enclaive
CONFIDENTIAL COMPUTING

SOLUTION BRIEF

Sovereign Multi-Cloud Application Platform for Public Sector and Healthcare

The Deutschland Platform and MEDICUS Platform

Jointly delivered by Codesphere and enclaive

AUTHORS: DR. SEBASTIAN GAJEK

COPYRIGHT © 2026 ENCLAIVE GMBH. ALL RIGHTS RESERVED.

01 Executive Summary

Public administrations and healthcare organizations are under increasing pressure to digitize critical services while maintaining sovereignty, regulatory compliance, and protection of sensitive data. Traditional cloud deployments require trust in infrastructure providers and managed service operators, creating challenges around data confidentiality, jurisdictional control, and operational transparency.

The Deutschland and MEDICUS Platform address these challenges through a sovereign virtual multi-cloud architecture jointly delivered by Codesphere and Enclaive.

The platforms provide a trusted ecosystem where software vendors can develop, validate, publish, and operate applications across heterogeneous cloud infrastructures while maintaining cryptographic protection of sensitive workloads throughout their lifecycle.

By combining multi-cloud orchestration, marketplace-based service delivery, confidential computing, remote attestation, and external key management, organizations can consume digital services with verifiable trust guarantees independent of the underlying cloud provider.

02 Business Challenge

Across both the public sector and healthcare, digital transformation is no longer optional—it is becoming the default operating model for delivering critical services. Government agencies and healthcare providers are increasingly dependent on digital platforms to run core processes, interact with citizens and patients, and coordinate across organizational boundaries. At the same time, these domains operate under some of the strictest regulatory, security, and trust requirements of any industry.

For government agencies, the shift toward digital Fachverfahren enables more efficient administration of citizen services such as taxation, social security, permitting, and regulatory oversight. However, this transformation introduces a set of structural challenges that are difficult to resolve with traditional IT architectures. Agencies must maintain digital sovereignty while relying on external cloud infrastructure, ensure compliance with complex national and European regulations such as GDPR, avoid long-term dependency on single cloud providers, and protect highly sensitive citizen data from unauthorized access or exposure. In addition, there is a growing expectation that digital services should be delivered faster and with higher reliability, without compromising security or control.

Healthcare systems face a similarly complex, and in many ways even more sensitive, set of constraints. Providers are responsible for safeguarding highly personal medical data while simultaneously enabling modern digital health services, such as telemedicine, electronic health records, and AI-driven diagnostics. These capabilities require secure and scalable cloud adoption, yet they must be implemented in a way that guarantees patient data protection, supports trusted and auditable processing of medical information, and enables collaboration across hospitals, insurers, and research institutions. The introduction of advanced analytics and AI further increases the need for verifiable security guarantees, as decisions may directly impact patient outcomes.

> **Taken together, both domains highlight a fundamental tension: the need to innovate rapidly through cloud and AI adoption while preserving control, compliance, and trust over highly sensitive data.**

03 A New Cloud Trust Model

Traditional cloud environments require trust in:

- Infrastructure providers
- Cloud administrators
- Managed service providers
- Platform operators

The Deutschland Platform and MEDICUS Platform replace implicit trust with cryptographic trust.

Only attested workloads running within approved confidential environments receive access to application secrets and cryptographic keys.

This establishes a verifiable chain of trust between:

01 Software publisher

02 Application artifact

03 Runtime environment

04 Service operator

05 Consuming organization

04 Solution Overview

The Deutschland Platform and MEDICUS Platform establish sovereign digital ecosystems for trusted application deployment and consumption.

The solution combines:

Codesphere Virtual Multi-Cloud

- Unified developer platform
- Application lifecycle management
- CI/CD and deployment automation
- Infrastructure abstraction
- Multi-cloud orchestration

Application Marketplace

- Trusted application catalog
- Service discovery
- Procurement and booking
- Lifecycle management
- Compliance transparency

Cloud Broker

- Automated placement of workloads
- Policy-driven cloud selection
- Multi-cloud deployment orchestration
- Resource provisioning and lifecycle management

Enclaive Dyneemes

- Confidential Kubernetes execution
- Confidential Execution Environments (CEE)
- Runtime protection against infrastructure operators
- Isolation from cloud administrators and managed service providers

Enclaive vHSM

- External key management
- Cryptographic policy enforcement
- Remote attestation services
- Secure key release based on workload integrity

Deutschland Platform & MEDICUS Platform

Sovereign Virtual Multi-Cloud Platform Architecture

Software Vendors / Developers
Build, test and publish secure applications

Public Sector Organizations
Discover, book and operate Fachverfahren

Healthcare Organizations
Discover, book and operate Fachdienste

1 DEVELOPMENT & TESTING LAYER

CODESPHERE — Virtual Multi-Cloud Developer & Operations Platform

- Cloud IDEs & Workspaces
- Source Code Management
- CI/CD Pipelines
- Testing & Quality Automation
- Preview Environments
- Observability & Logging
- Runtime & App Management

