

2024-11-19 IAM Workshop DHÖ (Datenhausökosystem)


IAM - Identity and Access Management

Exported on 11/21/2024

Table of Contents

1	Date.....	3
2	Attendees	4
3	Goals.....	5
3.1	IAM-relevante Komponenten für MVP.....	5
3.1.1	Resource-Server / Scopes	5
3.1.2	OIDC-Clients	6
3.2	Offene Fragen Zielbild	6
4	Konzept.....	8
5	Discussion items.....	10
6	Action items	11

1 Date

 19 Nov 2024

2 Attendees

BD IAM

- @Semih Kuru (BKA) - PM
- @Lars Wächtler (BKA) - PO
- @Dieter Steding (BKA) - Lead Developer
- @Christian Durst - Lead Ops (partial)
- @Dr. Patrik Stellmann (HH Extern) - SyA BD-IAM

DHÖ

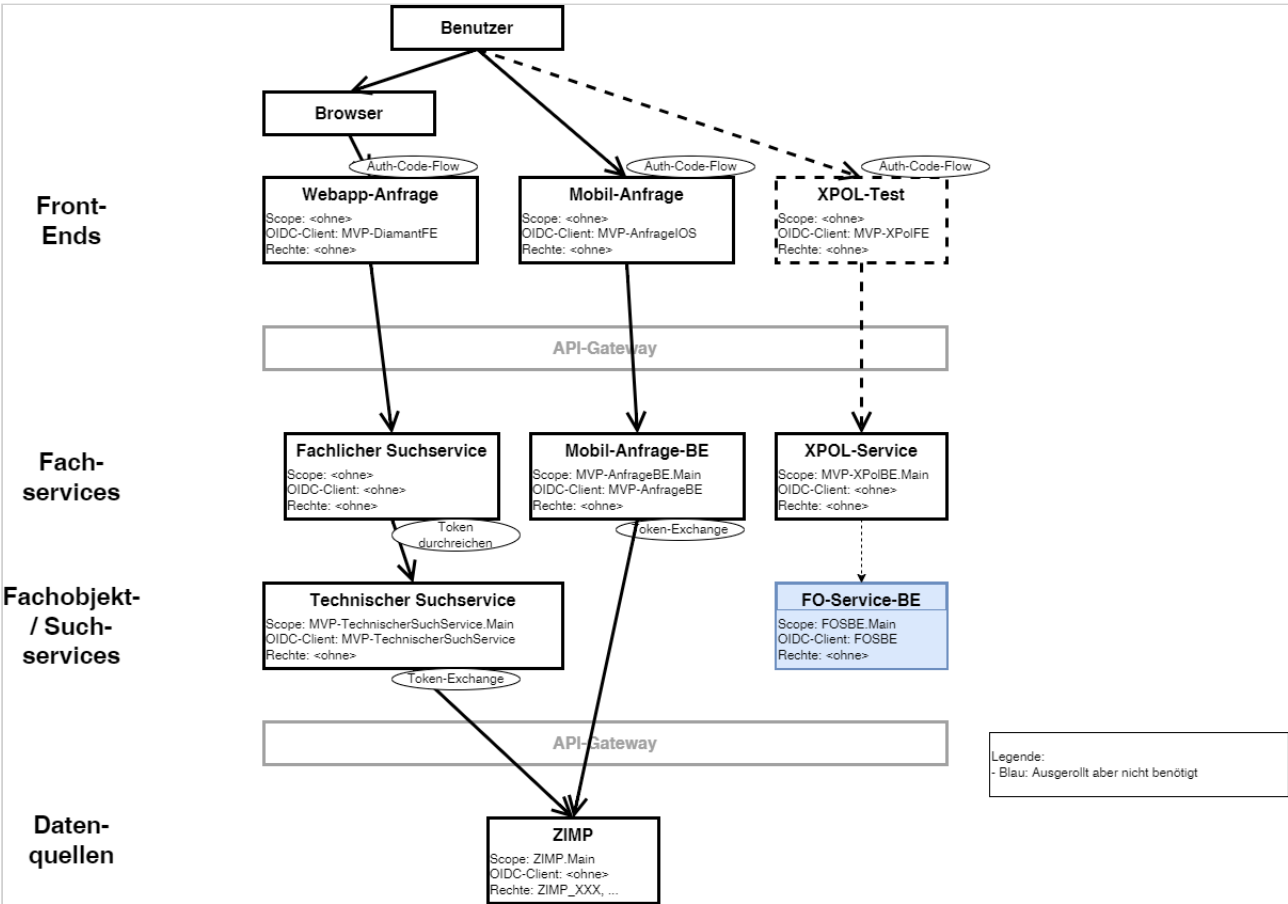
- @Felix Tschörner (BKA) - SyA DHÖ/SyA Fachlichkeit
- @Henrik Hackenberg (BMI) - Lead Developer Kernkomponenten

KTT

- @Rene Donner (BKA)

