MATTHIAS FALLAND
The Trusted Advisor — Microsoft Data Platform MVP

Daten unter Kontrolle

BSI C3A trifft Microsoft Fabric — Begleitdokument zur Session am X-SPIErience Day Bern 2026

Autor
Matthias Falland

Datum
28. April 2026

Version
v1.0

Klassifizierung
Public Handout

Empfänger
Teilnehmer X-SPIErience Day 2026 Bern

Änderungshistorie

Version	Datum	Autor	Beschreibung
0.1	2026-04-13	Matthias Falland	Initiale Session-Outline (v1, Cloud-Act-Framing)
0.5	2026-04-25	Matthias Falland	Story-Erweiterung um Zwei-Zonen-Modell und TokenDemo
1.0	2026-04-28	Matthias Falland	C3A-aligned Rebuild nach BSI-Publikation am 27.04.2026

Executive Summary

Am 27. April 2026 hat das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) das Dokument **C3A — Criteria enabling Cloud Computing Autonomy** veröffentlicht. Erstmals existiert damit ein *objektiver, auditierbarer Kriterienkatalog* für Cloud-Souveränität in DACH — sechs Dimensionen, anschlussfähig an die EU Cloud Sovereignty Framework und an BSI C5:2026.

> **Kernbotschaft dieses Dokuments**
>
> Microsoft Fabric in Switzerland North erfüllt grob die Hälfte der C3A-Kriterien out-of-the-box. Die andere Hälfte ist eine bewusste Architektur-Entscheidung — realisiert durch ein Zwei-Zonen-Modell mit on-premises betriebenem Tokenization-Gateway, dessen Vault den unternehmenseigenen Perimeter niemals verlässt.

Das vorliegende Dokument vertieft die Inhalte der 30-minütigen Session *Daten unter Kontrolle* am X-SPIErience Day 2026 Bern. Es folgt der Slide-Choreografie, expandiert die Speaker-Notes als Fliesstext und ergänzt das vollständige C3A-Kriterien-Mapping als Anhang.

Die zentrale Erkenntnis: **Souveränität ist nicht ein Feature. Sie ist die Summe Ihrer Architektur-Entscheidungen. Seit dem 27. April 2026 ist sie messbar.** Wer heute Architektur entscheidet, sollte C3A im Kopf haben — nicht weil das Dokument bindend wäre, sondern weil es das erste Vokabular ist, das in jede Ausschreibung, jedes Audit und jedes CISO-Briefing der nächsten zwölf Monate einfliessen wird.

Inhaltsverzeichnis

1

Was BSI gestern publiziert hat

Am 27. April 2026 hat das BSI das Dokument *Criteria enabling Cloud Computing Autonomy* (C3A) in Version 1.0 veröffentlicht — sechzehn Seiten, lizenziert unter Creative Commons CC-BY-ND 4.0, abrufbar unter `https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/C3A_Cloud_Computing_Autonomy.pdf`.

Die BSI-Definition lautet 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."*

Bis zum 27. April war "souveräne Cloud" ein Bauchgefühl; jeder Kunde hatte eine andere Vorstellung davon, was das konkret bedeutet. Mit C3A liegt nun ein *messbarer* Kriterienkatalog vor.

1.1 Drei Dinge, die für Schweizer Architekten wichtig sind

1. C3A ist **nicht bindend in sich**. Aber: das Dokument wird in jede kommende Ausschreibung, jede Audit-Vorgabe und jedes CISO-Briefing der nächsten Monate einfliessen. Spätestens 2027 ist davon auszugehen, dass es als Standard-Anhang in Schweizer Beschaffungsverfahren auftaucht.
2. C3A baut **strukturell auf der EU Cloud Sovereignty Framework** (EU CSF) auf und ist mit **BSI C5:2026** kompatibel. Wer C5-konform betreibt, hat einen Teil von C3A bereits abgedeckt — die Bereiche SOV-7 Security/Compliance und SOV-8 Sustainability sind bewusst ausgeklammert (C5 deckt Security ab; Nachhaltigkeit liegt ausserhalb des BSI-Mandats).
3. C3A definiert **sechs Dimensionen der Souveränität** — nicht eine, nicht drei. Die in der Schweizer Diskussion oft benutzte Trias "Daten / Technologie / Betrieb" bleibt gültig, aber sie ist eine vereinfachte Sicht. Die echte Reifegrad-Beurteilung läuft über sechs Achsen.

Anwendung des Dokuments

C3A kann von zwei Akteuren genutzt werden: einerseits von Cloud-Anbietern, die per Audit nachweisen, welche Kriterien sie erfüllen; andererseits von Cloud-Kunden, die ihren Souveränitäts- Anspruch pro Dimension formulieren und dann die für ihre Workloads relevanten Anbieter daran messen.

