enclaive

PUBLIC SECTOR

SOLUTION BRIEF

Confidential Computing as a Business Enabler in the Public Sector

How System Integrators and MSPs Deliver Operator Exclusion and Data Sovereignty – and Unlock New Market Opportunities

2–3%
ADDITIONAL OVERHEAD

~50%
MARKET CAGR

Top 10
GARTNER TREND 2026

Executive Summary

The digitalisation of public administration opens up significant business opportunities for system integrators and managed service providers – provided they can meet the sector‘s rigorous security requirements. In practice, this means migrating highly sensitive government applications into modern cloud architectures without compromising data protection obligations and federal or state sovereignty. This is where conventional security approaches fall short: they leave data unprotected during processing and can only guarantee the required operator exclusion through contractual agreements, not technical enforcement.

Confidential Computing closes this gap by encrypting data At Rest, In Transit, and, crucially, In Use. By utilising hardware-based, isolated Trusted Execution Environments (TEEs), this technology ensures that neither infrastructure providers nor administrators can access data while it is being processed. For IT service providers, this makes client data sovereignty verifiable, strengthening trust with public authorities and significantly accelerating approval processes.

The “Register-as-a-Service” (RaaS) project by GovTech Deutschland and FITKO serves as the practical reference case in this Solution Brief. It demonstrates how complex specialised registers (e.g., trade registries) can be protected in the cloud with high performance and legal certainty. The solution from the winning consortium, which included enclaive, was recognised as particularly robust and now serves as an open reference implementation to drive nationwide registry modernisation.

Through this case study, SIs and MSPs will learn what a Confidential Computing architecture looks like in practice, which components are used, and the technical and economic advantages it offers.

ONLY

2-3%

additional overhead for 3D Encryption

~50%

CAGR for the Confidential Computing market over the next 5 to 10 years

Top 10

Gartner ranks Confidential Computing among the Top 10 Strategic Technology Trends 2026

02 — THE PROBLEM

Why Public Sector Security Requires a New Approach

SIs and MSPs are essential for the digitalisation of the German public sector. In a sector under massive pressure to innovate due to the Online Access Act (OZG), they are the ones translating complex administrative procedures into modern architectures.

However, while scalability demands cloud-native approaches, government agencies and legislators have the highest expectations for data sovereignty. During project implementation in the public sector, IT service providers often face three critical challenges that can delay or jeopardise success:

The Trust Barrier (Operator Exclusion):

In public cloud or managed service environments, a residual risk always remains. Theoretically, the infrastructure provider or administrator has access to data in the RAM. This lack of technical operator exclusion is often the „showstopper“ in the approval process.

The Compliance Bottleneck:

Driven by the strict requirements of BSI Grundschutz and GDPR, implementation partners are under pressure to not just promise “Security by Design,” but to prove it beyond doubt for highly sensitive data.

Digital Sovereignty vs. Scaling:

The public sector demands full control over data and code. Traditional security concepts (encryption only for storage/transfer) often force organisations to fall back on expensive, inflexible on-premises silos.

Confidential Computing: The Enabler for Secure Stacks

Unlike traditional encryption, Confidential Computing protects data while it is being processed (Data In Use). Hardware-based, isolated Trusted Execution Environments (“enclaves”) ensure that neither infrastructure operators nor privileged administrators can gain insight into workloads.

As an IT service provider, you build your application stacks on a foundation that realises “Security by Design” at chip level. Trust is replaced by cryptographically verifiable Attestation. This decouples data security from the cloud infrastructure – the prerequisite for digital sovereignty and the successful implementation of public cloud projects.

Our project in registry modernisation demonstrates how this approach solves one of the most complex tasks in current administrative digitalisation.

RECOGNISED BY OFFICIAL BODIES

The BSI explicitly lists Confidential Computing in its current C5 catalog for highly sensitive cloud workloads. gematik also views it as a vital technological building block for secure cloud environments. Furthermore, the technology consistently implements the core principles and specific encryption algorithms defined in the “Deutschland-Stack.”

03 — CASE STUDY

Case Study: RaaS as a Proof of Concept

As part of the federal “Register-as-a-Service” (RaaS) competition hosted by GovTech Deutschland and FITKO, enclaive – together with Polyteia, Naviga, the DigitalAgentur Brandenburg, and the Amt Scharmützelsee – implemented a reference architecture for modern cloud-based registries. The solution was chosen as an exceptionally viable approach and is now being developed as an OS-based reference implementation to accelerate nationwide modernisation.

