

Trau, schau wem! „Secrets, Confidential Computing & Zero Trust“ unter Souveränitätsgesichtspunkten

Mark Neufurth, IONOS

Track 1, IONOS Summit 2026



The logo for the IONOS SUMMIT. The word "IONOS" is in white, and "SUMMIT" is in a light blue color. The background is a dark blue gradient with a white geometric pattern of interconnected lines and dots, resembling a network or a molecular structure.

IONOS SUMMIT

Track 1 · Public Sector · 2026

Trau, schau wem!

„Secrets, Confidential Computing & Zero Trust“
unter Souveränitätsgesichtspunkten

Mark Neufurth

Enterprise Strategist Public Sector, IONOS



DIE VERTRAUENSFRAGE

Die Ausgangslage

Vertrauen ist kein Sicherheitskonzept.

1

Fremde Infrastruktur

Daten liegen physisch, rechtlich und operativ in der Hand Dritter.

2

Frage der Jurisdiktion

Zugriff ist nicht nur Technik, sondern Rechtsraum – CLOUD Act & Co.

3

Schlüssel = Kontrolle

Wer die Schlüssel hält, kontrolliert die Daten – nicht, wer sie besitzt.

4

Vertrauen ist unsichtbar

Es lässt sich nicht prüfen – bis zu dem Tag, an dem es gebrochen wird.

DIGITALE SOUVERÄNITÄT

**Die Frage ist nicht „ob“ Cloud,
sondern „*mit wem*“**



Was das BSI daraus macht

Aus Prinzipien werden prüfbare Kriterien – Treiber ist „Cyber Dominance“.

01

Secrets Management

C3A · SOV-3 Datensouveränität, 04/2026

- Externe Schlüsselverwaltung integrierbar: BYOK / HYOK
- Clientseitige Verschlüsselung vor Verlassen der Umgebung
- Externe Identity-Provider über offene Standards

Datenresidenz ≠ Datensouveränität

02

Confidential Computing

C5:2026 · Operations & Krypto, 04/2026

- Erstmals dezidiert im Katalog: Zweck, Scope, Maßnahmen
- Flankiert von Post-Quanten-Krypto und Krypto-Agilität
- C5-Konformität ist Voraussetzung für C3A

Prüfbar ≠ souverän

03

Zero Trust

Positionspapier 07/2023 · Grundschutz++

- „Assume Breach“ als Architekturparadigma
- Umsetzung über ORP.4 und NET.1.1
- **Kein Souveränitätskriterium** – Anbieter framen es so

Sicherheits- ≠ Souveränitätskriterium

Notwendig, aber nicht ausreichend. SOV-4 verlangt jährlich getestete Trennbarkeit aller Nicht-EU-Verbindungen.

Souveränität entsteht nicht durch Vertrauen, sondern durch überprüfbare Kontrolle

Drei technische Antworten auf die Vertrauensfrage:

01

Secrets Management

Hoheit über Schlüssel, Tokens und Zugangsdaten – getrennt von den Daten.

02

Confidential Computing

Schutz der Daten auch während der Verarbeitung – selbst vor dem Betreiber.

03

Zero Trust

Kein Vertrauensvorschuss: jede Anfrage wird verifiziert, nichts implizit erlaubt.

Wer hält den Schlüssel?

Secrets Management

Kontrolle über das, was Zugriff gewährt

- **Zentral verwalten und rotieren.** Schlüssel, Tokens und Zertifikate an kontrolliertem Ort, mit klarer Lebenszyklus-Steuerung.
- **Daten- und Schlüsselhoheit trennen.** BYOK / HYOK: die Schlüssel bleiben in Ihrer europäischen Hand – nicht beim Betreiber.
- **Keine Secrets im Klartext.** Nie in Code, Konfigurationen oder Logs – Angriffsfläche systematisch entfernen.

Confidential Computing

IONOS SUMMIT

Verschlüsselung schließt die letzte Lücke: die Daten während der Verarbeitung.