2

Die sechs Dimensionen im Detail

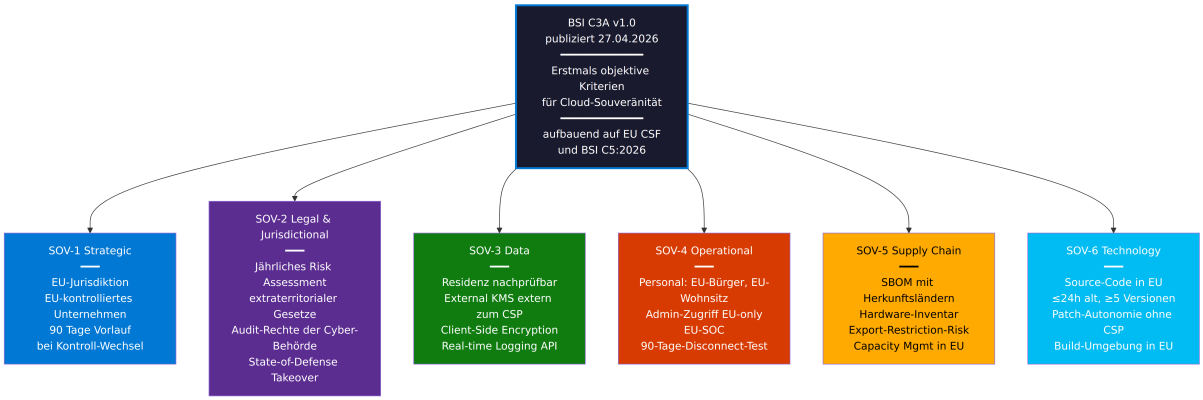

Abbildung 2.1: BSI C3A v1.0 — Sechs Dimensionen der Cloud-Souveränität. Jede Dimension wirft eine konkrete Architektur-Frage auf, die mit Ihrem CISO durchgegangen werden sollte.

2.1 SOV-1 Strategic Sovereignty

Kernfrage: Wer kontrolliert das Unternehmen, mit dem ich einen Vertrag habe?

C3A fordert für die strenge SOV-1-Variante, dass der Cloud-Anbieter unter EU- (oder deutscher) Jurisdiktion operiert, einen Hauptsitz in der EU hat und *effektiv durch ein oder mehrere EU-Unternehmen kontrolliert* wird. Effektive Kontrolle bedeutet, dass keine direkte oder indirekte Einflussnahme aus Drittstaaten auf strategische, finanzielle oder operative Entscheidungen möglich ist.

Zusätzlich verlangt C3A eine **90-tägige Vorlaufmeldung** bei Eigentümer- oder Governance-Wechseln, die die Souveränitäts-Kontrollen beeinträchtigen könnten.

Microsoft und SOV-1

Microsoft Corporation hat ihren Hauptsitz in den Vereinigten Staaten. Damit erfüllt kommerzielle Microsoft Fabric (auch in Switzerland North) das SOV-1-03-C1-Kriterium der effektiven EU-Kontrolle nicht. Microsofts EU Sovereign Cloud-Initiative adressiert genau diesen Punkt — mit eigenen rechtlichen Strukturen in Europa, aber zu einem Preis (Feature-Lag, höhere Kosten, eingeschränkte Region-Coverage).

2.2 SOV-2 Legal & Jurisdictional Sovereignty

Kernfrage: Welche extraterritorialen Gesetze haben Zugriff auf meine Daten?

C3A verlangt vom Anbieter ein *jährliches strukturiertes Risk Assessment* aller Nicht-EU-Gesetze, die grenzüberschreitend auf verfügbarkeit, Vertraulichkeit oder Integrität der Cloud-Services einwirken können (US CLOUD Act, US FISA 702 etc.).

Weiter werden **Audit-Rechte für die zuständige Cybersicherheits- Behörde** verlangt sowie ein dokumentierter Prozess, wie der Staat im Verteidigungsfall die operativen Capabilities übernehmen kann — inklusive Source Code, Administrationswerkzeugen und Personal.

2.3 SOV-3 Data Sovereignty

Kernfrage: Wo liegen meine Daten und wer kann sie lesen?

SOV-3 ist die operativ wichtigste Dimension und enthält fünf konkrete Kriterien:

- **SOV-3-01 Data Residence**: Der Kunde muss jederzeit nachprüfen können, wo seine Daten gespeichert und verarbeitet werden.
- **SOV-3-02 External Key Management**: Verschlüsselungs- Schlüssel müssen ausserhalb der CSP-Umgebung erzeugt, verwaltet und gespeichert werden können — für IaaS und PaaS verpflichtend, für SaaS als Additional Criterion.
- **SOV-3-03 External Identity Provider**: Authentifizierung über offene, nicht-proprietäre Standards.
- **SOV-3-04 Logging und Monitoring**: Audit-Logs in Echtzeit über standardisierte Open-Source-APIs.
- **SOV-3-05 Client-Side Encryption**: Klartextdaten werden mit einem Schlüssel verschlüsselt, der die CSP-Umgebung *niemals* betritt.

CMK ≠ Client-Side Encryption

Customer-Managed Keys im Azure Key Vault erfüllen SOV-3-02 für IaaS und PaaS — aber sie erfüllen **nicht** SOV-3-05. Der Schlüssel liegt zwar im Kundenkontext, befindet sich aber weiterhin in der Microsoft-Tenant-Umgebung. Echte Client-Side Encryption verlangt, dass der Schlüssel in einem HSM ausserhalb von Azure liegt — oder dass Daten on-premises durch ein eigenes Gateway verschlüsselt werden, bevor sie die Cloud erreichen. Genau das demonstriert die TokenDemo.

2.4 SOV-4 Operational Sovereignty

Kernfrage: Wer betreibt die Cloud — physisch und administrativ?

SOV-4 verlangt unter anderem, dass alle Personen mit logischem oder physischem Zugriff auf die operative Infrastruktur **EU-Bürger mit EU-Hauptwohnsitz** sind und dass administrativer Zugriff ausschliesslich aus der EU erfolgt. Weiter werden ein **EU-basiertes Security Operations Center**, redundante Konnektivität, ein definierter **Disconnect-Test** (Cloud funktioniert 90 Tage ohne Non-EU-Verbindungen) sowie kontrollierte Update-Prozesse über eine secured network area gefordert.

Der Disconnect-Test ist für Hyperscaler-Architekturen strukturell herausfordernd — viele Cloud-Komponenten haben Heartbeats und Lizenz-Server, die regelmässig zu Hauptquartieren ausserhalb der EU verbinden.

2.5 SOV-5 Supply Chain Sovereignty

Kernfrage: Aus welchen Ländern stammen Software und Hardware?