For the partners involved, Confidential Computing served as a trusted foundation that answered complex security questions at the architectural level. Our enclaves, based on open source and standardised APIs (PKCS#11, KMIP, REST), reduced integration efforts, allowing partners to focus on the business logic of trade and civil registries. The result: a fully compliant, high-performance application that scales in the cloud without security trade-offs – moving from project kickoff to live operation in just a few months.

REMOTE ATTESTATION

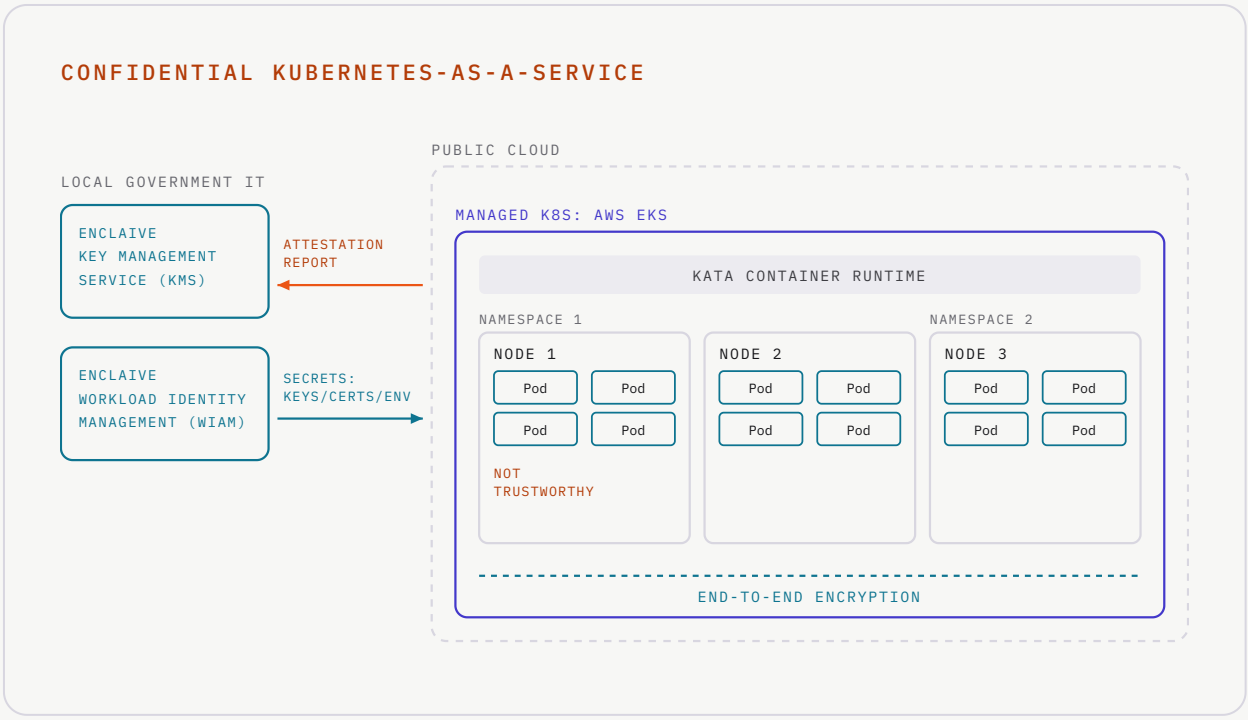
Before a workload launches inside an enclave, it must be verified that they are trusted and unaltered. This is where Remote Attestation comes in, providing a cryptographically secured certificate of hardware and software integrity. For compliance and audits, this is a gamechanger: Attestation provides technical proof that data processing occurs within a protected environment.

Architecture of the Confidential Kubernetes-as-a-Service

We implemented a Kubernetes cluster using Kata Containers to achieve hardware-based isolation at pod level. Unlike standard Linux namespaces, each pod runs in its own lightweight VM (enclaive Buckypaper) with a dedicated kernel, executed by the registry authority/municipality. For each pod, we established individual attestation mechanisms (enclaive Nitride) for cryptographic verification of pod integrity. Additionally, we implemented isolated key management (enclaive Vault) to ensure that compromised pods cannot affect other workloads.

