SPIE

X-SPIErience Day 2020

DIGITALE SOUVERÄNITÄT

Cisco Partner

FORTINET

HUAWEI

SPIE, sharing a vision for the future

Corporate Software
Member of SPIE Switzerland

X-SPIErience Day 2026
DIGITALE SOUVERÄNITÄT

SPIE

Daten unter Kontrolle: Wie eine Data- und Analytics-Plattform Digitale Souveränität ermöglicht

MATTHIAS FALLAND

Microsoft Data Platform MVP &
Managing Director bei Corporate Software,
Member of SPIE Switzerland

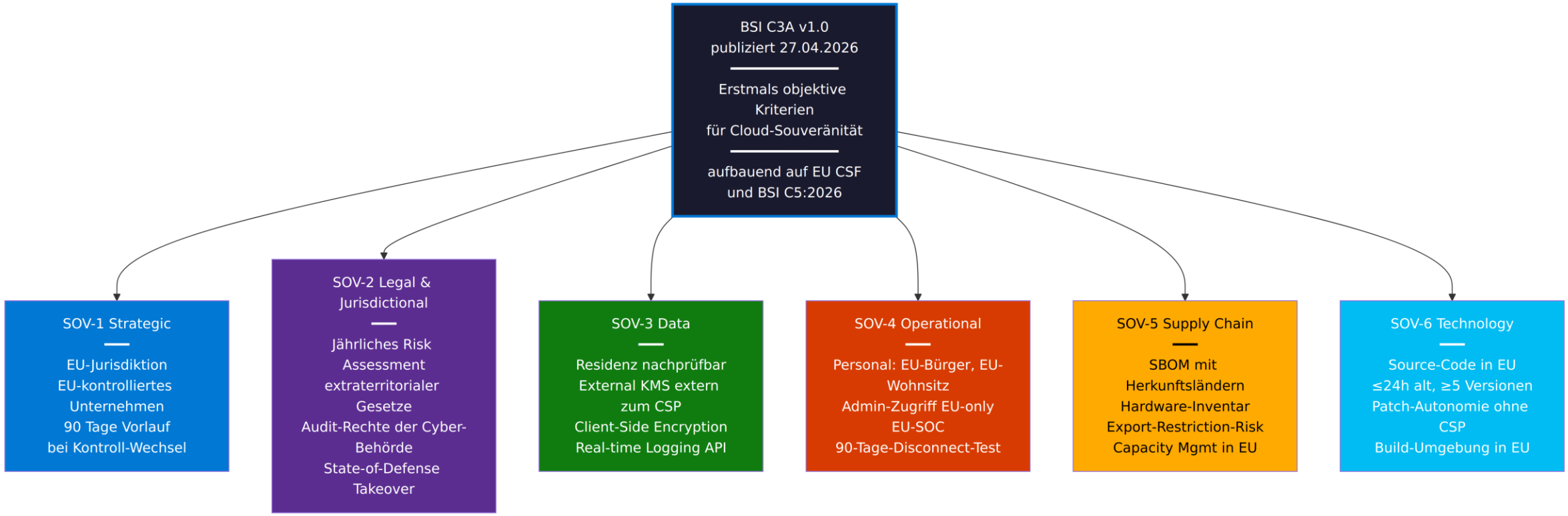
”

Souveränität ist nicht ein Feature.
Sie ist die Summe Ihrer Architektur-Entscheidungen.

Gestern, 27. April 2026 — die Souveränität ist messbar geworden

- BSI veröffentlicht C3A v1.0 — Criteria enabling Cloud Computing Autonomy. Erstmals ein objektiver, auditierbarer Kriterienkatalog dafür, was eine Cloud tatsächlich souverän macht.
- BSI-Definition (wörtlich): „Digital sovereignty describes the abilities and opportunities of individuals and institutions to perform their role(s) in the digital world independently, self-determinedly (autonomous) and securely.“
- Anschluss an die EU Cloud Sovereignty Framework, gestützt auf BSI C5:2026. Sechs Dimensionen — SOV-1 bis SOV-6. SOV-7 Security ist durch C5 abgedeckt; SOV-8 Sustainability liegt ausserhalb des BSI-Mandats.
- Nicht bindend in sich. Aber: das ist das erste Vokabular, das in jede kommende Ausschreibung, jede Audit-Vorgabe und jedes CISO-Briefing einfliessen wird. Wer heute Architektur entscheidet, sollte C3A im Kopf haben.
- Die heutige Frage: was leistet Microsoft Fabric davon out-of-the-box, und wo muss Architektur die Lücke schliessen?

