

Telematikinfrastruktur 2.0

Anhang Servicekatalog (SK) zur Leistungsbeschreibung

Los 1 – Anwendungen und Los 2 – Cloud Services

Anlage-02b der Vergabeunterlagen

**2026-0030 TI-Flow - Entwicklung, Bereitstellung und Betrieb
eines Workflow Fachdienstes, sowie der Aufbau und Betrieb
einer sicheren Infrastruktur-Plattform in der TI**

Version: 1.0.0
Stand: 14.10.2026
Klassifizierung: öffentlich

Inhaltsverzeichnis

Inhaltsverzeichnis	2
1 Service Katalog	3
1.1 Allgemeine Infrastruktur- und Plattformdienste	4
1.2 HCC-spezifische Leistungen	8

1 Servicekatalog

Diese Anlage definiert den Mindestumfang an Services, welche der HCC-Provider (AN Los 2) in seinem Servicekatalog anbieten muss und welche für die Umsetzung der TI-Flow HCC-Dienste durch den AN Los 1 zu verwenden sind. Als optional gekennzeichnete Services sind beispielhafte Erweiterungen des Mindestumfangs.

Services, die nicht als optional gekennzeichnet sind, werden vom HCC-Provider (AN Los 2) verbindlich bereitgestellt. Der Betreiber von HCC-Diensten (AN Los 1) darf deren Verfügbarkeit seiner Leistungserbringung zugrunde legen und diese entsprechend fest einplanen.

Der Katalog gliedert sich in zwei Teile:

1. Allgemeine Infrastruktur- und Plattformdienste ohne Confidential Computing Eigenschaften
2. HCC-spezifische Leistungen

Die genannten Technologien und Schnittstellen sind verbindliche Kompatibilitätsanforderungen. Services und Anforderungen sind verpflichtend, sofern nicht mit „optional“ gekennzeichnet.

Der AN Los 2 muss in seinem Servicekatalog beschreiben, welche Services als Standardleistungen verfügbar sind und welche Leistungen zusätzlich beauftragt werden können. Der AN muss beschreiben, welche Leistungsmerkmale, Betriebsmodelle und Service Levels für die jeweiligen Services gelten.

1.1 Allgemeine Infrastruktur- und Plattformdienste

Kategorie	Service	Abrechnungsmetrik durch HCC-Cloud	Anforderungen an HCC-Cloud	Nutzung für HCC-Dienst verpflichtend
Compute	Virtuelle Maschinen	vCPU / RAM pro Stunde	- Mehrere Leistungsklassen - Eine Leistungsklasse vergleichbar XENON Gold - Autoscaling - Update- und Patch-Management für OS-Images - Bereitstellung der OS-Images durch Kunden (optional)	
	Dedicated Hosts	Host je Monat	- Physischer Server exklusiv für einen Mandanten - Dynamisch provisionierbar, keine feste Hardwarereservierung. - Mehrere Leistungsklassen	
Storage	Block-Storage	GB je Monat je Klasse, Snapshot-Speicher	- Snapshots - Performance-Klassen	
	Object Storage	GB je Monat, Requests, Traffic	- Multi-Availability-Zone - S3-compatible API - Object-Versionierung - Object-Lock	
	Backup und Recovery	Backup-Speicher GB je Monat	Wiederherstellbarkeit von VMs und Volumes	
Container und Orchestrierung	Managed Kubernetes	Cluster je Stunde, Nodes gemäß Compute	- Control Plane durch den Auftragnehmer betrieben, verteilbar über mehrere Availability Zones - Node Pools über Availability Zones verteilbar, Cluster Autoscaler - Nodes nach Leistungsklassen konfigurierbar - Netzwerkregeln zwischen Pods durchsetzbar - Persistente Volumes mit Verschlüsselung und Snapshots	

Kategorie	Service	Abrechnungsmetrik durch HCC-Cloud	Anforderungen an HCC-Cloud	Nutzung für HCC-Dienst verpflichtend
			- Zulässige Workloads durch Regeln des Auftraggebers technisch durchgesetzbar (Policy as Code, Pod Security Standards) - Konsistente Wiederherstellbarkeit von Workloads und Volumes inkl. persistenten Ressourcen	
	Container Registry	Speicher GB je Monat, Traffic	- OCI-konform - Public Registries - Private Registries mit Access Control	
	Service Mesh	Produkt-spezifisch	- optional - Integration in Managed Kubernetes ohne Anwendungsänderung - Verschlüsselte und beidseitig authentifizierte Kommunikation zwischen Diensten (mTLS) mit automatischer Zertifikatsausstellung und -rotation - Observability Daten für Kunden exportierbar	
Netzwerk	Load Balancer	Per Instanz per Monat, Traffic	- Layer 4 und Layer 7 - Verteilt über mehrere Availability Zones, kein Single Point of Failure - Automatisches Failover auf verfügbare Ziele und Availability Zones	Muss genutzt werden
	DNS	Je Zone per Monat, Anfragen/Traffic	- Zonen-Verwaltung durch Kunden - Public und Private Zonen - Unterstützung von Fail-Over Mechanismen (optional)	Muss genutzt werden
	Site-to-Site VPN	Je Verbindung per Monat, Traffic	- optional - Verschlüsselte Anbindung von Fremdnetzen über das Internet, Verschlüsselung nach Stand der Technik	
	Anti-DDoS	Produktspezifisch	- Erkennung und automatische Abwehr von Angriffen auf Netzwerk- und Transportebene (Layer 3 und 4) - Schutz aller öffentlichen IP-Adressen und Endpunkte	Muss genutzt werden