Der Anbieter muss einen **Software Bill of Materials (SBOM)** mit Herkunftsländern aller Komponenten führen — C3A empfiehlt TR-03183 als Qualitätsstandard. Analoges gilt für Hardware, externe Service-Dependencies und Export-Restriction-Risikomanagement.

2.6 SOV-6 Technology Sovereignty

Kernfrage: Kann ich die Cloud weiterführen, wenn der Anbieter weg ist?

C3A verlangt ein Source-Code-Backup in der EU, das nicht älter als 24 Stunden ist und mindestens fünf Versionen vorhält — inklusive aller Build-Skripte und Deployment-Toolchains. Weiter

müssen dokumentierte Continuity-Strategien und EU-basierte Engineering-Talente vorhanden sein, die im Notfall Patches erstellen können.

3

Microsoft Fabric durch das C3A-Filter

3.1 Was Microsoft Fabric heute aus der Box erfüllt

- **SOV-3-01 Data Residence**: Workspace-Region in Switzerland North oder Switzerland West. Compliance Dashboard und Microsoft 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 als Pflicht-Settings.
- **SOV-3-03 External Identity Provider**: Entra ID Federation über SAML, OIDC. Stateless Authentication möglich.
- **SOV-4-05 Ingress Data Control**: Private Endpoints und Managed VNet (letzteres nur in CH-North, nicht CH-West). Update-Prozesse durchlaufen kontrollierte DMZ-Pattern.
- **SOV-4-08 Data Exchange Gateways**: OneLake DFS-API als dokumentierte, kontrollierbare Schnittstelle. EU Data Boundary deckt EFTA inklusive Schweiz ab.

3.2 Wo Architektur-Arbeit erforderlich ist

- **SOV-3-04 Logging Real-time API**: Microsoft Fabric bietet Audit-Logs über die M365 Activity API — diese ist eine REST-API, aber kein offener Standard im strengen C3A-Sinn.
- **SOV-3-05 Client-Side Encryption**: Wie oben erörtert, erfüllen CMK den Anforderungen nicht. Tokenization on-premises oder External Key Management (HYOK) sind die architektonischen Antworten.
- **SOV-2-01 Extraterritorial Risk Assessment**: Microsoft publiziert Transparency Reports, das jährliche strukturierte Risk Assessment liegt aber beim Kunden.
- **SOV-5-01 SBOM mit Herkunft**: Microsofts Transparency Reports erfüllen das TR-03183-Qualitätsniveau in der geforderten Form heute nicht.