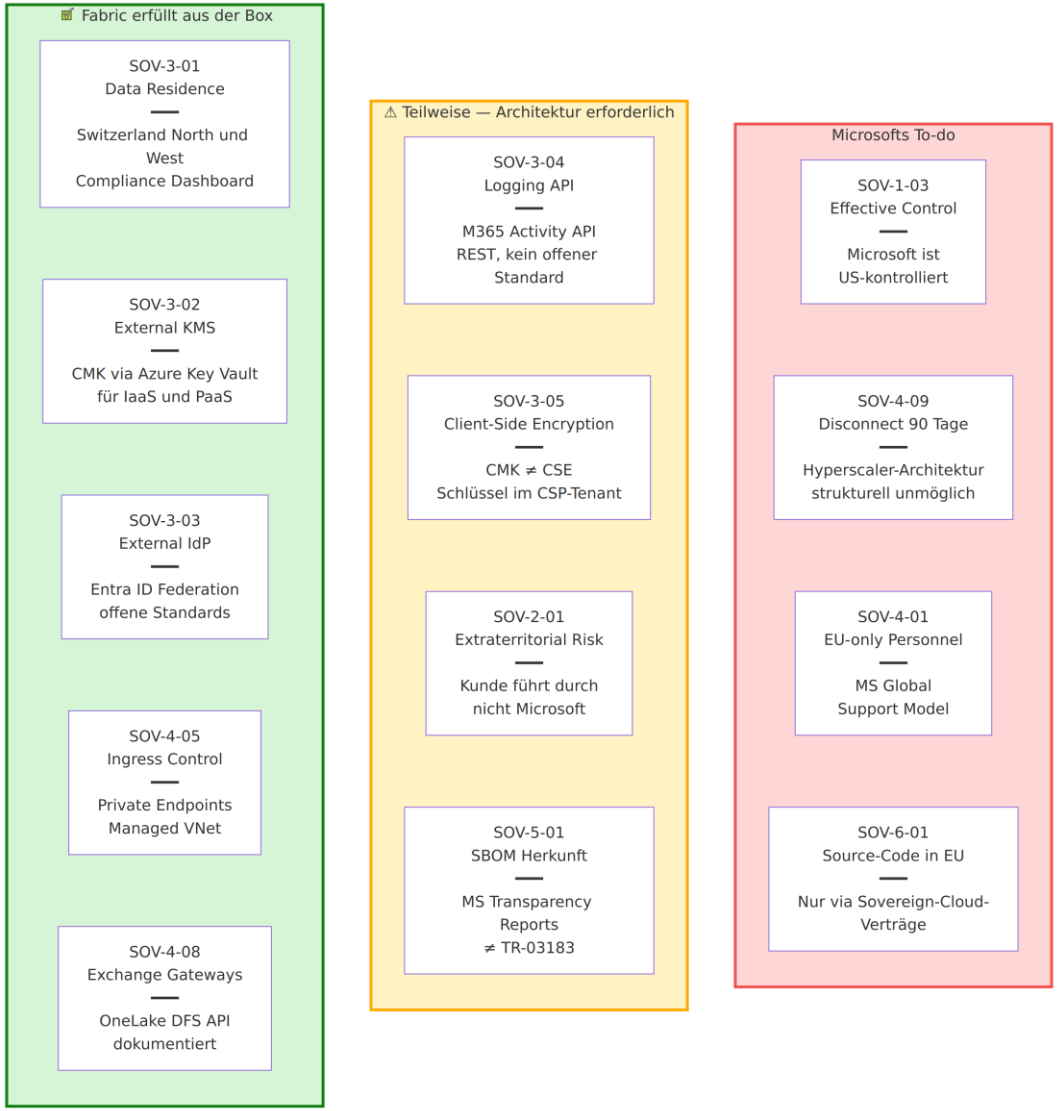
BSI C3A v1.0 — sechs Dimensionen der Cloud-Souveränität