2 TRUST & ATTESTATION LAYER

Security, Compliance & Attestation

- SAST / DAST Scanning
- Dependency & SBOM Analysis
- Container & Image Security
- Policy & Compliance Checks
- Vulnerability Management
- Attestation Preparation
- Digital Signing (Software Supply Chain)

3 MARKETPLACE LAYER

Deutschland Platform / MEDICUS Platform Marketplace

- Application Catalog (Fachverfahren / Fachdienste)
- Trust & Compliance Information
- Version & Lifecycle Management
- Licensing & Contracts
- Service Booking (Self-Service)
- Usage & Billing (Metering)

4 CLOUD BROKER LAYER

Cloud Broker & Orchestration

- Service Onboarding & Governance
- Policy Engine (Placement & Security)
- Cloud Selection & Optimization
- Provisioning & Automation
- Multi-Cloud Lifecycle Management
- Monitoring & SLA Management
- Chargeback & Cost Management

5 CONFIDENTIAL RUNTIME LAYER

Confidential Execution Across Sovereign Clouds

Hetzner Cloud
Kubernetes Cluster
Dyneemes Confidential Runtime
Confidential Pods (TEE)

Enclave vHSM (Service)
- Key Management
- Remote Attestation
- Policy Enforcement
- Secure Key Release

Microsoft Azure (Germany Region)
Kubernetes Cluster
Dyneemes Confidential Runtime
Confidential Pods (TEE)

