enclaive

Solution Brief

Confidential Computing als Business-Enabler im Public Sector

Wie Systemintegratoren und MSPs Betreiberausschluss und Datenhoheit technisch umsetzen – und so neue Marktpotenziale erschließen

enclaive

Executive Summary

Die Digitalisierung der Verwaltung bietet Systemintegratoren und Managed Service Providern eine Vielzahl an Business Opportunities – wenn sie das hohe Sicherheitsniveau erfüllen können. Konkret bedeutet dies: Sie müssen hochsensible Fachverfahren in moderne Cloud-Architekturen überführen, ohne die strengen Anforderungen an den Datenschutz und die staatliche Souveränität zu verletzen. Herkömmliche Sicherheitskonzepte stoßen hier an ihre Grenzen, da sie Daten während der Verarbeitung ungeschützt lassen und den notwendigen Betreiberausschluss oft nur organisatorisch, aber nicht technisch garantieren können.

Confidential Computing löst dieses Problem und verschlüsselt Daten „At Rest“, „In Transit“ und auch „In Use“. Durch den Einsatz hardwarebasierter, isolierter Ausführungsumgebungen stellt die Technologie sicher, dass weder Infrastruktur-Provider noch Administratoren Zugriff auf die verarbeiteten Daten haben. Für IT-Dienstleister wird die Datensouveränität ihrer Kunden nachweisbar, was das Vertrauen öffentlicher Stellen stärkt und Genehmigungsprozesse massiv beschleunigt.

Das Projekt „Register-as-a-Service“ (RaaS) von GovTech Deutschland und der FITKO dient in diesem Solution Brief als Praxisbeispiel dafür, wie sich komplexe Fachverfahren (z. B. Gewerberegister) rechtssicher und hochperformant in der Cloud schützen lassen. Die Lösung des Sieger-Konsortiums unter Beteiligung von enclaive wurde dabei als besonders tragfähig bewertet und dient nun als offene Referenzimplementierung für die bundesweite Modernisierung.

Systemintegratoren und Managed Service Provider erfahren anhand dieser Case Study, wie eine Confidential-Computing-Architektur in der Praxis aussieht, welche Komponenten zum Einsatz kommen und welche Vorteile sich ihnen sowohl technisch als auch wirtschaftlich bieten.

enclaive

Gartner zählt Confidential Computing zu den

Top 10 Strategic Technology Trends 2026

~50 %

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

Lediglich

2-3 %

zusätzliche Rechenleistung für 3D-Verschlüsselung

enclaive

Warum Sicherheit im Public Sector neue Wege gehen muss

Systemintegratoren und MSPs sind für die Digitalisierung der deutschen Verwaltung unverzichtbar. In einem Umfeld, das durch das Onlinezugangsgesetz (OZG) unter massivem Innovationsdruck steht, übersetzen Sie komplexe Fachverfahren in moderne Architekturen.

Doch während die technologische Skalierbarkeit nach Cloud-nativen Ansätzen verlangt, haben Behörden und der Gesetzgeber höchste Ansprüche an die Datensouveränität. IT-Dienstleister stehen bei der Projektumsetzung im öffentlichen Sektor oft vor drei kritischen Herausforderungen, die den Projekterfolg verzögern oder gar gefährden können:

- **Die Vertrauensbarriere (Betreiberausschluss):** In der Public Cloud oder bei Managed Services bleibt oft ein Restrisiko. Der Infrastruktur-Provider oder Administrator hat theoretisch Zugriff auf die Daten im Arbeitsspeicher. Dieser fehlende technische Betreiberausschluss ist oft der „Showstopper“ im Genehmigungsprozess.
- **Der Compliance-Flaschenhals:** Umsetzungspartner stehen durch die strengen Anforderungen von BSI-Grundschutz und DSGVO unter Druck, „Security by Design“ nicht nur zu versprechen, sondern für hochsensible Daten zweifelsfrei nachzuweisen.
- **Digitale Souveränität vs. Skalierung:** Der öffentliche Sektor fordert volle Kontrolle über Daten und Code. Klassische Sicherheitskonzepte (Verschlüsselung bei Speicherung/Übertragung) erzwingen hier oft einen Rückzug in teure, unflexible On-Premises-Silos.