The entire cluster (enclaive Dyneemes) was configured with end-to-end encryption:

- “In Transit” for all network connections between pods, nodes, and the Kubernetes API (Control Plane),
- “At Rest” for persistent data in etcd and storage volumes, and
- “In Use” via Confidential Computing technologies (AWS EC2 m6a instances on AMD EPYC processors) to protect data even during memory processing.



The core principle of the architecture is enclave-level pod isolation: rather than running as ordinary containers within the host kernel, pods execute inside Confidential VMs (podCVMs).

The Kubernetes operator (e.g., AWS EKS operator with full control plane privileges) retains control over VM instances but has no access to the encrypted contents of the podCVMs – because keys, attestation, and secrets are managed outside AWS via on-premises key and workload identity management.

A Kata Security Policy prevents the execution of critical administrative Kubernetes API commands (e.g., kubectl exec) inside the pod.

Komponenten

AWS EKS (Managed): Provides the Control Plane and Kubernetes API; the operator has full API/operational rights.

Kata Operator: Deploys pods as podCVMs (confidential VMs) rather than standard containers.

podCVM (Confidential VM): Each pod workload runs in a separate EC2 VM with AMD SEV-SNP support.

Guest OS "Buckypaper": An Kata-compatible Linux, modified by enclaive, acting as the Guest OS within the podCVM.

CloudAPI Connector / Cloud-remote Runtime: Installed by the operator; podCVMs with active Data-In-Use encryption are launched via the AWS Cloud API (EC2).

CSI-Driver (enclaive): An enclaive-developed AWS EBS driver that encrypts block devices using keys from external key management. Disk keys do not originate from AWS KMS (standard for AWS EKS).

CNI-Driver (Encrypted Mesh): Establishes an encrypted network between and to the pods (End-to-End encryption of Data In Transit).

Sidecar (Attestation & Secrets Provisioning): Performs Remote Attestation of the podCVM for an external On-Prem Workload Identity + Key Management Service (Local Government IT). It provisions the required secrets (e.g., decryption keys for encrypted drives).

Fig.: Detailed Technical Flow

01

Runtime Registration

The operator installs a CloudAPI Connector and registers a new cloud-remote runtime, configured to start pods in EC2 instances with Data-In-Use encryption (podCVMs).

02

Pod Start via Kata Operator

During deployment, the Kata Operator creates a podCVM instead of a standard container namespace. The podCVM boots the modified Guest OS ("Buckypaper") and starts the container runtime inside the VM.

03

Storage Encryption

The enclaive CSI-Driver ensures Block Volumes (EBS) are encrypted before attachment. The necessary disk decryption keys reside in the external On-Prem KMS – not AWS KMS.

04

Encrypted Mesh Network

The CNI-Driver establishes encrypted tunnels/overlays between podCVMs (and from clients to podCVMs), ensuring all traffic is end-to-end encrypted.

05

Attestation & Secrets Provisioning:

A sidecar within the podCVM initiates Remote Attestation with the On-Prem Workload Identity & Key Management system. Upon success, secrets (e.g., decryption keys) are securely provisioned into the podCVM.

06

Runtime

During operation, podCVM workloads, keys, and secrets exist only within the encrypted, attestation-protected guest context. The Control Plane manages instance objects but can‘t access In-Use data.

Key Benefits of this Kubernetes Architecture

Data-In-Use Encryption Prevents Provider/Operator Access

In a standard EKS, a privileged operator can access container filesystems, processes, and memory via node-level tools, kernel namespaces, or privileged daemons. With podCVMs, the application context is isolated inside a VM. The provider admin controls the VM instance as a resource but cannot access secrets or data held inside the guest, since keys are not stored in the cloud KMS.

External Key Management (No AWS KMS Dependency)

Disk and decryption keys are issued by an external on-premises KMS and remain under the control of the municipal IT department. Even with full access to the cloud management plane, the provider cannot read the keys or decrypt storage volumes.

Remote Attestation as a Trust Anchor

Secrets are only provisioned after successful attestation. This ensures that only authentic, unaltered podCVMs gain access to keys and secrets – while blocking manipulated instances or unauthorised snapshots.

Disk & Network Encryption = Defense in Depth

Storage is encrypted with external keys (At Rest). Network traffic is end-to-end encrypted (In Transit). Combined with Data In Use in the podCVM, this creates a continuous chain of confidentiality.

Protection Against Insider Threats from the Cloud Provider

Administrative actions by the provider (e.g., live migration, snapshots, host-level debugging) are insufficient to decrypt In-Use data or access secrets, because the keys are never held within the cloud environment.

