



Digitale Souveränität für Österreich

Warum sich digitale Handlungsfähigkeit am Endgerät entscheidet



07:42 – ein ganz gewöhnlicher Dienstag



Wer hätte an diesem Dienstag die Kontrolle über Ihre Endgeräte gehabt?

Endgeräte im öffentlichen Sektor



Öffentliche Verwaltung

Notebooks · Tablets · Ausweislesegeräte



Einsatzorganisationen

Digitalfunk · Rugged Tablets · Bodycams



Gesundheit & Rettung

Visitentables · Fahrzeugterminals · Scanner



Verkehr & Mobilität

Handhelds · Bordrechner · Leitstellentechnik



Energie & Wasser

Wartungstablets · Rugged Devices · Sensorik



Flughafen & Grenze

Dokumentenleser · Handhelds · RFID/NFC

**In der Diskussion über „Digitale Souveränität“
geht es nicht um technologische Autarkie,
sondern um autonomes Handeln.**

Digitaler Aktionsplan „Digitale Souveränität für Österreich“ · BMF / Digital Austria, 2023

Kriterien digitaler **Kontrolle und Unabhängigkeit**



Datenhoheit

- Schutz sensibler Daten
- Zugriffskontrollen
- Verschlüsselung
- Compliance

**Ziel: Schutz vor
Datenabwanderung**



Datenresidenz

- Kontrolle über Datenflüsse
- Verarbeitung im eigenen Rechtsraum
- Schutz vor extraterritorialen Zugriffen