Confidential Computing als Enabler für sichere Stacks

Im Gegensatz zur herkömmlichen Verschlüsselung schützt Confidential Computing Daten auch während der Verarbeitung (Data In Use). Durch hardwarebasierte, isolierte Trusted Execution Environments („Enklaven“) wird sichergestellt, dass weder der Infrastruktur-Betreiber noch privilegierte Administratoren Einblick in die Workloads erhalten.

Als IT-Dienstleister bauen Sie Ihre Applikations-Stacks so auf einem Fundament auf, das „Security by Design“ auf Chiplevel realisiert. Vertrauen wird durch eine kryptografisch prüfbare Attestierung ersetzt. Damit entkoppeln Sie Datensicherheit von der Cloud-Infrastruktur – die Voraussetzung für digitale Souveränität und die Umsetzung öffentlicher Cloud-Projekte.

Wie dieser Ansatz in der Praxis eine der komplexesten Aufgaben der aktuellen Verwaltungsdigitalisierung löst, zeigt unser Referenzprojekt im Bereich der Registermodernisierung.

Von offizieller Seite anerkannt

Das BSI empfiehlt Confidential Computing im aktuellen C5-Katalog ausdrücklich für hochsensible Cloud-Workloads. Auch die gematik sieht es als wichtigen Technologiebaustein für sichere Cloud-Umgebungen. Die Technologie setzt außerdem konsequent die im Deutschland-Stack enthaltenen Grundprinzipien und konkreten Verschlüsselungsalgorithmen um.

enclaive

Case Study: RaaS als Reifeprüfung

Im Rahmen des Bundeswettbewerbs „Register-as-a-Service“ (RaaS) von GovTech Deutschland und der FITKO hat enclaive gemeinsam mit Polyteia, Naviga, der DigitalAgentur Brandenburg und dem Amt Scharmützelsee eine wegweisende Referenzarchitektur für moderne Cloud-Register realisiert. Die Lösung überzeugte als besonders tragfähiger Ansatz und wird nun als offene Referenzimplementierung weitergeführt, um als stabiler OS-Baustein die bundesweite Registermodernisierung zu beschleunigen.

Für die Partner fungierte Confidential Computing als vertrauenswürdiges Fundament, das komplexe Sicherheitsfragen bereits auf Architekturebene beantwortete. Unsere Enklaven auf Basis von Open Source und standardisierten APIs (PKCS#11, KMIP, REST) reduzierten zudem den Integrationsaufwand, sodass sich unsere Partner auf die Abbildung der Gewerbe- und Melderegisterlogik konzentrieren konnten. Das Ergebnis: Eine vollständig Compliance-konforme und hochperformante Fachanwendung, die ohne Sicherheits-Trade-offs direkt in der Cloud skalieren kann – und von Projektbeginn bis Praxisbetrieb nur wenige Monate benötigte.

Architektur des Confidential Kubernetes-as-a-Service

Konkret implementierten wir einen Kubernetes-Cluster mit Kata-Containern, um hardwarebasierte Isolation auf Pod-Ebene zu erreichen. Im Gegensatz zu standardmäßigen Linux-Namespaces wird dabei jeder Pod in seiner eigenen leichtgewichtigen VM (enclaive Buckypaper) mit dediziertem Kernel von der registerführenden Stelle/Kommune ausgeführt. Für jeden Pod richteten wir individuelle Attestation-Mechanismen ein (enclaive Nitride), die die kryptographische Verifikation der Pod-Integrität ermöglichen. Darüber hinaus implementierten wir eine isolierte Schlüsselverwaltung (enclaive Vault), sodass kompromittierte Pods keine Auswirkungen auf andere Workloads haben.

Der gesamte Cluster (enclaive Dyneemes) wurde mit durchgängiger Verschlüsselung konfiguriert:

- „In Transit“ für alle Netzwerkverbindungen zwischen Pods, Nodes und der Kubernetes-API (Control Plane),
- „At Rest“ für persistente Daten in etcd und den Storage-Volumes, sowie
- „In Use“ durch Confidential-Computing-Technologien (AWS EC2 m6a Instanzen auf AMD EPYC Prozessoren), um die Daten selbst während der Verarbeitung im Speicher schützen.