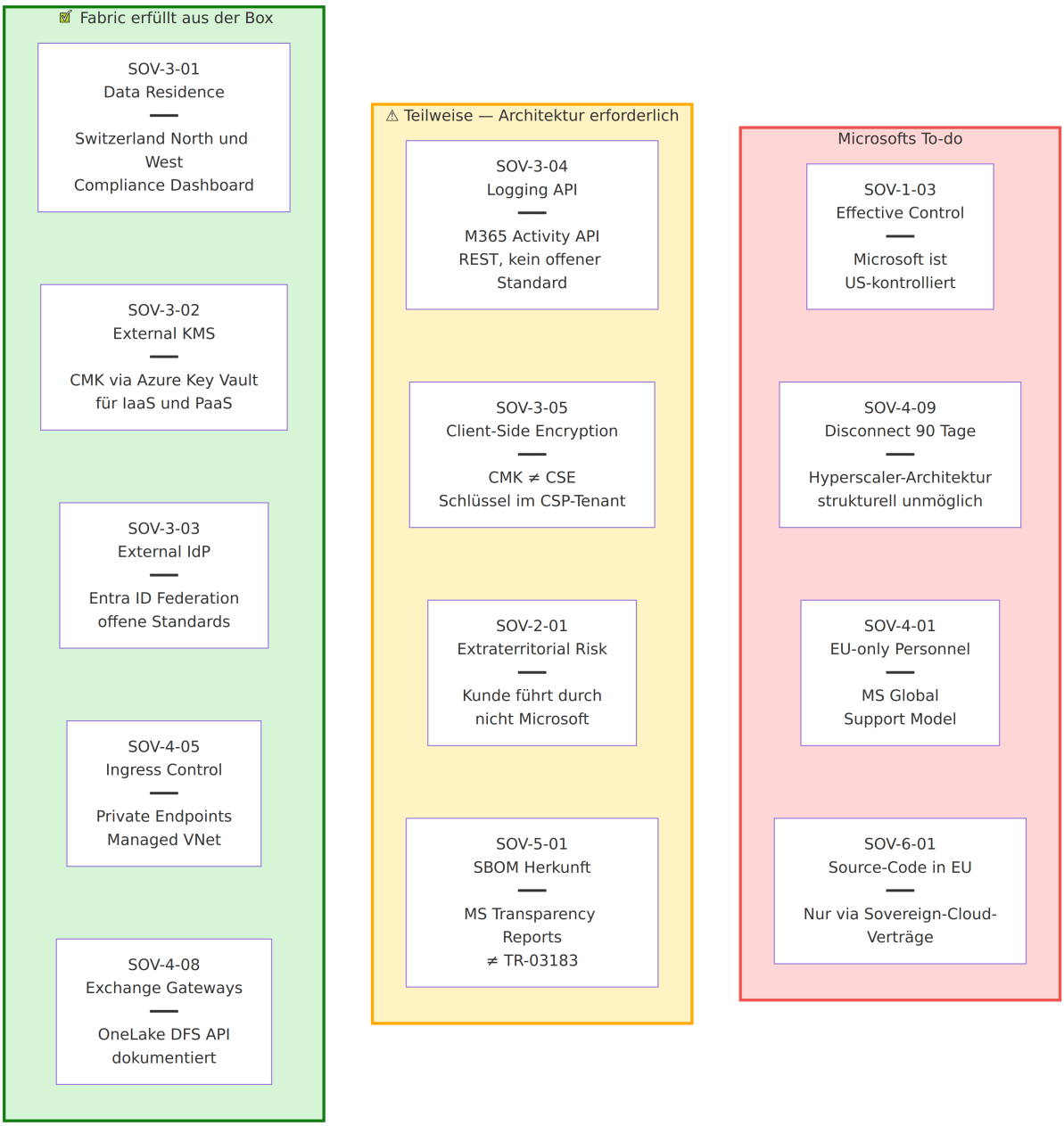

Abbildung 3.1: Coverage-Matrix — was Fabric in Switzerland North heute aus der Box erfüllt (grün), was Architektur-Arbeit erfordert (gelb) und was kommerzielle Fabric strukturell nicht liefert (rot, “Microsofts To-do”).

3.3 Was kommerzielle Fabric strukturell nicht liefert

- **SOV-1-03 Effective Control durch EU-Unternehmen**: Microsoft Corporation ist US-kontrolliert. Adressiert wird das durch Microsoft EU Sovereign Cloud, Bleu (Frankreich), Delos (Deutschland) und ähnliche Initiativen.
- **SOV-4-09 Disconnect 90 Tage**: Die Hyperscaler- Architektur ist strukturell auf permanente globale Konnektivität ausgelegt.
- **SOV-4-01 EU-only Personnel**: Microsoft betreibt ein globales Support-Modell mit Operations-Personal weltweit.
- **SOV-6-01 Source-Code in EU**: Source-Code-Backup mit 24-Stunden-Frische in der EU ist nur über Sovereign-Cloud- Verträge möglich, nicht im kommerziellen Standard-Fabric.

Was diese Coverage-Matrix nicht ist

Die Matrix ist keine Verkaufs-Folie für Microsoft Sovereign Cloud. Wer dorthin geht, deckt mehr Kriterien ab — zahlt aber anderswo (Feature-Lag von typischerweise mehreren Monaten gegenüber commercial Azure, höhere Kosten, eingeschränkte Region-Coverage). Das ist Architektur-Arbeit, nicht Produkt-Wechsel.

4

Der Sovereignty Stack — fünf Schichten

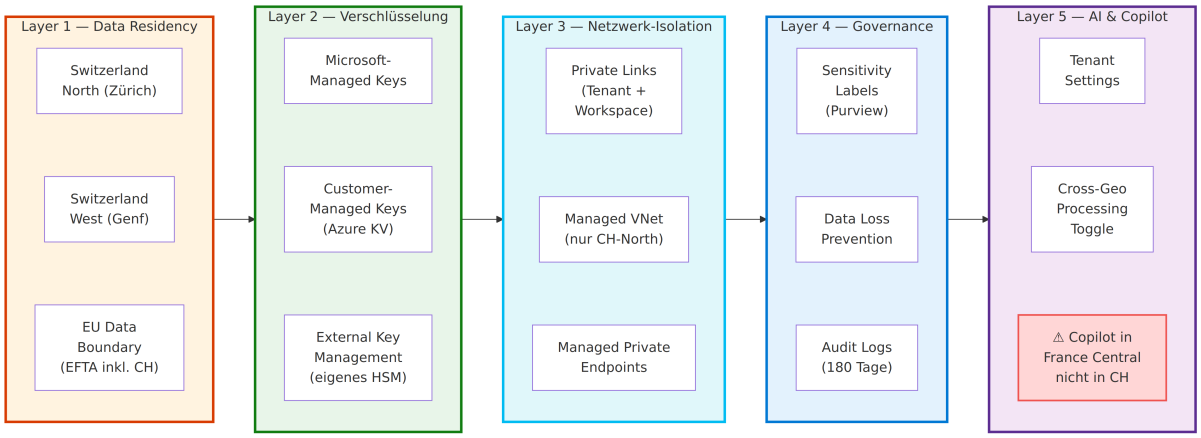

Abbildung 4.1: Fabric Sovereignty Stack — gelesen von links (Fundament: Data Residency) nach rechts (jüngste Schicht: AI Controls). Jede Schicht baut auf der vorhergehenden auf, jede ist auch einzeln aktivierbar, und jede hat ihre Trade-offs.

4.1 Layer 1 — Data Residency

Switzerland North (Datacenter Zürich) und Switzerland West (Genf) als physische Region-Optionen. EU Data Boundary deckt EFTA inklusive Schweiz ab, was eine wichtige rechtliche Klärung darstellt.

Wichtig: Die Region wird bei der Workspace-Erstellung festgelegt und ist **nicht nachträglich änderbar**. Eine Migration zwischen Schweizer Regionen ist möglich, aber aufwendig.

4.2 Layer 2 — Verschlüsselung

Drei Eskalationsstufen:

1. **Microsoft-Managed Keys**: Default. Microsoft erzeugt, rotiert, schützt die Schlüssel.
2. **Customer-Managed Keys (CMK)**: Schlüssel im Azure Key Vault. Pflicht-Settings: Soft-Delete + Purge-Protection. Fabric-Identität braucht Wrap- und Unwrap-Rechte; niemals Purge oder Delete.
3. **External Key Management (EKM, HYOK)**: Schlüssel im eigenen HSM (z. B. Thales, Fortanix, Azure KV Managed HSM). Fabric ruft Unwrap über eine Policy-Bridge — die Netzwerk-Latenz wird Teil jeder Query.

Jeder Sprung gibt mehr Kontrolle, kostet mehr Operations-Last und erhöht Latenzen.