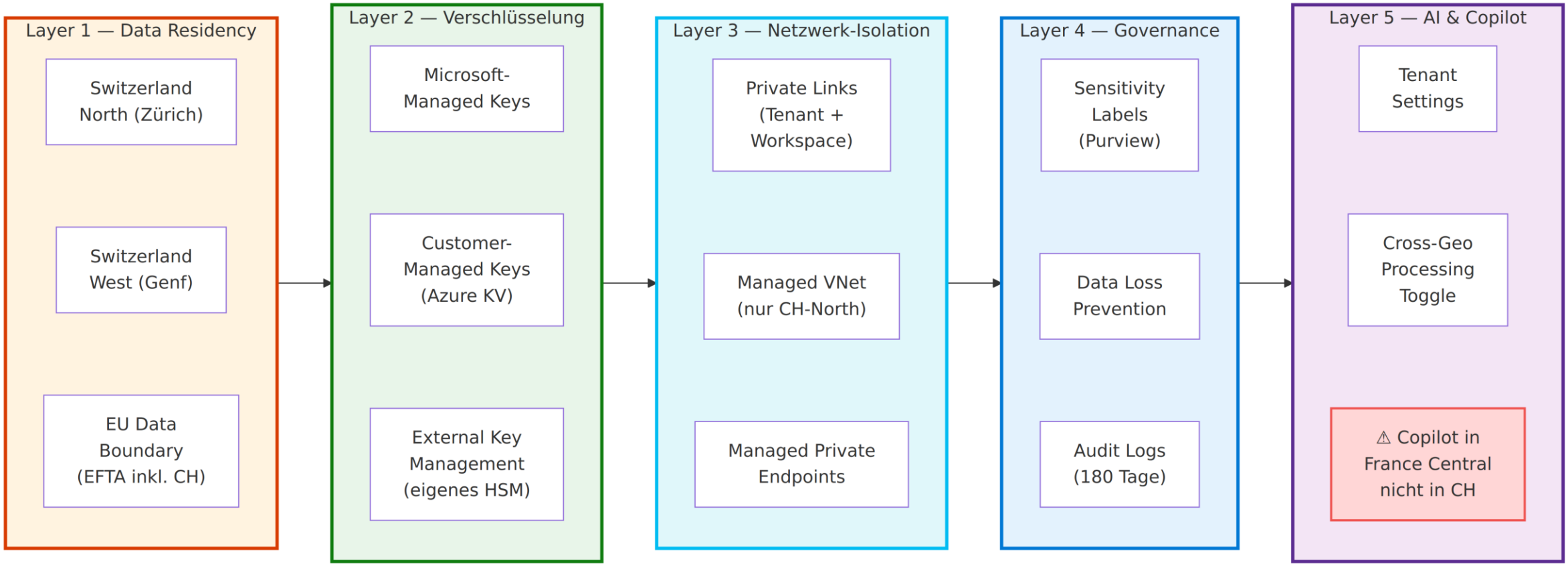
Fabric in Switzerland North — was C3A heute bekommt

- SOV-3-01 Data Residence: Workspace-Region Switzerland North oder West. Compliance Dashboard und Purview machen den Speicherort jederzeit nachprüfbar.
- SOV-3-02 External Key Management (IaaS und PaaS): Customer-Managed Keys via Azure Key Vault, FIPS 140-2 Level 3, mit Soft-Delete und Purge-Protection.
- SOV-3-03 External Identity Provider: Entra ID Federation über offene Standards (SAML, OIDC). Stateless Authentication möglich.
- SOV-4-05 Ingress Data Control: Private Endpoints und Managed VNet (letzteres nur in CH-North) mit DMZ-Pattern für Updates.
- SOV-4-08 Data Exchange Gateways: OneLake DFS-API als dokumentierte, kontrollierbare Schnittstelle. EU Data Boundary deckt EFTA inkl. CH ab.
- Das ist nicht nichts. Das ist eine ehrliche Hälfte einer Liste, die sechs Dimensionen umfasst — und Fabric liefert sie out-of-the-box.

