Leistungsbeschreibung

für die Erstellung eines Fachkonzeptes zum Aufbau eines föderierten Videokonferenzsystems unter Verwendung von XFSC-Komponenten

Auftraggeber

eco – Verband der Internetwirtschaft e.V.

Lichtstr. 43h

50825 Köln

Ref.: GXFS-Conf

Inhaltsverzeichnis

1. Hintergrund und Rahmenbedingungen

Die Gaia-X Föderationsdienste[1] (GXFS) stellen Basisbetriebsfunktion für föderierte Benutzergruppen (Föderationen) mit gemeinschaftlicher Nutzung von digitalen Diensten zur Verfügung.

Folgende Kernfunktionen sind dafür erforderlich:

- Identitäts- und Vertrauensdienste
- Katalogdienste mit Selbstbeschreibungen von Teilnehmern und Diensten
- Mechanismen für souveränen Datenaustausch
- Verfahren zur Bewertung von regulatorischen Anforderungen und Compliance

Die technischen GXFS-Komponenten wurden Mitte 2023 unter neuem Projektnamen Cross Federation Services Components (XFSC) an die Eclipse Foundation übergeben.

Zur Anwendung von Videokonferenzdiensten bedarf es besonderer Umfeldbedingungen, um datenschutzkonforme, sichere und skalierende Dienste sowohl innerhalb von Benutzergruppen als auch zwischen diesen zu ermöglichen.

Eine grundsätzliche Orientierung stellt die KRITIS-Verordnung (BSI-KritisV[2] von 2016, geändert 2017 und 2021) dar. Sie ist maßgeblich für die Einstufung von Betreibern kritischer Infrastrukturen oberhalb definierter Schwellenwerte, und setzt den Rahmen für die Umsetzung der Anforderungen des Gesetzes.

2. Auftragsgegenstand

Das Ziel dieses Projekts ist es, basierend auf dem Konzept souveräner Daten-Infrastrukturen konkrete Orientierung zum Einsatz von Videokonferenz-Plattformen für öffentliche Einrichtungen zu schaffen. Die zur Wahl stehenden Komponenten müssen auf Open-Source-Produkten basieren.

Der Betrieb solcher Dienste soll hierbei gemäß ISO 27001 nach IT-Grundschutz erfolgen. Die ISO 27001 ist ein international anerkannter Standard für Informationssicherheitsmanagementsysteme (ISMS), der sicherstellt, dass Organisationen angemessene und verhältnismäßige Sicherheitsmaßnahmen implementieren. Der IT-Grundschutz des BSI (Bundesamt für Sicherheit in der Informationstechnik) bietet eine Methodik zur Erreichung dieses Standards und stellt sicher, dass alle Aspekte der Informationssicherheit berücksichtigt werden. Dies wird nicht nur das Vertrauen in die Plattform stärken, sondern auch sicherstellen, dass sie den höchsten Sicherheitsstandards entspricht.

Zusammenfassend zielt dieses Projekt darauf ab, die konzeptionelle Grundlage für eine sichere, vertrauenswürdige und unabhängige Videokonferenz-Servicestruktur für öffentliche Einrichtungen zu schaffen, die den aktuellen und zukünftigen Anforderungen an Kommunikation und Datenschutz gerecht wird.

[1] https://www.gxfs.eu/download/6543 (GXFS - Gaia-X Federation Services – Die Werkzeugkiste)

[2] https://www.gesetze-im-internet.de/bsi-kritisv/ (BSI-KritisV)

3. Erstellung Fachkonzept

3.1.Ziel des Konzepts

Ziel dieser Konzeptentwicklung ist die Ausarbeitung einer funktionalen Analyse und Gesamtgestaltung einer Betriebsumgebung für den folgenden Anwendungsfall:

Es sollen 2 Föderationen (logische Gruppen von identifizierbaren Nutzern) jeweils individuelle Videokonferenzdienste nutzen. Die Provisionierung kann im Eigenbetrieb, über Managed Service Betreiber oder als „as-a service“ erfolgen. Die Identifikation der beteiligten rechtlichen Entitäten (Participants) und deren berechtigten Teilnehmer: innen (Principals) erfolgt mittels SSI-Prinzipien (Self Sovereign Identity) gemäß der technischen GXFS-Konzeption[3]. Die Repräsentation von Video-Services in unterschiedlichen Charakterisierungen (z.B. Anzahl Teilnehmer, Sicherheitsstufe, Servicelevel) werden in Gaia-X konformen Servicebeschreibungen deklariert und in einem XFSC-Katalog verwaltet[4].