4.3 Layer 3 — Netzwerk-Isolation

Private Links eliminieren Public-Internet-Hops zwischen Tenant- und Workspace-Endpoints. **Managed VNet** isoliert Workspace-Egress vollständig — aber nur in Switzerland North, *nicht* in Switzerland West. Diese Region-Asymmetrie zwingt regulierte Workloads de facto nach CH-North.

Managed Private Endpoints erlauben kontrollierte Verbindungen zu definierten Sinks. **Tenant Restriction** mit Conditional Access plus Private Link Workspace Access erlaubt Zugriff nur aus dem Corporate-Netzwerk.

4.4 Layer 4 — Governance (Microsoft Purview)

Sensitivity Labels wandern mit den Daten und triggern Verhaltensrichtlinien. **Data Loss Prevention** verhindert unkontrollierte Exfiltration. **Audit Logs** dokumentieren Zugriffe.

Audit-Log-Retention

Die 180-tägige Default-Retention der Fabric-Audit-Logs reicht weder für Finma-Anforderungen noch für SOV-2-Audit-Rechte. Spiegelung in Microsoft Sentinel oder Splunk ab Tag 1 ist Pflicht, nicht Kür.

4.5 Layer 5 — AI & Copilot Controls

Tenant-Setting "Users can use Copilot" — darunter Security Groups — darunter Capacity-Enable/Disable — darunter Cross-Geo-Processing-Flag. Eine Kaskade von vier Hebeln, kein Workspace-weiser Opt-out.

Fabric Copilot läuft nicht in der Schweiz

Stand April 2026: Fabric Copilot wird für EU-Mandanten in France Central, für US-Mandanten in East US oder South Central US inferiert. **Es gibt keine CH-Inferenz-Region für Fabric Copilot.**
Wer strenge CH-Residenz braucht, muss Copilot bewusst deaktivieren oder über ein eigenes Azure OpenAI-Deployment in Switzerland North arbeiten (GPT-4o, GPT-4.1, o1/o3-Familie). Das gibt kein Copilot-Erlebnis, aber die volle Kontrolle.

5

Die Architektur-Antwort: Zwei-Zonen-Modell

Die Frage ist: Was machen wir mit der roten Spalte der Coverage-Matrix? Es gibt drei Antworten — zwei sind falsch, eine ist richtig.

5.1 Zwei falsche Antworten

1. “Dann eben kein Fabric.” — Sie verlieren OneLake, Direct Lake, Copilot, das ganze Ökosystem. Sie bauen einen handgemachten Stack. Den können Sie auch nicht souverän halten — Sie haben einfach das Problem auf Ihre eigenen Schultern gelegt.
2. “Microsoft Sovereign Cloud löst das.” — Adressiert mehr von der roten Spalte, ja. Aber Sie zahlen Feature-Lag, höhere Kosten, eingeschränkte Region-Coverage. Und vertrauen am Ende immer noch demselben Anbieter — nur mit einem anderen Vertrag.

5.2 Die richtige Antwort: Zwei Zonen, ein Gateway

Die Public Zone ist Fabric in CH-North mit allen SOV-3- und SOV-4-Kontrollen, die Sie schon kennen. Die Restricted Zone ist on-premises mit den Klartext-PII. Das Gateway tokenisiert dazwischen.

Schlüssel-Erkenntnis: Nicht alles muss in die Public Zone. Aggregierte Reports, Trends, Mengen — ja. Klartext-PII, die für Re-Identifikation nutzbar wäre — nie. Das ist Data Minimization als Architektur-Prinzip, nicht als Versprechen.

5.3 C3A-Mapping dieses Patterns

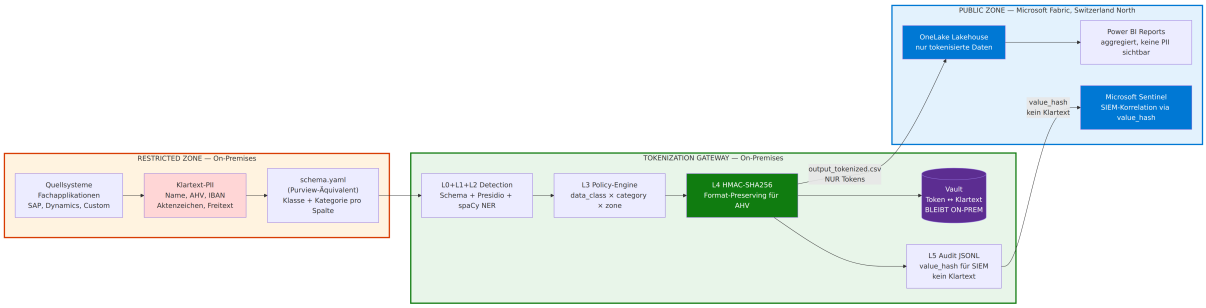

Abbildung 5.1: Zwei-Zonen-Modell mit Tokenization Gateway. Klartext-PII bleibt in der Restricted Zone on-premises. Das Gateway tokenisiert. Die Public Zone (Microsoft Fabric in Switzerland North) sieht nur Tokens. Der Vault verlässt den Perimeter niemals.

Tabelle 5.1: Wie das Zwei-Zonen-Modell C3A-Kriterien adressiert

Kriterium	Status	Mechanismus
SOV-3-05 Client-Side Encryption	funktional	HMAC-SHA256 mit Pepper im Gateway, Tokens in Cloud
SOV-3-04 Logging Real-time	erfüllt	Audit-JSONL mit dokumentiertem Schema, value_hash
SOV-4-07 Data Exchange Monitor	erfüllt	Pro Zelle: Layer, Recognizer, Entity, Policy, Confidence
SOV-4-08 Data Exchange Gateway	erfüllt	Genau eine Schnittstelle: `fabric_upload.py`

6

Three-Axis Policy — wie das Gateway entscheidet

Die zentrale Innovation des Tokenization-Gateways ist nicht die Tokenisierung selbst (HMAC ist seit Jahren Stand der Technik), sondern die **Drei-Achsen-Policy** pro Datenzelle.