Remote Attestation

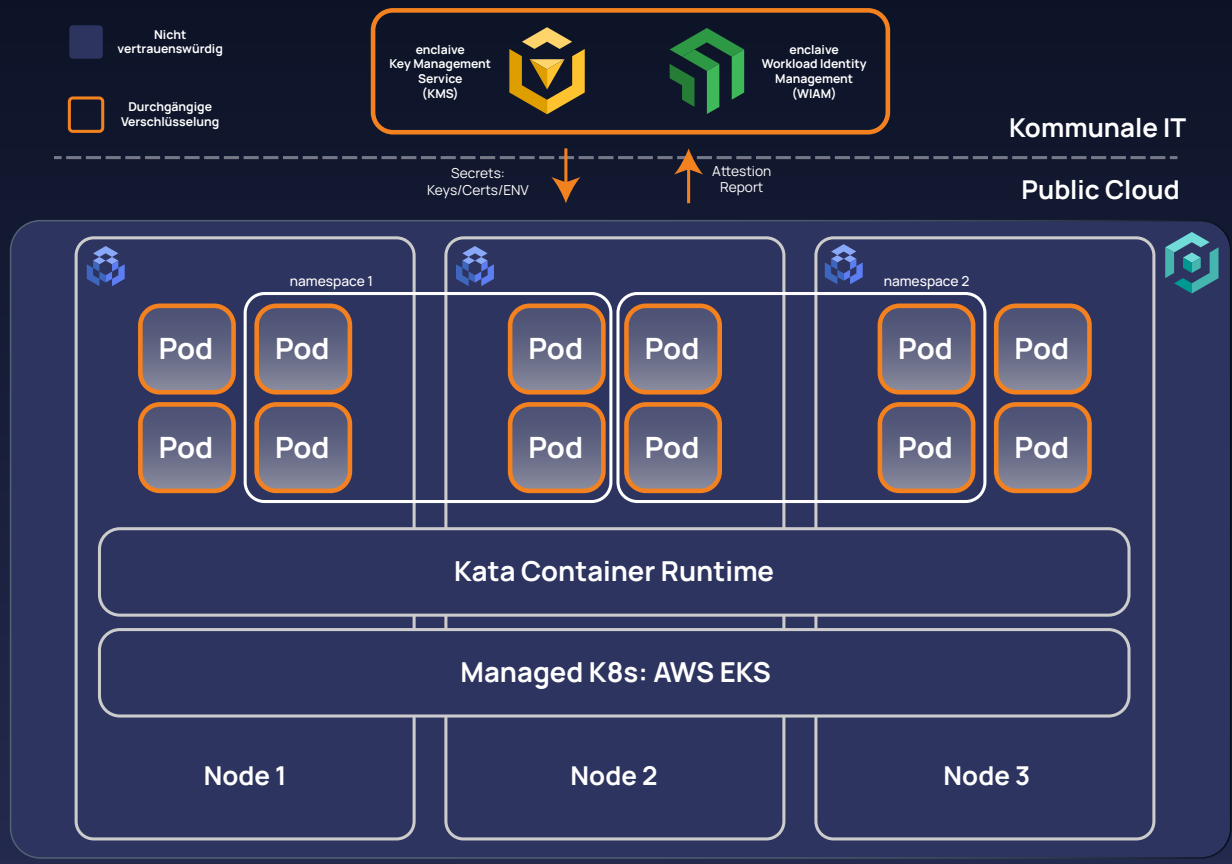
Bevor Workloads in einer Enklave starten, muss sichergestellt sein, dass diese vertrauenswürdig und unverändert ist. Hier kommt Remote Attestation ins Spiel, die genau dies durch ein kryptografisch gesichertes Zertifikat der Hardware- und Software-Integrität gewährleistet. Für Compliance und Audits ist das ein echter Gamechanger: Die Attestation liefert den technischen Beweis, dass die Datenverarbeitung in einer geschützten Umgebung stattfindet.

enclaive

Der Kerngedanke der Architektur ist, Pods zu enklavieren, indem sie nicht als normale Container im Host-Kernel laufen, sondern in confidential VMs (podCVM).