Bei der Betrachtung der technischen Umsetzung sind verschiedene aufbauende Szenarien zu evaluieren:

- Zusammenschalten von Videokonferenzteilnehmern auf einer dedizierten technischen Plattform mit Zugangsberechtigungen über „Wallet Dienste“ und zugewiesenen „Verifiable Credentials“.
- Zusammenschalten von Videokonferenzteilnehmer über mehrere Installationen und Darstellung technische Konzepte zur Multiknotenskalierung, also der Lastverteilung von Videositzungen über örtlich verteilte Instanzen.
- Provisionierung von IX-Konnektivität mit dediziertem Routing zwischen den technischen Instanzen.

Die Zugangswege der Teilnehmer: innen zu den ersten Eingangspunkten für die Nutzung von Videoservices ist nicht Bestandteil der Analyse. Es wird aber vorausgesetzt, dass der Einsatz von besonderen Sicherungsverfahren, wie z.B. VPN oder anderer Verschlüsselungsverfahren, keine Einschränkung für die gewählten Szenarien verursachen.

Zusammenfassend sind folgende Rahmenbedingungen zu berücksichtigen:

- Provisionierung von IX-Konnektivität mit dediziertem Routing zwischen den technischen Instanzen
- Provisionierung von Videokonferenzsystemen in verschiedenen Betriebsstätten
- Identitäts- und Credentialverfahren gemäß SSI (Self Sovereign Identities) unter Verwendung der Cross Federation Services Components (XFSC) aus dem Bereich Identity & Trust (AAS, PCM, OCM, TSA, NOT)[5]
- Katalogbeschreibung verschiedener Servicekategorien, bis hin zu konkreten Buchungsverfahren mittels XFSC CAT[6]
- Verfahren des Sitzungsmanagement über verteilte Betriebsstätten

[3] https://www.gxfs.eu/download/3059/ (GXFS SSI Whitepaper: Gaia-X-sichere und vertrauenswürdige Ökosysteme mit souveränen Identitäten)
[4] https://www.gxfs.eu/download/4314/ (GXFS SD Whitepaper: Selbstbeschreibung von Ressourcen, Serviceangeboten und Teilnehmern im Gaia-X-Ökosystem)
[5] https://projects.eclipse.org/projects/technology.xfsc
[6] https://gaia-x.gitlab.io/data-infrastructure-federation-services/cat/architecture-document/architecture/catalogue-architecture.html

- Auswahl verschiedener Skalierungsstufen (20, 50, 100, 500, 1000 Teilnehmer: innen)
- Auswahl verschiedener Vertraulichkeitsstufen gemäß BSI Kompendium Videokonferenzsysteme[7]
- Alle Lösungskomponenten entsprechen den Kriterien einer freizügigen Open-Source-Lizenz[8]
- Kubernetes[9] als Betriebsebene wird unterstützt
- Mindestens eine Videoservice Variante muss grundsätzlich auf einem Sovereign Cloud Stack[10] zu betreiben sein.

3.2.Leistungsanforderung

Das Ergebnisdokument muss folgende Elemente beinhalten:

