"), lässt sich eine finanzielle Prognose für die kommenden 12 Quartale nach der aktiven Vermarktung des vHSM-Produkts gemäß Abbildung 2 ableiten. Der Listenpreis des Produkts beträgt 699,- Euro pro Monat (zzgl. USt), wobei wir davon ausgehen, dass im Durchschnitt ein Rabatt von 25% über alle Kunden gewährt werden muss.

	Quartal											
Kundengruppe	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12
Security Hersteller		2	4	10	15	20	25	35	20	25	30	40
MSCs/CSPs	2	5	10	20	25	30	40	50	50	50	50	50
Public Sector			2	2	2	2	10	10	20	20	30	30
Weitere Expansion							2	2	5	10	10	25
Umsatzprognose	1.573 €	8.650 €	26.737 €	64.483 €	122.675 €	196.594 €	298.036 €	434.865 €	585.849 €	743.124 €	920.059 €	1.128.448 €

Abbildung 2: Prognose von Einnahmen

DIE NUTZBARKEIT

Das vHSM wird über eine REST-API, eine CLI als auch über ein Web-Interface bereitgestellt. Um die Gebrauchstauglichkeit zu verdeutlichen, haben wir einen Testzugang zum Web-Interface unter https://vhsm.enclaive.cloud konfiguriert.

Username: hgi
Password: ksla78&=KJLfd349JKnkgi

DIE VERMARKTUNGSSTRATEGIE

Marktsondierungsgespräche im Eintrittsmarkt DACH haben ein weitreichendes Interesse in zahlreichen Industrien und Anwendungsfällen offenbart. In drei spezifischen Bereichen hat sich dieses Interesse besonders deutlich gezeigt. Der Hauptfokus der Vermarktung richtet sich somit auf:

1. Unternehmen der IT-Security: Insbesondere solche, die mit ihren gegenwärtigen HSM-basierten Produkten den Weg in die Cloud eingeschlagen haben.
2. Managed und Cloud Service Provider: Hier liegt der Schwerpunkt auf Anbietern, die ihre Kunden auf dem Weg in eine (Hybride-)Multi-Cloud begleiten und dabei die Abstraktion der Infrastruktur nutzen, um wirtschaftlichere Angebote zu realisieren.
3. Öffentlicher Dienst: Insbesondere Organisationen, die im Rahmen der Digitalisierung die Sicherheitsauflagen des Bundesamts für Sicherheit in der Informationstechnik (BSI) einhalten müssen, wie beispielsweise den Schutz von Verschlusssachen - Nur für den Dienstgebrauch (VS-NfD) und den C5-Katalog.

Im Hinblick auf den Markteintritt liegt unser geografischer Fokus auf Zentraleuropa, wobei wir auf die Unterstützung von Industrieverbänden wie beispielsweise Teletrust und dem ECO-Verband setzen. Um den Vertriebserfolg insbesondere im Bereich der Serviceprovider (Kategorie 2) zu beschleunigen, streben wir eine enge Kooperation mit Distributoren an. Durch diese Zusammenarbeit intensivieren wir unseren Marktzugang und schaffen Integrationspartner, die nicht nur den direkten Kundenzugang ermöglichen, sondern darüber hinaus Projekte mit kompetentem Personal begleiten, um sämtliche Fragen und Herausforderungen neben dem eigentlichen Produkt zu bewältigen. Auf diese Weise steigern wir die langfristige Kundenzufriedenheit und verbessern die Marktadaption.

LITERATURVERZEICHNIS

[1] https://docs.enclaive.cloud/confidential-cloud/overview
[2] https://www.intel.com/content/www/us/en/developer/tools/trust-domain-extensions/overview.html
[3] https://www.amd.com/en/developer/sev.html
[4] https://www.arm.com/architecture/security-features/arm-confidential-compute-architecture
[5] https://utimaco.com/products/categories/hardware-security-modules-hsm
[6] https://cpl.thalesgroup.com/encryption/hardware-security-modules
[7] https://eviden.com/solutions/digital-security/data-encryption/
[8] https://azure.microsoft.com/en-us/products/azure-dedicated-hsm
[9] https://aws.amazon.com/cloudhsm/
[10] https://cloud.google.com/kms/docs/hsm
[11] https://azure.microsoft.com/en-us/products/key-vault
[12] https://aws.amazon.com/kms/
[13] https://cloud.google.com/security/products/security-key-management
[14] https://www.vaultproject.io
[15] https://www.heise.de/hintergrund/Gestohlener-Master-Key-Der-kleingeredete-GAU-der-Microsoft-Cloud-9234601.html
[16] https://trustedcomputinggroup.org/about/what-is-a-virtual-trusted-platform-module-vtpm

Über enclaive

enclaive enables businesses to securely protect their sensitive data and applications in untrusted cloud environments by leveraging the use of Confidential Computing. Its comprehensive, multi-cloud operating system allows for Zero Trust security by encrypting data in use and shielding applications from both the infrastructure and solution providers. With enclaive, businesses can confidently build, test, and deploy a wide range of cloud applications, all while maintaining complete control over their confidential information. enclaive's goal is to provide a universal, cloud-independent technology for enclaving sophisticated multi-cloud applications, that can be deployed with confidence and ease.

Kontaktinfos

github.com/enclaive

linkedin.com/company/enclaive

https://enclaive.io

youtube.com/@confidentialcompute

KONTAKT

contact@enclaive.io
+49 30233292973
Chausseestr. 40, 10115 Berlin, Germany
www.enclaive.io