

**Anlage 1 zu Nutzungsbedingungen
für die unentgeltliche Nutzung des
Federation Master der gematik GmbH**

Leistungsbeschreibung Federation Master

1. Rolle und Zweck des Federation Master

Der Federation Master ist die zentrale Vertrauens- und Steuerungskomponente der föderierten Identitätslandschaft in der Telematikinfrastruktur (TI). Er verankert den Vertrauensraum der Föderation und stellt standardisierte Schnittstellen bereit, über die Informationen zu registrierten Teilnehmern – insbesondere sektoralen Identity Providern (IDP) und Fachanwendungen als Relying Parties (RP) – abgefragt und verwaltet werden können. Technologisch basiert er auf OpenID Connect (OIDC), OAuth 2.0 und JSON Web Token (JWT) sowie dem Profil OpenID Connect Federation 1.0.

2. Grundprinzip Föderation in der TI

- Dezentralität: Identitäten werden nicht von einem zentralen Dienst bereitgestellt, sondern von mehreren sektoralen Identity Providern, die jeweils von den zuständigen Institutionen verantwortet werden.
- Vertrauensraum: Anwendungen und Identity Provider kommunizieren abgesichert über Vertrauensketten (Trust Chains), ohne zuvor bilateral-organisatorische Vereinbarungen treffen zu müssen.
- Einheitliche Vorgaben: Für eine einfache und interoperable Gesamtlösung gelten einheitliche technische und organisatorische Leitplanken:
 - Einheitliche Identitätsattribute je Nutzergruppe (Minimal Claim Sets, Scopes)
 - Grundstruktur der Vertrauensbeziehungen (IDP Federation/Trust Chains)
 - Einheitliche Verfahren zur Auffindbarkeit von IDPs (IDP Discovery)
 - Einheitliche Vertrauensniveaus (Trust Framework)

3. Kernaufgaben des Federation Master

- Vertrauensanker: Verwaltung des Vertrauensraums der Föderation; Gewährleistung der Integrität und Nachprüfbarkeit von Vertrauenskette und Richtlinien.
- Schlüsselmanagement: Verwaltung der öffentlichen Schlüssel aller registrierten Teilnehmer (OP und RP gemäß openid-connect-core).
- Validierung: Prüfung und Validierung von Anfragen, Metadaten und Aussagen (Entity Statements) innerhalb der Föderation.
- Schnittstellenbereitstellung:
 - Auskunft zum Federation Master selbst (Entity Statement)
 - Abfrage von Informationen über Teilnehmer der Föderation
 - Bereitstellung einer Liste aller registrierten OpenID Provider (OP)
 - Registrierung neuer OP und RP
 - Löschung nicht mehr benötigter OP und RP
- Registrierungspflicht: Alle sektoralen Identity Provider sowie alle Fachanwendungen (Relying Parties), die Identitäten nutzen möchten, müssen beim Federation Master registriert sein.

- Konforme Metadaten: Jede Partei – einschließlich des Federation Master – veröffentlicht ein OIDC-spezifikationskonformes Entity Statement. Dieses bildet die Grundlage für die automatisierte Vertrauensableitung in der Föderation.

4. Anwendungsfälle des Federation Masters

Use Case	Kurzbeschreibung
Teilnehmer registrieren	Jede Fachanwendung und jeder Identity Provider muss sich als Teilnehmer beim Federation Master registrieren. Im Zuge der Registrierung wird der öffentliche Teil des Schlüssels, mit dem der Teilnehmer sein Entity Statement signiert, beim Federation Master hinterlegt. Für jede Fachanwendung wird zusätzlich hinterlegt, welche Informationen zum Nutzer (<i>scopes</i>) diese beim Identity Provider erfragen dürfen. Für jeden Identity Provider werden die Schlüssel der TLS-Verbindungen in die VAU hinterlegt.
IDP-Liste bereitstellen	Zu allen in der Föderation registrierten Identity Providern werden die Informationen 'Organisationsname', 'Logo' und 'Zieladresse (URL)' ermittelt und als Liste bereitgestellt.
Entity Statement bereitstellen	Der Federation Master stellt zu jedem registrierten Teilnehmer ein Entity Statement aus.
Schlüssel der TLS-Zertifikate abgleichen	In regelmäßigen Abständen und bei Zertifikaterstellung prüft der Federation Master die TLS-Zertifikate der in der VAU mündenden TLS-Verbindungen in der Weise, ob die öffentlichen Schlüssel der Zertifikate im Federation Master hinterlegt sind. Zur Ermittlung aller in Frage kommender TLS-Zertifikate nutzt der Federation Master öffentlich zugängliche Certificate Transparency Provider.
Schlüssel verwalten	Der Federation Master verwaltet die Schlüssel und Adressen der Teilnehmer und beglaubigt sie gegenüber anderen Diensten. Das Einbringen der Daten neuer Teilnehmer bzw. das Löschen der Daten auszuschließender Teilnehmer erfolgt über organisatorische Prozesse (Teilnehmer registrieren, Teilnehmer löschen).

Trotz umfangreicher technischer und organisatorischer Maßnahmen zur Sicherstellung der Betriebsstabilität durch die gematik und den Anbieter des Federation Masters – einschließlich Vorkehrungen, die Ausfälle auch während geplanter Wartungsarbeiten verhindern sollen – kann die durchgehende Erreichbarkeit des Federation Masters nicht garantiert werden. Im Störfall arbeitet die gematik umgehend gemeinsam mit dem Anbieter daran, die Beeinträchtigung zu identifizieren und zu beheben. Um eine reibungslose Authentifizierung der Nutzer sicherzustellen, wird den Anbietern, die über ihre Anwendungen den Federation Master nutzen, empfohlen Informationen vom Federation Master asynchron und proaktiv abrufen (z. B. regelmäßiges Caching und Aktualisieren relevanter Metadaten), um über etwaige Störungen informiert zu bleiben. Die Bereitstellung des Federation Master erfolgt ohne Gewähr einer Verfügbarkeit ("as is" / "as available")