- Aufbau einer Kurzübersicht von FOSS-Videokonferenzlösungen mit
  - Kurzbeschreibung und Funktionsumfang
  - Abschätzung der Markadaption in der EU
  - Technologie Stack, Deployment und grundlegende Skalierungsmechanismen
  - Einschränkungen bei der Anwendung in föderierten Umgebungen
- Vergleichende SWOT-Analyse von mindestens drei der relevantesten identifizierten Videokonferenzlösungen
- Adaption von SSI-Verfahren bei der Nutzung von Videokonferenzlösungen
- Konkrete Architekturen von mindestens zwei der Lösungen, jeweils einzeln und im Verbund und deren Kernfunktionen für Skalierung und resilientem Betrieb.[11]
- Evaluierung der Betriebskosten einer Lösung für den Betrieb mit bis zu 500 Teilnehmern pro Sitzung und bis zu 2000 gleichzeitigen Nutzern in mehreren Sitzungen
- Anforderungen an eine Betriebsumgebung in den Kategorien
  - Öffentlich (keine Vertraulichkeitsanforderungen über den gesetzlichen Rahmen hinaus)
  - Kritische Infrastrukturen in Anlehnung an KRITIS Gesetzgebung
  - VS-NfD
- Analyse zur Integration von Videodiensten in das Bundesmessenger Web Matrix SDK[12] und den Laufzeitumgebungen[13]

3.3.Funktionale Anforderungen

3.3.1. Auswahlkriterien Videoservices

Bei der Auswahl einer geeigneten Open-Source-Videokonferenz-Plattform sind mehrere Kriterien zu berücksichtigen:

- Sicherheitsfunktionen und -protokolle
- Skalierbarkeit und Leistungsfähigkeit
- Verfügbarkeit von Community-Support und regelmäßigen Updates

[7] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Kompendium-Videokonferenzsysteme.pdf (BSI Kompendium Videokonferenzsysteme)
[8] https://de.wikipedia.org/wiki/Freiz%C3%BCgige_Open-Source-Lizenz (FOSS)
[9] https://de.wikipedia.org/wiki/Kubernetes (Kubernetes)
[10] https://scs.community/de/
[11] https://de.wikipedia.org/wiki/Kubernetes (Kubernetes)
[12] https://gitlab.opencode.de/bwi/bundesmessenger/clients/bundesmessenger-web-matrix-sdk
[13] https://gitlab.opencode.de/bwi/bundesmessenger

- Kompatibilität mit gängigen Betriebssystemen und Geräten
- Einfache Integration in die geplante Cloud-Umgebung

3.3.2. Open Source Lösungen

Es gibt verschiedene Open-Source-Videokonferenz-Lösungen auf dem Markt, darunter Jitsi, BigBlueButton und Nextcloud Talk. Jede dieser Lösungen hat ihre eigenen Stärken und Anwendungsbereiche, die im Kontext der Anforderungen öffentlicher Einrichtungen zu bewerten sind. Es können weitere Lösungen in Betracht gezogen werden, sofern diese den Kriterien einer freizügigen Open-Source-Lizenz genügen[14].

3.3.3. ISO 27001 und IT-Grundschutz

ISO 27001 ist ein weltweit anerkannter Standard für Informationssicherheitsmanagementsysteme (ISMS). IT-Grundschutz, entwickelt vom Bundesamt für Sicherheit in der Informationstechnik (BSI), bietet einen methodischen Ansatz zur Implementierung und Einhaltung von ISO 27001, wobei ein besonderer Schwerpunkt auf der Umsetzung in deutschen Organisationen und öffentlichen Einrichtungen liegt. Die Zertifizierung nach ISO 27001 und IT-Grundschutz stellt sicher, dass Videokonferenz-Dienste den höchsten Sicherheitsstandards entsprechen. Dies stärkt das Vertrauen der Nutzer, minimiert Risiken und stellt sicher, dass der Betrieb den gesetzlichen und regulatorischen Anforderungen in Bezug auf Datenschutz und Informationssicherheit gestaltet ist.

3.3.4. Integration mit XFSC basiertem Federated IAM

Die Vorteile der Integration mit XFSC basiertem IAM (siehe Anlage annex_GX_IDM_AO) stellen sich unter anderem wie folgt dar.

Einheitliche Benutzererfahrung: Benutzer müssen sich nur einmal authentifizieren und können dann auf verschiedene Dienste zugreifen mit durchgängiger Kontrolle eigener Profildaten.

Erhöhte Sicherheit: Durch die Konsolidierung von Authentifizierungsprozessen in einem föderierten IAM können Sicherheitsrichtlinien konsistent durchgesetzt werden.