6.1 Die drei Achsen

`data_class` Wie sensitiv ist die Spalte? `public`, `internal`, `confidential`, `strict_confidential`.

`data_category` Was für Daten sind das? `pii`, `financial`, `free_text`, `metadata`.

`target_zone` Wohin sollen die Daten? `public` (z. B. Power BI Reports für externe Sicht) oder `internal_analytics` (interne Analyse hinter der Firewall).

6.2 Selbe Detection — andere Aktion

Konkretes Beispiel

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 unverändert durchgereicht — weil interne Analytics Ihr eigener Perimeter ist, dem Sie schon vertrauen.
Detection ≠ Decision.

6.3 Vier Aktionen

1. `TOKENIZE`: voller Cell-Hash mit HMAC-SHA256.
2. `MASK`: Span im Freitext mit Block-Zeichen ersetzen.
3. `REVIEW`: Mid-Konfidenz-Treffer kommen in eine menschliche Review-Queue.
4. `PASS`: kein Eingriff.

Jede Entscheidung wird mit einer Rule-ID im Audit-Log persistiert. Das System ist **first-match-wins**: Die Reihenfolge der Regeln *ist* die Policy, nicht ein 800-seitiges Compliance-Manual.

7

Die Live-Demo: TokenDemo

Die Live-Demo der Session demonstriert die obigen Konzepte als ausführbaren Code. Sie können das Repository hier clonen:

```
git clone https://dev.connect-me.ch/coso/2026-04-spie-xspierience.git
cd 2026-04-spie-xspierience
uv sync
uv run streamlit run app.py
```

7.1 Sechs Layer, eine CSV

Tabelle 7.1: Die sechs Layer der TokenDemo-Pipeline

Layer	Mechanismus	Zweck
L0 Schema	`schema.yaml`	Purview-Äquivalent: Klasse + Kategorie pro Spalte
L1 Patterns	Microsoft Presidio mit CH-Recognizern	AHV mod-10, IBAN mod-97, ISO-Kantonscode
L2 NER	spaCy `de_core_news_lg`	Erkennt Personen-Namen in Freitext-Spalten
L3 Policy	YAML, first-match-wins	Drei-Achsen-Entscheidung pro Detection
L4 Tokenizer	HMAC-SHA256, Format-Preserving für AHV	Token-Erzeugung; Vault als CSV-Mapping
L5 Audit	JSONL	Eine Zeile pro (Detection, Decision); SIEM-tauglich

7.2 Sieben Schweizer Demo-Datensätze

Die Demo arbeitet auf sieben handverlesenen Records, die zusammen die Drei-Achsen-Logik demonstrieren:

- **R-0001 / R-0002**: `vertraulich` → `public`. Volle Tokenisierung aller PII-Felder.
- **R-0003**: `streng_vertraulich` → `public`. Strikte Regel R-001 maskiert auch zwei Personennamen im Freitext.
- **R-0004 / R-0006**: `intern` → `internal_analytics`. Kein Eingriff (PASS).
- **R-0005**: NER findet "Hr. Nguyen-Fischer" im Freitext — ein Name, den die L1-Patterns nie gesehen hätten.
- **R-0007**: Mid-Konfidenz-NER-Treffer "Hyazinth Brönni…" geht in den REVIEW-Pfad.

7.3 Was die Demo C3A-konform leistet

C3A-Mapping der TokenDemo

- **SOV-3-05 Client-Side Encryption** (funktional): Klartext-PII wird on-prem durch HMAC-SHA256 ersetzt; der Pepper hat das Gateway nie verlassen.
- **SOV-3-04 Logging Real-time API**: `audit.jsonl` mit dokumentiertem Schema; `value_hash` ist SHA-256 des Klartextes auf 16 Hex-Zeichen abgeschnitten — 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.
- **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.

7.4 Was die Demo nicht zeigt — bewusst weggelassen

Für eine produktive Implementierung sind folgende Erweiterungen nötig:

- Echte Format-Preserving Encryption (FF1/FF3 nach NIST SP 800-38G) statt des HMAC-Hash-Hacks.
- Pepper im HSM (Azure KV Managed HSM, Thales, Fortanix) statt als File neben dem Vault.

- Detoken-Service als gesicherter API-Endpunkt mit Mehraugenprinzip und Just-in-Time-Access.
- CDC/Streaming via Debezium plus Kafka in der Restricted Zone statt einmaligem CSV-Read.
- Open Policy Agent (Rego) statt der 30-Zeilen-Python-Engine.

8

Architektur-Entscheidungsbaum

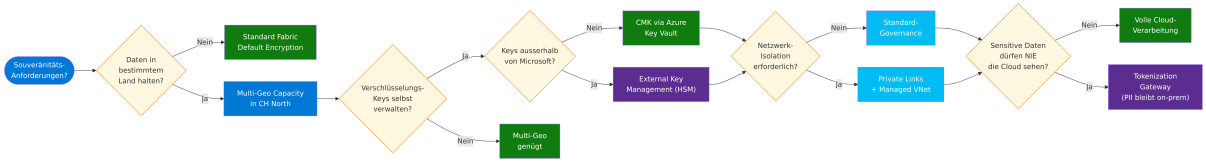

Abbildung 8.1: Architektur-Entscheidungsbaum — fünf Fragen, ein Pfad von Souveränitäts-Anforderung zu konkreter Architektur. Mit Ihrem CISO durchgehen.