**Ziel: Kontrolle über Daten
und Rechtsraum**

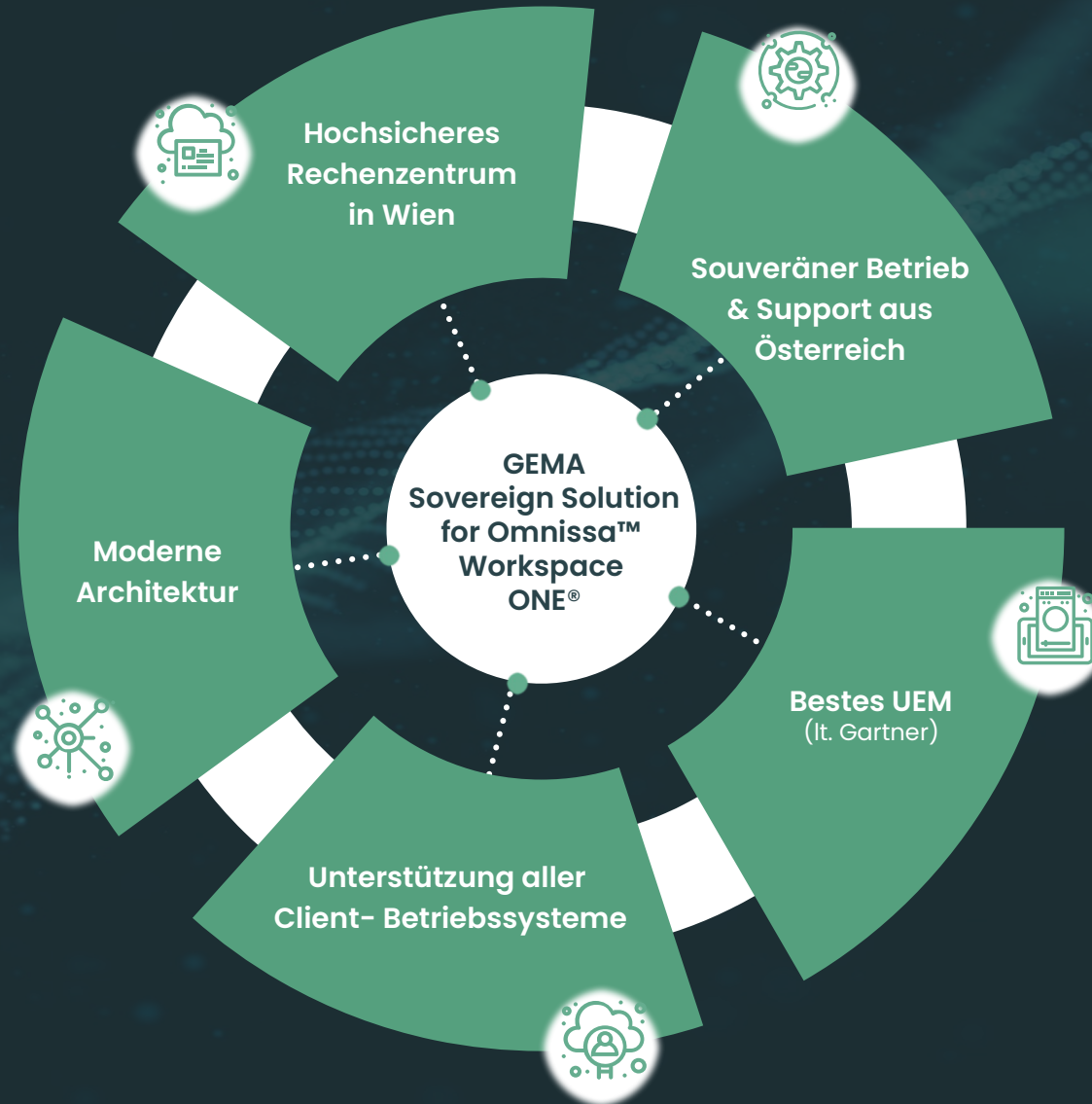


Betriebssouveränität

- Plattform bleibt ohne Hersteller handlungsfähig
- Business Continuity
- Betrieb bleibt im eigenen Einflussraum möglich

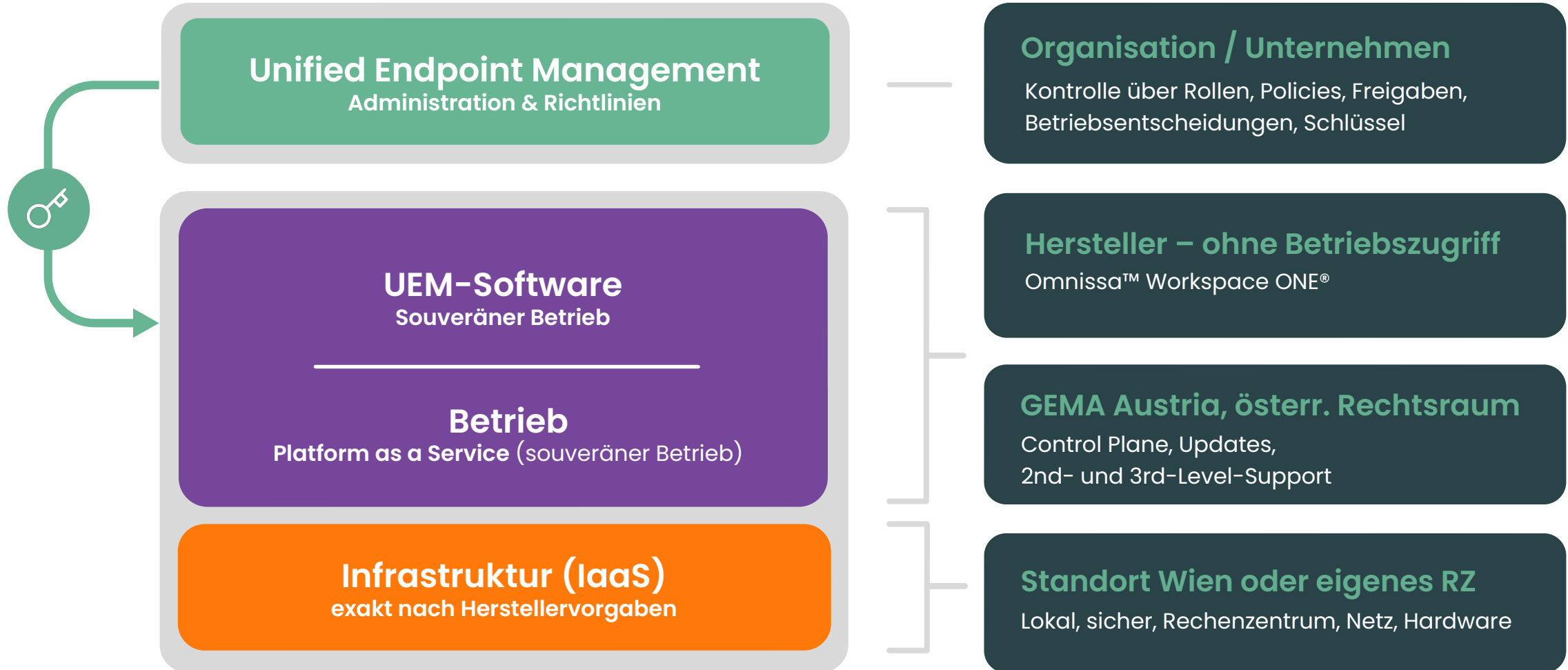
**Ziel: Sicherstellung der
operativen Steuerungsfähigkeit**