Kategorie	Service	Abrechnungsmetrik durch HCC-Cloud	Anforderungen an HCC-Cloud	Nutzung für HCC-Dienst verpflichtend
			Benachrichtigung und Reporting bei erkannten Angriffen	
Datenbanken und Daten-dienste	Relationale Datenbank	Instanz je Stunde, Storage und Backup GB je Monat	- PostgreSQL oder kompatibel (unveränderte PostgreSQL-Clients nutzbar) - Weitere SQL-Engines (optional) - Multi-AZ mit standortübergreifender Synchronisation - Wiederherstellung auf einen wählbaren Zeitpunkt (Point-in-Time Recovery), konfigurierbar bis mind. 7 Tage - Speicher je Instanz im laufenden Betrieb erweiterbar	Soll genutzt werden
	Cache	Instanz je Stunde	- Flüchtiger In-Memory-Zwischenspeicher für Sitzungs- und Abfragedaten mit Antwortzeiten im Millisekundenbereich - Kompatibel zum Redis/Valkey-Protokoll, unveränderte Clients nutzbar - Multi-AZ Unterstützung	Soll genutzt werden
	Key-Value Store (optional)	Instanz je Stunde, Speicher GB je Monat	- Kompatibel zu einem offenen, verbreiteten Protokoll, unveränderte Open-Source-Clients nutzbar - Dauerhafte Speicherung - Multi-AZ mit standortübergreifender Synchronisation	
Sicherheit	Cloud IAM	Produktspezifisch	- Verwaltung von Identitäten und Berechtigungen für alle Services - Integrierbar mit Kubernetes - Identitäten für Menschen und Maschinen - Anbindung externer Identitätssysteme	
	Key Management Service	Schlüssel / Partition je Monat	- Verwaltung und Provisionierung kryptographischer Schlüssel - Nutzung-Protokollierung	

2026-0030 TI-Flow - Los 1+2 – Anwendungen + Cloud Services

Anlage-02a Leistungsbeschreibung - Anhang SK Los 1 und 2

Kategorie	Service	Abrechnungsmetrik durch HCC-Cloud	Anforderungen an HCC-Cloud	Nutzung für HCC-Dienst verpflichtend
			• Bring-Your-Own-Key (optional) • Hold-Your-Own-Key (optional)	
	Secrets Management	Instanz / Namespace per Monat	• Vault/OpenBao-API-kompatibel	
	Hardware Security Module (HSM)	HSM-Instanz oder dedizierte Partition je Monat	• Mandantenfähiges, dediziertes HSM oder dedizierte Partition mit exklusiver administrativer Kontrolle des Auftraggebers • Zertifiziert nach FIPS 140-2 Level 3 oder Common Criteria EAL 4+ mit hohem Angriffspotenzial • Betrieb über mindestens zwei Availability Zones mit Sicherung und Wiederherstellung • Als Teil von HCC-spezifische Leistungen nutzbar	
Observability	Observability as a Service	Ingest GB je Monat, Speicher GB je Monat	• Aufnahme von Metriken, Logs und Traces aus Workloads der Kunden über OTLP • Aufbewahrung und Export der Daten	
CI/CD-Plattform	CI/CD-Plattform als Software as a Service	Aktive Nutzer je Monat, Runner gemäß Compute, Speicher GB je Monat	• Siehe TI-Flow Leistungsbeschreibung Los Kapitel 3.1.4 & Kapitel 3.2.4.1	

1.2 HCC-spezifische Leistungen

Der Servicekatalog des AN Los 2 muss die für den Betrieb der HCC-Plattform erforderlichen HCC-spezifischen Leistungen umfassen.

Hierzu gehören insbesondere:

- temporär exklusiv provisionierte HCC-Hosts,
- HCC-konform attestierte Confidential Virtual Machines auf geteilten Hosts (RU/TU/RU-DEV),
- Trust Domains,
- HCC-fähige Kubernetes-Plattformen oder gleichwertige Dienste,
- Attestation- und Schlüsselmanagementfunktionen auf Basis von HSM-Clustern sowie
- weitere für die Umsetzung der HCC-Anforderungen erforderliche Leistungen

Der AN Los 2 muss die technischen Eigenschaften und Einsatzbedingungen dieser Leistungen beschreiben.

Kategorie	Service	Abrechnungsmetrik	Anforderungen	Nutzung für HCC-Dienst verpflichtend
Compute	HCC Virtuelle Maschinen	vCPU / RAM per Stunde	- Mehrere Leistungsklassen - Autoscaling - Update- und Patch-Management für OS-Images inkl. cVM-Template	Muss genutzt werden
	Dedicated HCC-Hosts	Host je Stunde / Monat	- Physischer Server exklusiv für eine HCC-TrustDomain Dynamisch provisionierbar, keine feste Hardwarereservierung - Mehrere Leistungsklassen	Muss genutzt werden
Container und Orchestrierung	Managed Kubernetes HCC	Cluster je Stunde, Nodes gemäß Compute	- Control Plane durch den Auftragnehmer betrieben, verteilbar über mehrere Availability Zones - Node Pools über Availability Zones verteilbar, Cluster Autoscaler - Nodes nach Leistungsklassen konfigurierbar - Netzwerkregeln zwischen Pods durchsetzbar - Persistente Volumes mit Verschlüsselung und Snapshots - Zulässige Workloads durch Regeln des Auftraggebers technisch durchgesetzbar (Policy as Code, Pod Security Standards) - Konsistente Wiederherstellbarkeit von Workloads und Volumes inkl. persistenten Ressourcen	Muss genutzt werden
Administration	Trust Domain	Produktspezifisch	Dienste und Interfaces für Betrieb und Administration einer TrustDomain	Muss genutzt werden
Sicherheit	HCC-HSM	Schlüssel / Partition je Monat		Muss genutzt werden