Die fünf Fragen, links nach rechts:

1. **Müssen die Daten in einem bestimmten Land bleiben?** Ja → Multi-Geo Capacity in CH-North. Nein → Standard Fabric mit Default-Encryption ist eine valide Antwort.
2. **Wollen Sie die Verschlüsselungs-Schlüssel selbst verwalten?** Ja → Customer-Managed Keys via Azure Key Vault. Nein → Multi-Geo allein genügt für Datenresidenz.
3. **Müssen die Schlüssel ausserhalb von Microsoft liegen?** Ja → External Key Management mit eigenem HSM. Nein → Azure Key Vault CMK ist ausreichend.
4. **Brauchen Sie Netzwerk-Isolation?** Ja → Private Links plus Managed VNet (Achtung: Managed VNet nur in CH-North). Nein → Standard-Governance.
5. **Dürfen sensitive Daten NIE die Cloud sehen?** Ja → Tokenization Gateway, was wir gerade gesehen haben. Nein → volle Cloud-Verarbeitung mit den oben gewählten Kontrollen.

Die meisten Schweizer Enterprises landen auf der mittleren Achse: Q3 ja, Q4 ja, Q5 nein. Das ist Fabric mit CMK, Private Links und CMK-Management.

Banking, GWG-relevante Daten, einzelne Gesundheits-Szenarien sowie Verteidigungs-Kontexte landen rechts beim Tokenization-Pattern.

9

Fünf Takeaways

1. **C3A als Self-Assessment durchgehen.** Pro SOV-Dimension dokumentieren, wo Ihre heutige Architektur steht — grün, gelb, rot. Eine Tagesarbeit, kein Projekt. Output: ein Aufhänger für jede Architektur-Diskussion der nächsten zwölf Monate.
2. **Microsoft Fabric in Switzerland North bleibt der richtige Ausgangspunkt.** CMK plus Private Endpoints plus Purview Sensitivity Labels ab Tag 1. Das deckt die grüne Hälfte von C3A out-of-the-box ab — und das ist beachtlich.
3. **Zwei-Zonen-Modell mit Tokenization Gateway,** sobald Sie Daten haben, die SOV-3-05 oder SOV-4-09 strikt verlangen — Bankgeheimnis, Geldwäscherei-Daten, Gesundheits-Datensätze, Verteidigungs-Kontext. Pseudonymisierungs-Schlüssel im On-Prem HSM, nicht in Azure Key Vault.
4. **Three-Axis Policy als operatives Prinzip** für die Datenplattform: `data_class`, `data_category`, `target_zone`. Keine binären "Cloud ja/nein"- Entscheidungen mehr — pro Zelle, dokumentiert, auditierbar.
5. **Vault on-prem, Audit überall.** Die Cloud sieht nur Tokens. Audit-Logs spiegeln in Sentinel oder Splunk — die 180 Tage Default-Retention von Fabric reichen 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.

A

Vollständiges C3A-Kriterien-Mapping

Die folgende Tabelle listet alle relevanten C3A-Kriterien aus SOV-1 bis SOV-6 mit ihrem Status für commercial Microsoft Fabric in Switzerland North.

Tabelle A.1: Vollständiges C3A-Mapping für commercial Microsoft Fabric (Stand April 2026)

Kriterium	Status	Anmerkung
SOV-1-01 EU-Jurisdiktion	🔴	Microsoft Corporation, US-Hauptsitz
SOV-1-02 Registered Office	🔴	US-Hauptsitz; EU-Tochter Microsoft Ireland
SOV-1-03 Effective Control	🔴	US-kontrolliert
SOV-1-04 Control Change Notice	🟢	Microsoft kommuniziert wesentliche Änderungen
SOV-2-01 Extraterritorial Risk	🟠	Risk Assessment ist Kunden-Pflicht
SOV-2-02 Audit Rights	🟠	Über C5 und SOC2 Type 2 möglich
SOV-2-03 State of Defense Takeover	🔴	Vertraglich nicht abgebildet
SOV-3-01 Data Residence	🟢	Switzerland North/West, Compliance Dashboard
SOV-3-02 External KMS (IaaS/PaaS)	🟢	CMK via Azure Key Vault
SOV-3-02-AC External KMS (SaaS)	🟠	Selektive Coverage über Fabric-SaaS
SOV-3-03 External Identity Provider	🟢	Entra ID Federation, offene Standards
SOV-3-04 Logging & Monitoring	🟠	M365 Activity API, kein offener Standard
SOV-3-05 Client-Side Encryption	🔴	CMK $\neq$ CSE; Schlüssel im CSP-Tenant
SOV-4-01 EU-Personnel	🔴	Globales Microsoft Support Model
SOV-4-02 Remote Work EU-only	🔴	Globaler Admin-Zugriff
SOV-4-03 Redundant Connectivity	🟢	Multi-Provider, Azure Backbone
SOV-4-04 EU-SOC	🟠	MS Defender SOCs global
SOV-4-05 Ingress Data Control	🟢	Private Endpoints, DMZ-Pattern
SOV-4-06 Update Threat Analysis	🟢	MSRC Risk-Based Security Process
SOV-4-07 Data Exchange Monitor	🟢	Documented gateways
SOV-4-08 Data Exchange Gateways	🟢	OneLake DFS, Documented Endpoints
SOV-4-09 Disconnect 90 Tage	🔴	Hyperscaler-Architektur strukturell unmöglich
SOV-4-10 Reconnect	🔴	Hängt von SOV-4-09 ab
SOV-5-01 Software Dependencies	🟠	MS Transparency Reports $\neq$ TR-03183
SOV-5-02 Hardware Dependencies	🟠	MS Datacenter Hardware Disclosures
SOV-5-03 External Service Deps	🟠	Subprocessor List veröffentlicht
SOV-5-04 Export Restriction	🟢	US Export Control Compliance dokumentiert
SOV-5-05 Capacity Mgmt	🔴	Globales Capacity Management
SOV-6-01 Source Code in EU	🔴	Nur via Sovereign-Cloud-Verträge
SOV-6-02 Continuous Service Delivery	🔴	Hängt von Microsoft Engineering ab
SOV-6-03 Software Development	🔴	Microsoft-internes Build/Deploy

Legende: ● erfüllt, ● teilweise, ● nicht erfüllt.