Der Kubernetes-Operator (z. B. AWS EKS Operator mit vollen Control-Plane-Rechten) behält die Kontrolle über VMs/ Instanzen, hat aber keinen Zugriff auf die verschlüsselten Inhalte in den podCVMs, weil Keys, Attestation und Secrets außerhalb von AWS (On-Prem Key and Workload Identity Management) verwaltet werden.

Eine Kata Security Policy verhindert die Ausführung kritischer administrativer Kommandos der KubeAPI (z. B. kubectl exec) im Pod.



enclaive

Komponenten

- **AWS EKS (gemanagt):** Bietet Control Plane und Kubernetes API; Operator hat volle API-/ Betriebsrechte.
- **Kata Operator:** Startet Pods nicht als normale Container, sondern als podCVMs (confidential VMs).
- **podCVM (confidential VM):** Jede Pod-Workload läuft in einer separaten EC2 VM mit AMD SEV-SNP Support.
- **Guest OS „Buckypaper“:** Von enclaive modifiziertes, Kata-Container-fähiges Linux als Guest OS innerhalb der podCVM.
- **CloudAPI Connector / cloud-remote runtime:** Vom Operator installiert; podCVMs mit aktivierter Data-In-Use-Encryption werden über die AWS Cloud API (EC2) gestartet.
- **CSI-Driver (enclaive):** Von enclaive entwickelter AWS-EBS-Treiber, der das Block Device mit einem Schlüssel aus einem externen Key Management verschlüsselt; Disk-Keys stammen nicht aus dem AWS-KMS, was der Standard bei AWS EKS ist.
- **CNI-Driver (verschlüsseltes Mesh):** Stellt ein verschlüsseltes Netzwerk zwischen Pods und zu den Pods her (Ende-zu-Ende-Verschlüsselung der Data In Transit).
- **Sidecar (Attestation & Secrets Provisioning):** Führt Remote-Attestation der podCVM gegenüber einem externen On-Prem Workload Identity + Key Management Service durch (kommunale IT). Provisioniert die benötigten Secrets (z. B. Decryption-Key für verschlüsselte Laufwerke).