Data at Rest

Etabliert

Gespeicherte Daten sind mehrfach redundant verschlüsselt – auf Datenträgern und in Backups.

Data in Transit

Etabliert

Übertragene Daten sind verschlüsselt – TLS auf jeder Verbindung.

Data in Use

Die Lücke – jetzt schließbar

Daten werden im geschützten Speicher (TEE) verarbeitet – unsichtbar selbst für den Betreiber.

Confidential VM: kryptografisch statt vertraglich

Verfügbar seit 12. August 2026 · AMD SEV-SNP

01

Hardware-erzwungene Isolation

Speicher und CPU-State in Runtime AES-128-verschlüsselt. Schlüssel entstehen im AMD Secure Processor und verlassen das Silizium nicht.

02

Der Betreiber hält keine Schlüssel

Hypervisor, Host-OS und IONOS sind aus Entschlüsselungspfad ausgeschlossen – auch für Support, Incident & behördliche Anfragen.

03

Attestation vor Secret-Freigabe

Signierte Measurements (VCEK/VLEK über AMD KDS) werden geprüft, bevor Volume Master Key/Secrets in VM gelangen.

04

Nachprüfbare Firmware-Herkunft

SLSA-Level-2-Provenance der OVMF-Builds, unveränderlich in Sigstore Rekord – Plattformaussagen unabhängig verifizierbar.

Referenz-Toolchain: SNPGuard · LUKS2-Verschlüsselung im Image · Grenzen: keine Live-Migration, kein cloud-init, SMT nicht abschaltbar, Storage- und Netzverschlüsselung in Kundenverantwortung

Wer hält den Schlüssel?

SEAL-3

Kontrolle über das, was Zugriff gewährt

- **Zentral verwalten & rotieren.** Schlüssel, Tokens und Zertifikate an kontrolliertem Ort, mit klarer Lebenszyklus-Steuerung.
- **Daten- und Schlüsselhoheit trennen.** BYOK/HYOK: die Schlüssel bleiben in Ihrer Hand – nicht beim Betreiber.
- **Keine Secrets im Klartext.** Nie in Code, Konfigurationen oder Logs – Angriffsfläche systematisch entfernen.

Regulatorik macht Souveränität zur Pflicht

Aus politischem Ziel wird ein Vergabe- und Architekturkriterium



Cloud and AI Development Act (CADA)

- Entwurf vom 3. Juni 2026 – Kern EU-Tech-Sovereignty-Pakets
- Vier Assurance-Level regeln Zugang zu Public-Sector-Verträgen
- „Union added value“ nachrangiges Vergabekriterium
- Verzahnt mit Data Act · DMA · AI Act · NIS2 · DORA · EUCS

CADA: vier „Union-Assurance-Level“ für Cloud im öffentlichen Sektor – abgestuft nach Schutzbedarf

Bund · IT-Architekturrichtlinie v6.2.1

AV-9 „Digitale Souveränität“ ist MUSS-Vorgabe:
Austauschbarkeit, offene Standards, kein Lock-in

ZUSAMMENSPIEL

Vom *Vertrauen* zur Verifizierbarkeit



Für Compliance-lastige Kunden

Handlungs- empfehlungen

Souveränität planbar machen – nicht dem Zufall überlassen.

1

Schlüsselhoheit einfordern

BYOK/HYOK und europäische Key-Management-Services als Vergabekriterium.

2

Confidential Computing verlangen

Schutz der Daten „in use“ als Anforderung – nicht als Kür.

3

Zero Trust als Zielbild

Identitätszentrierte Architektur schrittweise etablieren und messen.

4

Souveränität nachweisbar machen

Attestation, Audits & Nachweise statt vertraglicher Versprechen.

IONOS SUMMIT

DANKE

Mark Neufurth

Enterprise Strategist Public Sector, IONOS
mark.neufurth@cloud.ionos.com