B

Glossar

BSI Bundesamt für Sicherheit in der Informationstechnik (Deutschland).

C3A
: Criteria enabling Cloud Computing Autonomy. BSI-Kriterienkatalog v1.0 vom 27.04.2026.

C5 Cloud Computing Compliance Catalogue. BSI-Sicherheits-Standard, Version 2026 ist die aktuelle.

CMK
: Customer-Managed Keys. Verschlüsselungs-Schlüssel im Azure Key Vault, vom Kunden verwaltet.

CSE Client-Side Encryption. Verschlüsselung mit einem Schlüssel, der die CSP-Umgebung niemals betritt.

CSF Cloud Sovereignty Framework. EU-Vorlage für nationale Souveränitäts-Frameworks.

CSP
: Cloud Service Provider.

DLP Data Loss Prevention. Technische und organisatorische Massnahmen gegen unkontrollierten Datenabfluss.

EKM
: External Key Management. Schlüsselverwaltung in einem HSM ausserhalb der CSP-Umgebung.

EU CSF
: EU Cloud Sovereignty Framework.

EU Data Boundary
: Microsofts Compliance-Programm zur Datenverarbeitung in der EU/EFTA.

FPE Format-Preserving Encryption. Verschlüsselung, die das Format der Eingabe erhält (z. B. AHV-Nummer bleibt 13 Ziffern). NIST SP 800-38G definiert FF1 und FF3.

HMAC
: Hash-based Message Authentication Code. Hier: SHA-256-basierter Tokenisierungs-Mechanismus.

HSM
: Hardware Security Module. Tamper-resistant Hardware für Schlüssel-Verwaltung.

HYOK
: Hold Your Own Key. Variante von EKM mit lokalem HSM-Betrieb.

IBAN
: International Bank Account Number. Mod-97-Validierung gegen Tippfehler und Manipulation.

NER
: Named Entity Recognition. ML-basierte Erkennung von Entitäten in Freitext.

OneLake
: Microsoft Fabrics einheitliche Datenebene auf Azure Data Lake Storage Gen2.

Presidio
: Microsoft-Bibliothek für PII-Erkennung und -Anonymisierung.

Purview
: Microsoft Compliance- und Governance-Plattform.

SBOM
: Software Bill of Materials. Liste aller Software-Komponenten mit Herkunftsangaben.

TR-03183
: BSI-Spezifikation für SBOM-Qualität.

Vault
: Speicher für Token-zu-Klartext-Zuordnungen. In der TokenDemo eine CSV-Datei, in Production eine sicherheitsgehärtete Datenbank.

C

Weiterführende Ressourcen

C.1 Primärquellen

- BSI: *C3A — Criteria enabling Cloud Computing Autonomy*, v1.0, 27.04.2026.
  https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/C3A_Cloud_Computing_Autonomy.pdf
- BSI: *C5 — Cloud Computing Compliance Catalogue*, Edition 2026.
  https://www.bsi.bund.de/EN/Topics/CloudComputing/Compliance_Criteria_Catalogue/Compliance_Criteria_Catalogue_node.html
- BSI: *TR-03183 — Cyber Resilience Requirements for Manufacturers and Products*.
  https://www.bsi.bund.de/dok/TR-03183
- Europäische Kommission: *Cloud and Edge Computing Strategy*.
  https://digital-strategy.ec.europa.eu/en/policies/cloud-computing

C.2 Microsoft Fabric — Souveränität und Sicherheit

- Microsoft Learn: *Microsoft Fabric Region Availability*.
  https://learn.microsoft.com/fabric/admin/region-availability
- Microsoft Learn: *Customer-Managed Keys for Microsoft Fabric*.
  https://learn.microsoft.com/fabric/security/security-customer-managed-keys
- Microsoft Learn: *Private Endpoints for Microsoft Fabric*.
  https://learn.microsoft.com/fabric/security/security-private-links-overview
- Microsoft Learn: *Managed Virtual Networks for Microsoft Fabric*.
  https://learn.microsoft.com/fabric/security/security-managed-vnets-fabric-overview
- Microsoft: *EU Data Boundary Overview*.
  https://learn.microsoft.com/privacy/eudb/eu-data-boundary-overview

C.3 Open-Source-Bausteine der TokenDemo

- Microsoft Presidio (PII Detection & Anonymization).
  https://github.com/microsoft/presidio
- spaCy `de_core_news_lg` (Deutsches NER-Modell).
  https://spacy.io/models/de#de_core_news_lg
- NIST SP 800-38G — Format-Preserving Encryption.
  https://csrc.nist.gov/publications/detail/sp/800-38g/final

C.4 Live-Demo Source Code

- TokenDemo Repository (Forgejo, public-read):
  https://dev.connect-me.ch/coso/2026-04-spie-xspierience

C.5 Weitere Inhalte vom Speaker

- Landing Page zur Session inkl. weiterführender Materialien:
  https://www.the-trusted-advisor.com/events/2026-04-28-spie-xspierience-data-sovereignt
- Fabric Friday auf YouTube: https://youtube.com/@The-Trusted-Advisor
- Copilot-Cockpit (Governance & Guardrails): https://www.copilot-cockpit.com
- LinkedIn: https://www.linkedin.com/in/matthias-falland/