3 Goals

3.1 IAM-relevante Komponenten für MVP



3.1.1 Resource-Server / Scopes

Resource Server	Scope	Rechte
MVP-AnfrageBE	.Main	-
MVP-TechnischerSuchService	.Main	-
MVP-XPoIBE	.Main	-

3.1.2 OIDC-Clients

Client	Typ	Auth-Code-Scopes	Token-Exchange	Redirect-URLs auf F-IAM-Instanzen			
				PP-DEV	PP-INT	EDU	Wirk
MVP-DiamantFE	private	MVP-TechnischerSuchService.Main	-	https://diamant-web.dhoes-dev.k8s-shared-2-ext.app.dev-w0.caas.psp.bka.bund.de/api/auth/callback/oam	https://suche.dhoes.int.caas.psp.extrapol.de/api/auth/callback/oam	https://suche.dhoes.prod.caas.psp.extrapol.de/api/auth/callback/oam	https://p20.extrapol.de/suche/api/auth/callback/oam
MVP-AnfrageIOS	public	MVP-AnfrageBE.Main	-	P20-suche://oauth2-callback (see page 3)			
MVP-AnfrageBE	private	-	ZIMP	-			
MVP-TechnischerSuchService	private	-	ZIMP	-			
MVP-XPolFE	private	MVP-XPolBE.Main	-	https://www.example.com			

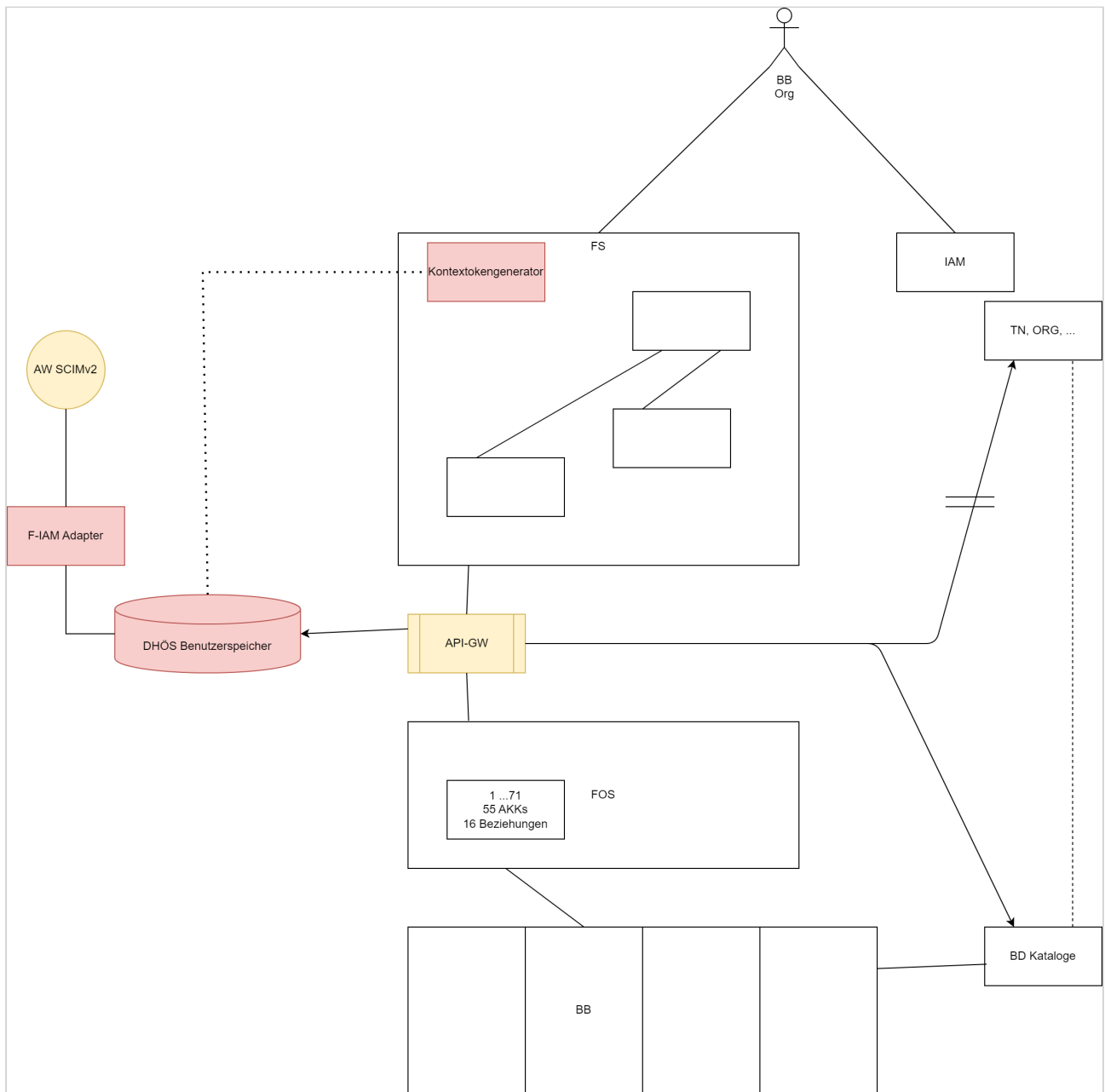
3.2 Offene Fragen Zielbild

- Abstimmung Struktur vom letzten WS (siehe <https://confluence.bka.extrapol.de/x/OhVoG>)