Coverage-Matrix — Met, Teilweise, Lücke



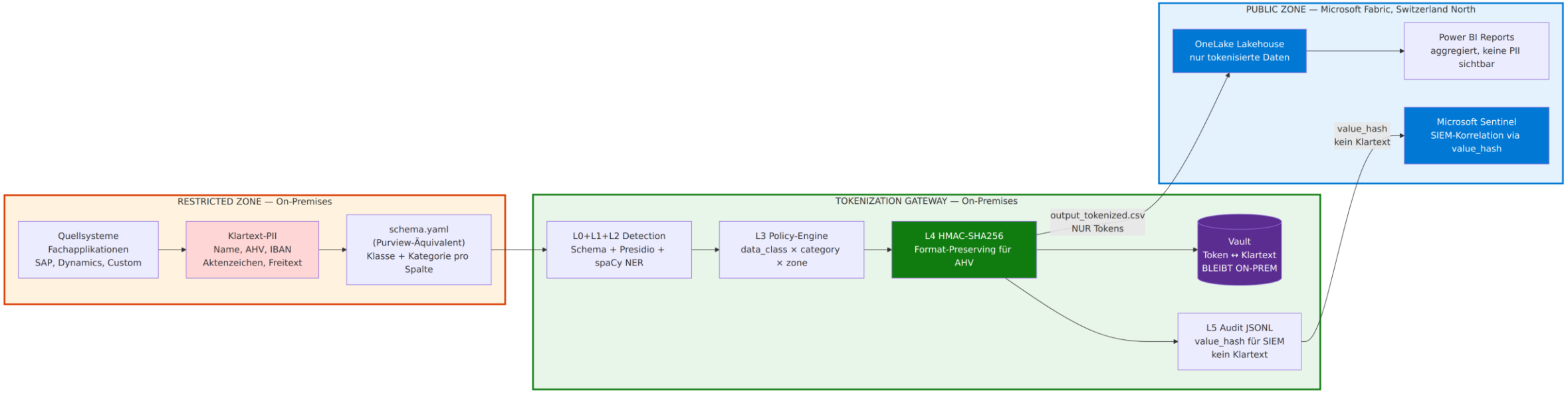
Fabric Sovereignty Stack — die Schichten, die heute existieren



Strategie — die Lücke architektonisch füllen

- Was kommerzielle Fabric strukturell nicht liefern kann: SOV-1 Effective Control (Microsoft ist US-kontrolliert), SOV-4-09 Disconnect-Test über 90 Tage, SOV-3-05 Client-Side Encryption (CMK ≠ CSE — der Schlüssel ist in Azure KV, also im CSP-Tenant), SOV-6-01 Source-Code in EU.
- Falsche Antwort: „Dann eben kein Fabric." Sie verlieren OneLake, Direct Lake, Copilot — und gewinnen einen handgebauten Stack, den Sie auch nicht souverän halten können.
- Falsche Antwort: „Microsoft Sovereign Cloud löst das." Sie zahlen Feature-Lag, höhere Kosten, eingeschränkte Region-Coverage — und vertrauen am Ende immer noch demselben Anbieter.
- Richtige Antwort: zwei Zonen, ein Gateway dazwischen. Die Public Zone ist Fabric in CH-North mit allen SOV-3 und SOV-4 Kontrollen. Die Restricted Zone ist on-prem mit den Klartext-PII. Das Gateway tokenisiert.
- Schlüssel-Erkenntnis: nicht alles muss in die Public Zone. Aggregierte Reports, Trends, Mengen — ja. Klartext-PII für Re-Identifikation — nie. Das ist Data Minimization als Architektur, nicht als Versprechen.

Zwei-Zonen-Modell mit Tokenization Gateway



Three-Axis Policy — wie das Gateway entscheidet

- Drei Achsen pro Datenzelle, nicht eine: data_class (public, internal, confidential, strict_confidential), data_category (pii, financial, free_text, metadata), target_zone (public, internal_analytics).
- Selbe Detection, andere Aktion. Eine AHV-Nummer in einem strict_confidential-Feld auf dem Weg in die Public Zone wird tokenisiert. Dieselbe AHV-Nummer in einem internal-Feld auf dem Weg in internal_analytics wird durchgereicht.
- Vier Aktionen, keine mehr: TOKENIZE (full-cell HMAC), MASK (Span im Freitext), REVIEW (Mid-Konfidenz an menschliche Prüfung), PASS (kein Eingriff). Jede Entscheidung mit Rule-ID im Audit-Log.
- First-match-wins. R-001 vor R-010 vor R-002. Die Reihenfolge ist die Policy — nicht ein 800-seitiges Compliance-Manual.
- Gleich live: TokenDemo zeigt diese Logik auf sieben Schweizer Demo-Datensätzen, mit echter AHV-mod-10-Validierung, IBAN-mod-97, spaCy-NER auf Freitext, und einem Vault, der den Laptop nicht verlässt.