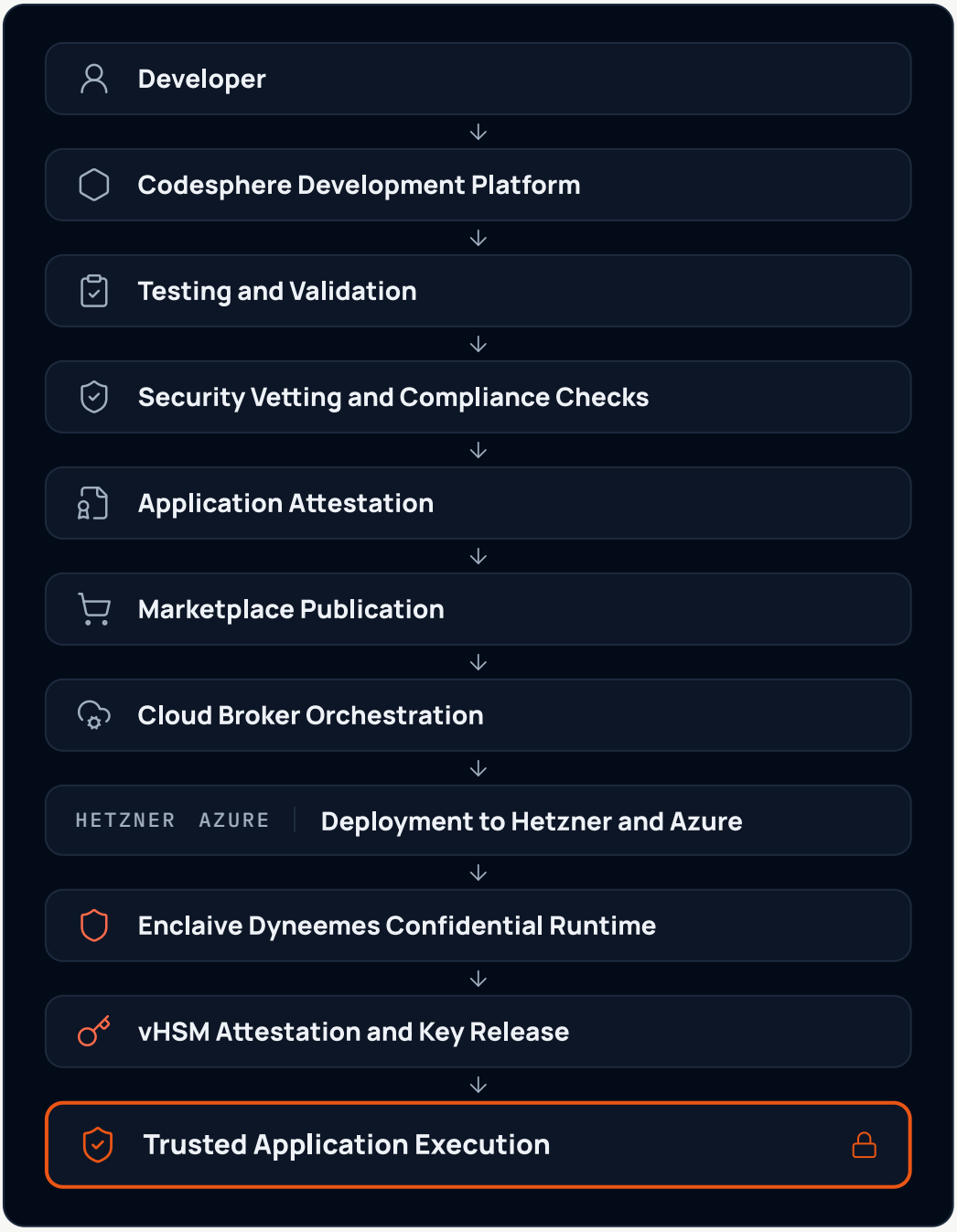
End-to-End Security & Trust

- Identity & Access Management
- Zero Trust Network Access
- Encryption In Transit & At Rest
- Confidential Computing (TEE)
- Remote Attestation
- Central Key Management (vHSM)
- Audit Logging & Monitoring
- Compliance & Reporting

Confidential Computing (TEE) · End-to-End Encryption · Zero Trust Architecture · Sovereignty & Data Residency · Auditability & Compliance

—— WORKFLOW / CONTROL FLOW ---- ORCHESTRATION / INTEGRATION

05 Platform Architecture



06 Benefits by Role

FOR CTOS

Accelerated Service Delivery

Organizations can consume and deploy applications through a marketplace model rather than operating bespoke infrastructure for every service.

Reduced Vendor Lock-In

Applications can be deployed across multiple cloud providers through a common operational layer.

Future-Proof Architecture

The platform supports hybrid and multi-cloud strategies while maintaining a consistent operational model.

Faster Innovation

Developers gain a cloud-native platform experience while organizations retain governance and control.

FOR CISOS

Confidential Computing

Sensitive workloads remain protected while executing. Infrastructure administrators cannot access application data, memory contents, or cryptographic material.

Verifiable Trust

Remote attestation verifies that workloads execute within approved confidential environments.

Externalized Key Control

Encryption keys remain under independent control through Enclaive vHSM.

Reduced Insider Risk

Cryptographic enforcement minimizes exposure to privileged cloud operators and managed service personnel.

Compliance Support

Supports implementation of GDPR, healthcare regulations, and public-sector security requirements.

For Solution Architects

Sovereign Multi-Cloud Design

Applications can be deployed across Hetzner, Azure, and future providers without architectural redesign.

Cloud Abstraction

Infrastructure-specific complexity is hidden behind a consistent platform layer.

Security by Design

Confidential computing and attestation become part of the deployment architecture rather than afterthoughts.

Service-Oriented Consumption

Applications become deployable and consumable services through marketplace-based provisioning.

Standardized Trust Framework

A common trust architecture applies across all participating clouds and service providers.

07 Target Use Cases

Deutschland Platform

- Citizen service portals
- Social security systems
- Tax and finance applications
- Permit and licensing services
- Justice and administrative applications
- Government AI services

MEDICUS Platform

- Electronic patient record services
- Clinical decision support systems
- Medical AI applications
- Telemedicine platforms
- Healthcare data exchange services
- Research and analytics workloads

08 Conclusion

The Deutschland Platform and MEDICUS Platform establish a new operating model for sovereign digital services.

By combining Codesphere's Virtual Multi-Cloud platform with Enclaive's confidential computing, attestation, and key management technologies, public-sector and healthcare organizations gain a trusted environment for deploying and consuming sensitive applications across heterogeneous cloud infrastructures.

The result is a sovereign, auditable, and cryptographically verifiable platform that enables digital transformation without compromising security, compliance, or operational independence.

ABOUT ENCLAIVE

enclaive builds the post-quantum secure, confidential multi-cloud platform that keeps data encrypted at rest, in transit and in use, encrypted even while being processed. Regulated industries run any workload on any cloud without trusting the infrastructure beneath it. enclaive secures Germany's GovTech-Platform and is a NATO DIANA 2026 innovator. Founded 2022, headquartered in Frankfurt am Main. enclaive.io

Copyrights

All content, text, and materials in this document are the property of enclaive. This document may not be copied, reproduced, distributed, or shared in whole or in part without the prior written consent of enclaive.

© 2026 enclaive GmbH. All rights reserved.

ACKNOWLEDGEMENT

All product names, logos, brands, and trademarks mentioned herein—including but not limited to AMD, Intel, NVIDIA—are the property of their respective owners. Any use of these names is for identification purposes only and does not imply endorsement. All rights, including copyrights and trademarks, remain solely with the corresponding companies.

NOTICES

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) may represent or impact current enclaive product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from enclaive and its affiliates, suppliers, or licensors. enclaive products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of enclaive to its customers are governed by enclaive agreements, and this document is not part of, nor does it modify, any agreement between enclaive and its customers.