Enhanced Compliance Reporting

For privacy-sensitive data such as registry records, you can provide technical proof that key management and secrets provisioning remain within the responsibility of the municipal IT department. This is crucial for GDPR and local regulations.

Granular Minimisation of the Trusted Computing Base (TCB)

The TCB surface is reduced: rather than the entire cloud stack, only the podCVM TCB (Buckypaper, attestation, sidecar) is considered critical. Everything else (AWS control plane) is treated as untrusted-but-honored: it can manage the VM lifecycle but cannot view the data.

In Summary

The architecture achieves complete operator exclusion, even in sensitive multi-tenant environments. The infrastructure provider operates the hardware and Kubernetes platform (here, Amazon Elastic Kubernetes Service / EKS); the application provider delivers the software, while the registry authority or municipality, as the sole holder of cryptographic keys and secrets, retains full control over its sensitive data. Only the registry authority can access and decrypt the data through its own cryptographic keys, ensuring trustworthy data processing even in externally operated environments.

06 — YOUR ADVANTAGE

Your Strategic Advantage with enclaive

Implementing Confidential Computing is more than a technical upgrade — it is an economic enabler for Public Sector projects. IT service providers integrating enclaive into their stack benefit from:

Accelerated Project Delivery:

Data protection is often the single biggest bottleneck in GovTech projects. With enclaive, operator exclusion is technically verifiable, shortening complex approval cycles.

Market Differentiation:

The RaaS project has established Confidential Computing as a new benchmark in public sector IT. Position yourself as an innovation leader and stand out in competitive tenders.

Significant Risk Reduction:

The technical separation of application and infrastructure substantially limits your liability exposure: even if the host system is compromised, data inside the enclave remains inaccessible.

Infrastructure Flexibility Equals Cost Efficiency:

enclaive provides an abstraction layer that makes your software stack infrastructure-agnostic. Built on open source and standardised APIs, our enclaves integrate seamlessly into any environment – meaning portable security architectures instead of expensive custom builds for every new client.

06 — YOUR ADVANTAGE

Digital Sovereignty in the Cloud

Full Data Control

The respective authority remains the sole holder of cryptographic keys. Neither the IT service provider nor the cloud provider can access the data.

Technical Operator Exclusion

Data protection is enforced by hardware, not just contracts. Access by providers is physically impossible.

Legal Certainty (GDPR)

The strict technical separation of infrastructure and data processing substantially simplifies obligations such as Data Protection Impact Assessments (DPIA).

Secure Multi-Tenancy

Hardware-based separation ensures data from different municipalities remains isolated on shared platforms.

Future-Proof Interoperability

Full compliance with federal architectural guidelines and seamless integration via open standards.

07 — PRICING

Buckypaper Preis und Discount Staffel

vCPUs = 20,-€ monatl.

VCPU STAFFEL A	1 – 99	Discount 5 %
VCPU STAFFEL B	100 – 249	Discount 15 %
VCPU STAFFEL C	250 – 499	Discount 25 %
VCPU STAFFEL D	500 – 999	Discount 35 %
VCPU STAFFEL E	>= 1000	Discount 40 %

Dyneemes Preis und Discount Staffel

Control Plane 100,-€ monatl.
vCPUs = 30,-€ monatl.

VCPU STAFFEL A	1 – 99	Discount 5 %
VCPU STAFFEL B	100 – 249	Discount 15 %
VCPU STAFFEL C	250 – 499	Discount 25 %
VCPU STAFFEL D	500 – 999	Discount 35 %
VCPU STAFFEL E	>= 1000	Discount 40 %

GET IN TOUCH

Become the Guardian of Public Sector Sovereignty

Leverage our experience from the registry modernisation project and secure your competitive edge in the public sector. Let's discuss how you can unlock new market potential and technically guarantee your clients' digital sovereignty with Confidential Computing.

At enclaive, we actively support IT service providers in integrating Confidential Computing into their stacks – and in deploying it efficiently and compliant in end-customer environments.

HOW ENCLAIVE SUPPORTS YOU:

- Workshops and training
- Co-marketing and co-selling
- Attractive partner and pricing models
- Setting up lab / test environments
- Tender and bit support

enclaive

Contact · sales@enclaive.io

FOR MORE INFORMATION, VISIT ENCLAIVE.IO