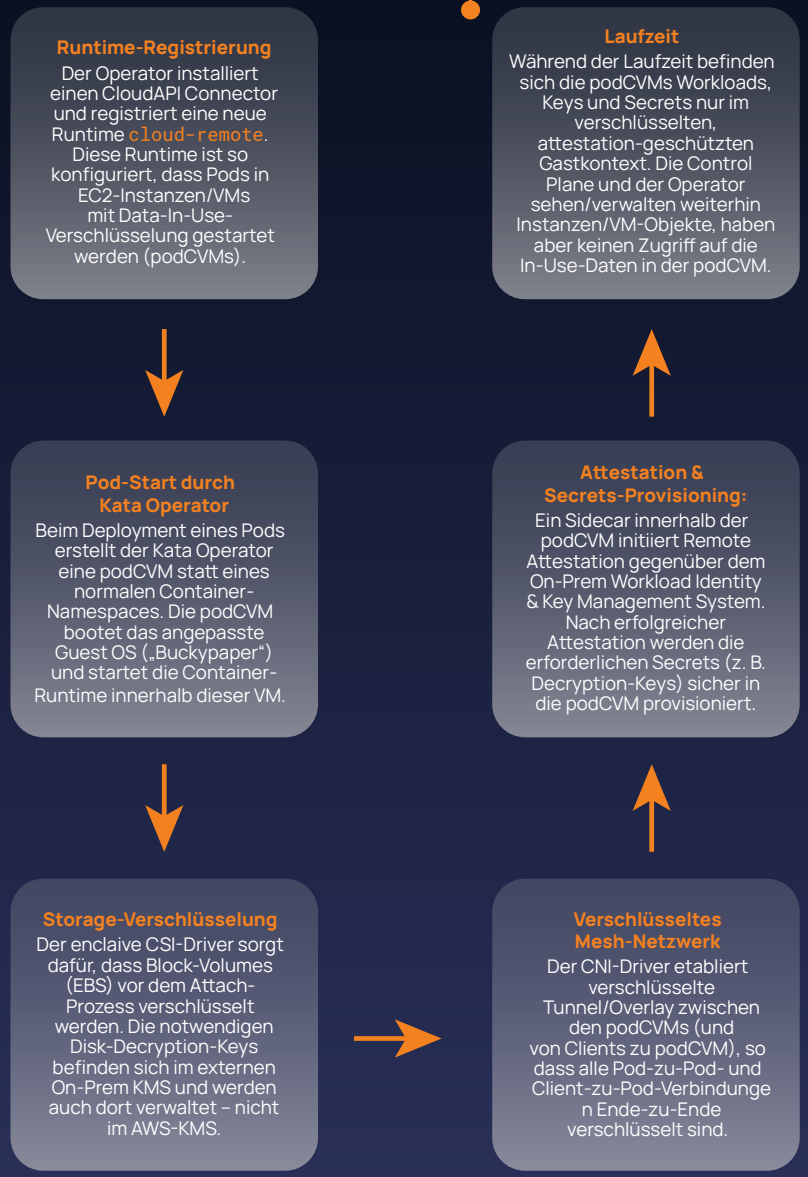


Abb.: Detaillierter technischer Ablauf (Flow)

enclaive

Vorteile dieser Kubernetes-Architektur

Keys außerhalb des Cloud-Providers (keine AWS-KMS-Abhängigkeit)

Disk- und Decryption-Keys werden von einem externen On-Prem-KMS ausgegeben und bleiben dort unter Kontrolle der kommunalen IT. Selbst bei vollständigem Zugriff auf die Cloud-Management-Ebene kann der Provider die Keys nicht auslesen und die Laufwerke nicht entschlüsseln.

Verschlüsselung von Disk und Netzwerk = Defense in Depth

Storage ist mit externen Keys verschlüsselt (Data At Rest). Netzwerkverkehr zu und zwischen Pods ist Ende-zu-Ende verschlüsselt (Data In Transit). Zusammen mit Data In Use in der podCVM ergibt das eine lückenlose Vertraulichkeitskette.

Remote Attestation als Vertrauensanker

Die On-Prem-Instanz (Workload Identity Service) provisioniert Secrets nur nach erfolgreicher Attestation. Damit wird sichergestellt, dass nur authentische, unveränderte podCVMs Zugriff auf Keys/ Secrets erhalten – und nicht etwa manipulierte Instanzen oder Snapshots.

Data-In-Use-Verschlüsselung verhindert Einsicht durch Provider/Operator

In einem normalen EKS kann ein privilegierter Operator durch Node-Level Tools, Kernel-Namespaces oder privilegierte Daemons auf Container-Dateisysteme, Prozesse und Speicher zugreifen. Durch podCVMs ist der Anwendungs-Kontext dagegen in einer VM isoliert. Der Provider-Admin hat zwar Kontrolle über die VM-Instanz als Ressource, aber nicht über die im Gast gehaltenen Geheimnisse/ Daten, da Keys nicht im Cloud-KMS liegen.

Granulare Minimierung der Trusted Computing Base (TCB)

Die TCB-Fläche wird reduziert: statt dem gesamten Cloud-Stack ist nur die podCVM-TCB (Buckypaper, Attestation, Sidecar) als kritisch anzusehen – alles andere (AWS Control Plane) ist untrusted-but-honored (kann also den VM-Lifecycle managen, aber nicht die Daten einsehen).

Schutz gegen Insider beim Cloud-Provider

Administrative Aktionen des Providers (z. B. Live-Migration, Snapshot, Host-Level-Debugging) reichen nicht aus, um die In-Use-Daten zu entschlüsseln oder Secret-Material zu lesen, weil das Schlüsselmaterial sich nicht in der Cloud befindet.