Souveräne Lösung für Österreich



**Haben wir die Kontrolle über
sicherheitskritische UEM-Daten
und deren Schutzmechanismen?**

Architektur im Überblick: Gewaltenteilung



**Bleiben unsere UEM-Betriebsdaten innerhalb
des österreichischen Rechts- und Hoheitsraums?**

Eine Frage der Kontrolle

Derselbe Rechtsraum. Zwei Architekturen.

Konventionell

Extraterritorialer Hersteller

liefert und betreibt Software

Befehl von außen



UEM in Hersteller-Cloud



Endgeräte-Daten



Endgeräte

ÖSTERREICHISCHER RECHTSRAUM

Souverän

Extraterritorialer Hersteller

liefert Software

Kein Zugriff



hostet und betreibt



Endgeräte-Daten



UEM



Endgeräte

ÖSTERREICHISCHER RECHTSRAUM



„Darf nicht zugreifen“ ist eine Regel.

„Kann nicht zugreifen“ ist Architektur.

**Sind wir auch bei Ausfall oder Dienstsperre
des UEM handlungsfähig?**

Handlungsfähig, auch ohne Hersteller

Angenommen, die Hersteller-Cloud ist nicht erreichbar oder der Mandant ist gesperrt:
Was funktioniert dann noch?

	Konventioneller Betrieb	Souveräner Betrieb
Neue Geräte in Betrieb nehmen	✗	✓
Richtlinien und Compliance durchsetzen	✓ ✗	✓
Zertifikate ausstellen und erneuern	✗	✓
Fachanwendungen (z.B. ELAK) bereitstellen und entziehen	✗	✓
Verlorene Geräte sperren und löschen	✗	✓
2nd- und 3rd-Level-Support leisten	✗	✓

Zur Einordnung: Betriebssystem-Updates und App-Stores liegen weiter bei Apple und Google. Souveränität ist keine Autarkie. Souveränität sorgt dafür, dass die Steuerung Ihrer Geräte unabhängig bleibt.

Was bedeutet das für uns?



Ein Zugang. **Fünf Vollmachten**



Fernlöschung

Ein Kommando · tausende Geräte · sofort wirksam



Richtlinien-Push

Konfigurationen · Restriktionen · ohne Zutun der Nutzenden



Zertifikate

Schlüsselverteilung · steuert jede Authentifizierung



Applikationen

Verteilen · entziehen · sperren – auch im Einsatz



Compliance

Richtlinienerfüllung · Offline Umsetzung von Sicherheitsvorgaben

Wer die UEM-Konsole kontrolliert, kontrolliert die Flotte. Unabhängig vom Speicherort der Daten.

Architektur Checkliste



Datenhoheit

Technische Souveränität

- Administrative Kontrolle
- Control-Plane-Souveränität
- Kryptografische Kontrolle
- Richtlinien- und Compliance-Kontrolle



Datenresidenz

Datensoeveränität

- Datenklassifikation
- Datenverarbeitung
- Rechtsraum und Betreiberstruktur
- Mandantentrennung



Betriebssouveränität

Operative Souveränität

- Betrieb ohne Hersteller
- Betriebsmodell
- Notfall- und Wiederanlauf-konzepte



Heiko Friedrich

oss@at.thegema.com



Souveränes Endgeräte-Management
in sicherheitskritischen Umgebungen