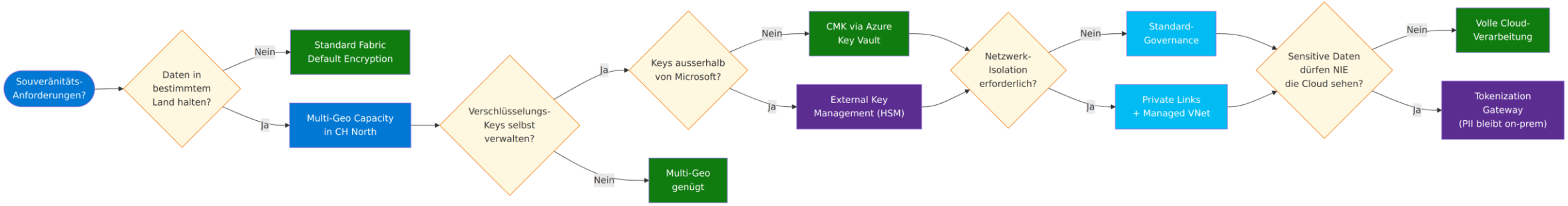
Demo

TokenDemo — sechs Layer, eine CSV.

Was die letzten Minuten C3A-konform geleistet haben

- SOV-3-05 Client-Side Encryption (funktional): Klartext-PII wurde on-prem durch HMAC-SHA256 ersetzt. Der Pepper hat das Gateway nie verlassen. Die Cloud sieht nur Tokens. Produktion: FF1/FF3 oder AEAD im HSM.
- SOV-3-04 Logging Real-time API: audit.jsonl mit dokumentiertem Schema. value_hash ist SHA-256(klartext)[:16] — SIEM kann korrelieren, ohne PII zu replizieren.
- SOV-4-07 Data Exchange Monitoring: Austauschformat ist explizit (output_tokenized.csv). Pro Zelle: detection layer, recognizer, entity type, policy rule, confidence. Komplette Nachvollziehbarkeit.
- SOV-4-08 Data Exchange Gateways: genau eine Schnittstelle nach aussen — fabric_upload.py mit OneLake DFS PUT. vault.csv und pepper.txt sind im Code-Pfad nicht erreichbar. Architektonische, nicht prozessuale Garantie.
- Das ist die Botschaft: C3A ist kein Microsoft-Privileg. Sie können die Lücke aus 250 Zeilen Python schliessen — wenn Sie die richtige Architektur haben. Microsoft Fabric ist die Public Zone. Das Gateway ist Ihres.

Architektur-Entscheidungsbaum — welche Kontrollen brauchen Sie?



Fünf Takeaways — was Sie morgen tun können

- C3A als Self-Assessment durchgehen. Pro SOV-Dimension dokumentieren, wo Sie heute stehen — grün, gelb, rot. Das ist eine Tagesarbeit, nicht ein Projekt. Output: ein Aufhänger für jede Architektur-Diskussion der nächsten zwölf Monate.
- Fabric in Switzerland North bleibt der richtige Ausgangspunkt. CMK plus Private Endpoints plus Purview-Sensitivity-Labels ab Tag 1. Das deckt die Hälfte von C3A out-of-the-box ab — und das ist beachtlich.
- Zwei-Zonen-Modell mit Tokenization Gateway, sobald Sie Daten haben, die C3A SOV-3-05 oder SOV-4-09 strikt verlangen — Bankgeheimnis, GWG, Gesundheits-Daten, Verteidigungs-Kontext. Pseudonymisierungs-Schlüssel im On-Prem HSM, nicht in Azure Key Vault.
- Three-Axis Policy als operatives Prinzip: data_class, data_category, target_zone. Keine binären „Cloud ja/nein"-Entscheidungen mehr — pro Zelle, dokumentiert, auditierbar. Das ist die Operationalisierung von C3A in der Plattform-Logik.
- Vault on-prem, Audit überall. Die Cloud sieht nur Tokens. Audit-Logs spiegeln in Sentinel oder Splunk — die 180-Tage-Retention von Fabric reicht weder für Finma noch für SOV-2-Audit-Rechte.
- Die Klammer darüber: C3A definiert das Vokabular. Architektur liefert die Antwort. Nicht ein Produkt, nicht ein Audit, nicht ein Hyperscaler-Versprechen — sondern Ihre Architektur-Entscheidungen, getroffen bevor ein Auditor, eine Behörde oder ein Incident sie für Sie trifft.

Ihr Ansprechpartner bei Corporate Software und SPIE CIS

Danke!

Und jetzt: Ihre Fragen.

spie.ch/ai

Matthias Falland

Microsoft Data Platform MVP &
Managing Director bei Corporate Software, Member of SPIE Switzerland

Mail matthias@falland.ch