Bessere Compliance-Nachweise

Für datenschutzrechtlich sensible Daten (z. B. Registerdaten) kann der Nachweis geführt werden, dass Schlüsselverwaltung und Secret-Provisionierung im Verantwortungsbereich der kommunalen IT bleiben – relevant für DSGVO und lokale Auflagen.

enclaive

Zusammengefasst

Die Architektur realisiert einen lückenlosen Betreiberausschluss, auch in sensiblen Multi-Tenant-Umgebungen. Der Infrastruktur-Provider betreibt lediglich die Hardware und Kubernetes-Plattform (in diesem Fall Amazon Elastic Kubernetes Service oder EKS), der Anwendungs-Provider stellt die Applikation bereit, während die registerführende Stelle/Kommune als alleiniger Schlüssel- und Secrets-Inhaber die volle Kontrolle über ihre sensiblen Daten behält. Nur die registerführende Stelle/Kommune kann durch ihre kryptographischen Schlüssel auf die Daten zugreifen und diese entschlüsseln, was eine vertrauenswürdige Datenverarbeitung auch in extern betriebenen Umgebungen gewährleistet.

enclaive

Ihr strategischer Vorsprung mit enclaive

Die Implementierung von Confidential Computing ist mehr als ein technisches Upgrade – sie ist ein wirtschaftlicher Enabler für Projekte im öffentlichen Sektor. IT-Dienstleister, die enclaive in ihren Stack integrieren, profitieren von entscheidenden Vorteilen:

- **Beschleunigte Projektumsetzung:** Das größte Hindernis in GovTech-Projekten ist oft der Datenschutz. Mit enclaive lässt sich der Betreiberausschluss technisch nachweisen, wodurch sich komplexe Freigabeprozesse verkürzen.
- **Alleinstellungsmerkmal:** Mit dem RaaS-Wettbewerb hat sich Confidential Computing als neuer Standard empfohlen. Positionieren Sie sich hier als Innovationsführer und heben Sie sich in Ausschreibungen von anderen Anbietern ab.
- **Signifikante Risikoreduzierung:** Durch die technologische Trennung von Applikation und Infrastruktur minimieren Sie Ihr Haftungsrisiko, da selbst bei einer Kompromittierung des Host-Systems kein Zugriff auf die verarbeiteten Daten in der Enklave möglich ist.
- **Infrastruktur-Flexibilität gleich Kosteneffizienz:** enclaive bietet eine Abstraktionsschicht, die Ihren Software-Stack Infrastruktur-agnostisch macht. Basierend auf Open Source und standardisierten Schnittstellen lassen sich die Enklaven nahtlos in jede Umgebung implementieren. Heißt für Sie: Übertragbare Sicherheitsarchitekturen statt kostspieliger Neuentwicklungen für jeden Kunden.

Digitale Souveränität in der Cloud

Absolute Datenhoheit

Die Behörde bleibt alleiniger Inhaber der kryptografischen Schlüssel. Weder IT-Dienstleister noch Cloud-Provider können die Daten einsehen.

Sichere Mandantenfähigkeit

Die hardwarebasierte Trennung garantiert, dass Daten verschiedener Kommunen auf geteilten Plattformen absolut isoliert bleiben.

Technischer Betreiberausschluss

Zugriffsschutz basiert nicht auf Verträgen, sondern wird durch Hardware-Isolation erzwungen. Ein Zugriff durch Administratoren ist physikalisch ausgeschlossen.

Rechtssicherheit (DSGVO)

Die strikte technische Trennung von Infrastruktur und Datenverarbeitung vereinfacht Vorgaben wie die Datenschutz-Folgenabschätzung (DSFA) erheblich.

Zukunftssichere Interoperabilität

Vollständige Konformität mit föderalen Architektur-Vorgaben und nahtlose Integration dank Nutzung offener Standards.

enclaive

Werden Sie zum Souveränitäts-Garanten der öffentlichen Verwaltung

Profitieren Sie von unseren Erfahrungen aus der Registermodernisierung und sichern Sie sich Ihren Vorsprung im Public Sector. Lassen Sie uns gemeinsam evaluieren, wie Sie mit Confidential Computing neue Marktpotenziale erschließen und die digitale Souveränität Ihrer Kunden technisch garantieren können.

Bei enclaive begleiten wir IT-Dienstleister aktiv dabei, Confidential Computing in ihren Stack zu integrieren – und die Technologie anschließend effizient und rechtssicher in Endkunden-Umgebungen zu implementieren.

Wie enclaive Sie unterstützt:

- Workshops und Schulungen
- Aufbau einer Labor-/Testumgebung
- Co-Marketing und Co-Selling
- Support bei Ausschreibungen
- Attraktive Partner- und Preismodelle

Kontakt
sales@enclaive.io

Mehr Informationen unter
enclaive.io