Interoperabilität: Die Integration in ein XFSC basiertes IAM stellt sicher, dass die Komponenten in der Lage sind, mit anderen Gaia-X konformen Diensten und Anwendungen zu interagieren.

Datensouveränität: Die Einhaltung der SSI-Verfahren gewährleistet, dass die Datenhoheit bei den Benutzern bleibt und europäische Datenschutzstandards eingehalten werden.

3.3.5. Architektur

3.3.5.1. Netzwerkdesign und Sicherheitsmaßnahmen

Das Netzwerkdesign ist mehrschichtig, wobei jede Schicht spezielle Sicherheitsmaßnahmen aufweist, die den Richtlinien der ISO 27001 und des IT-Grundschutzes entsprechen:

Perimeter-Schutz: Firewalls und Intrusion Detection Systeme überwachen und kontrollieren den eingehenden und ausgehenden Verkehr, um unerwünschte Zugriffe zu blockieren.

Interne Sicherheit: Netzwerksegmentierung und -isolierung werden verwendet, um sicherzustellen, dass kompromittierte Systeme nicht auf andere Teile des Netzwerks zugreifen können.

Zugriffskontrolle: Der Zugriff auf die Systeme und Daten ist streng geregelt. Nur autorisierte Benutzer und Systeme können auf bestimmte Ressourcen zugreifen, und alle Zugriffsversuche werden protokolliert.

3.3.5.2. Datenfluss und Kommunikation zwischen den Systemen

Die Kommunikation zwischen den Systemkomponenten erfolgt über dedizierte und gesicherte Kanäle. Alle Transaktionen werden überwacht und protokolliert, um die Integrität und Sicherheit der Daten zu gewährleisten. Eventuelle Unregelmäßigkeiten im Datenfluss werden sofort erkannt und können schnell adressiert werden.

3.3.5.3. Skalierbarkeit und Hochverfügbarkeit

Die Videokonferenzlösungen müssen dynamisch und sicher skaliert werden. Redundanz ist erforderlich, um eine hohe Verfügbarkeit zu gewährleisten, und Failover-Mechanismen sind zu implementieren, um die Dienstkontinuität auch bei Ausfällen zu gewährleisten.

3.3.6. Sicherheitskonzept

3.3.6.1. Sicherheitsrichtlinien und Best Practices

Die Grundlage für ein robustes Sicherheitskonzept sind klar definierte Richtlinien und Verfahren. Diese werden in Anlehnung an die Standards der ISO 27001 und des IT-Grundschutzes erstellt und regelmäßig überprüft. Die Richtlinien umfassen Aspekte wie Zugriffskontrollen, Datenklassifizierung, Incident Management und regelmäßige Sicherheitsüberprüfungen.

3.3.6.2. Zugriffskontrolle und Authentifizierung

Das föderierte IAM, basierend auf XFSC-Komponenten, wird als primäres Werkzeug zur Authentifizierung und Autorisierung von Benutzern und Systemen eingesetzt. Benutzer müssen starke, einzigartige Passwörter verwenden, und Multi-Faktor-Authentifizierung (MFA) wird für kritische Systemzugriffe und Administrationsaufgaben eingeführt. Attributbasierte Zugriffskontrollen (ABAC) gewährleisten, dass Benutzer und Systeme nur auf die Informationen und Ressourcen zugreifen können, die sie benötigen.

3.3.6.3. Datenverschlüsselung und Datenschutz

Data-in-transit: Alle Daten, die zwischen den Systemen übertragen werden, sind mittels TLS (Transport Layer Security) oder entsprechenden Protokollen verschlüsselt.

Data-in-use: Daten, die aktuell von der Plattform verarbeitet werden, sind durch verschiedene Sicherheitsmechanismen geschützt, darunter Speicherzugriffsbeschränkungen und fortgeschrittene Verschlüsselungsfunktionen.

Data-at-rest: Alle auf der Plattform gespeicherten Daten, einschließlich Videokonferenzaufzeichnungen und Benutzerinformationen, werden sowohl auf Datei- als auch auf Datenbankebene verschlüsselt.