- **Korrektur zum letzten Workshop: Freischaltung von Scopes für Token-Exchange nur auf komplette Resource-Server, nicht pro Scope möglich.**
 - *Verworfen*
- Auth-Code-Flow **nicht** durch API-Gateway
 - *ist geklärt: Dies ist nicht möglich und nicht notwendig.*
- Token-Exchange zwischen Front-Ends und Fachservices durch API-Gateway?
 - (→ Alle Front-Ends können effektiv alle Fachservices ansprechen, keine Einschränkung durch F-IAM)
 - *Hinfällig durch neue gekürzte Struktur.*
- Zusammenspiel
 - Mandanten
 - Kontexte (Bearbeitung/Freigabe)
 - AW-Rechte
 - Dienststelle
- Warum müssen mehrere AWs dieselben Rechte prüfen? AW-Rechte, die von verschiedenen AWs zu prüfen sind, sind keine AW-Rechte!
 - *Hinfällig, da AW-Rechteprüfung wird auf FOS-Ebene oder ähnlich durchgeführt.*
- Erfolgt die Zuordnung von Konten und Mandanten tatsächlich auf Benutzer-Ebene? Nicht auf TN-Ebene? (TN1 darf auf Daten von TN2 zugreifen)
 - *Definition, Mandant == Teilnehmer; Freigabekontexte nicht auf BV Ebene sondern länderspezifische Beziehungen welche innerhalb des DHÖS gespeichert werden (separate Anwendung)*
- Kann die Zuordnung von Mandanten und Kontexten zu Benutzern tatsächlich von einem Benutzerverwalter erfolgen?
 - *geklärt, siehe oben.*
- Warum gibt es im DHÖ keine Dienststellen-bezogenen Rechte, wenn dies u.a. für alle iVBS essentiell ist?
 - *gibt es, siehe Darstellung unten.*
- Kann man Mandanten evtl. durch Dienststellen ersetzen?
 - *Nein, siehe Beschlüsse.*
- Ergibt es Sinn, einen DHÖ-Nutzerspeicher zu erstellen und zu provisionieren, wo mehrere DHÖ-Services Berechtigungszuweisungen (auch mit Dst-Bezug) abfragen können?
 - Zu viele Rechte können eh nicht ins Token, sondern müssen per userprofile abgefragt werden
 - Komplexe Berechtigungen können weder ins Token noch in userprofile → Benutzerspeicher erforderlich
 - Es gibt Fälle, wo ohnehin eine Liste von Benutzern erforderlich ist (eher AW-gebunden als gesamt-DHÖ)
 - *Ja, es ergibt Sinn und ist auch angedacht.*

4 Konzept

- Beschluss:
 - es wird definiert, dass ein Mandant == ein Teilnehmer/Partnerbehörde == IDP Claim im Token
 - die MVP IDM Entitäten werden voraussichtlich 2025 durch zielbildkonforme Entitäten ersetzt
 - das äußere API-GW prüft nur auf gültiges F-IAM Token (aktuell keine Scope Prüfung, im Zielbild definierte Menge von Scopes)
- Idee:
 - ein Kontexttoken ist technisch als JWT realisiert
 - ein Kontexttoken, wird vom Service XPol und weitere Sachservices mittels eines Basisservice erstellt
 - im Kontexttoken sind u.a. enthalten:
 - Kontext, z.B. iVBS-NW
 - Dienststelle
 - HyDaNe Label
 - Freigabekontext (Freigaben gem. Verträgen zwischen Teilnehmern)
- Das API-GW der Fachobjektservices stellt sicher, dass nur Benutzer mit korrekten Dienststellen - bezogen auf den Dienststellenkatalog - akzeptiert werden.
 - Berechtigungsprüfung auf Dienststellenebene über dienststellenbezogene AW-Rechte und zugriff auf DHÖ Benutzerspeicher (vom F-IAM provisioniert)
 - Im lesenden Teilnehmerkontext (rechte Seite) erfolgt die Abfrage der untergeordneten Dienststellen mittels BD Kataloge



5 Discussion items

Item	Who	Notes

6 Action items

- ☐ @Felix Tschörner (BMI Extern) 📅 22 Nov 2024 : Rechte zur Rollenerstellung an F-IAM bereitstellen.
- ☐ @Lars Wächtler (BKA) 📅 25 Nov 2024 : Prüfung ob notwendige Rechte zur Rollenerstellung an F-IAM bereitgestellt wurden.
- ☒ @Dr. Patrik Stellmann (HH Extern) 📅 21 Nov 2024 : Bitte Grafik und Tabellen zum MVP anpassen, incl. MVP- Präfix.