



SACHSEN-ANHALT

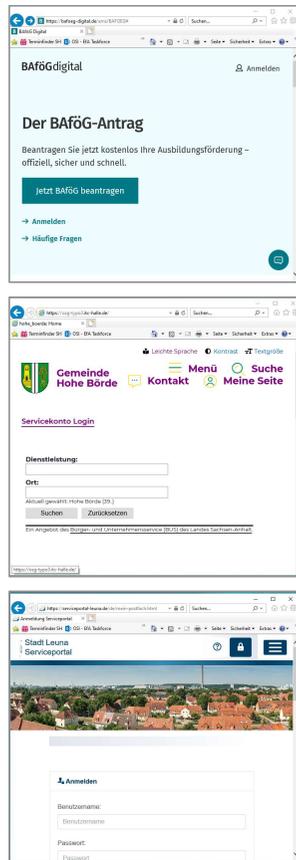
#moderndenken

2. OZG Sprechstunde

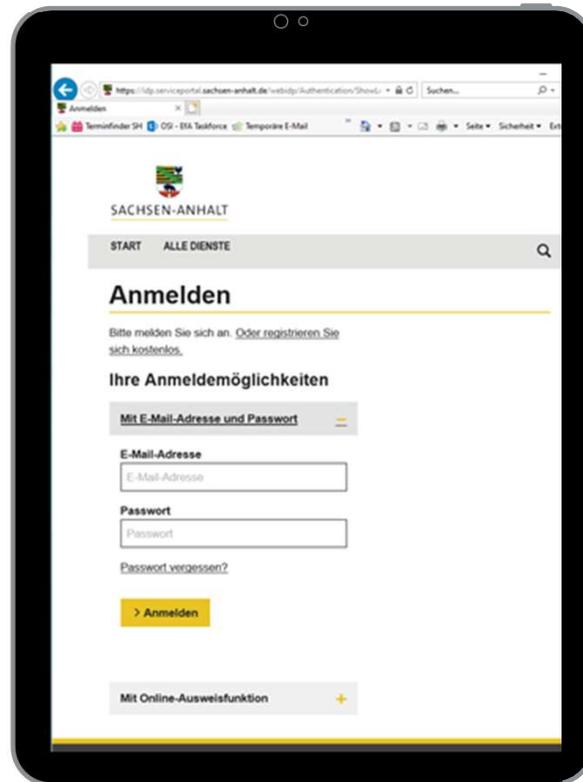
Anbindung Dritter an OSI und AFM

18.11.2020

“MOTIVATION” - NUTZERKONTO



Service Provider
(Kommunale) Portale, Online-Dienste

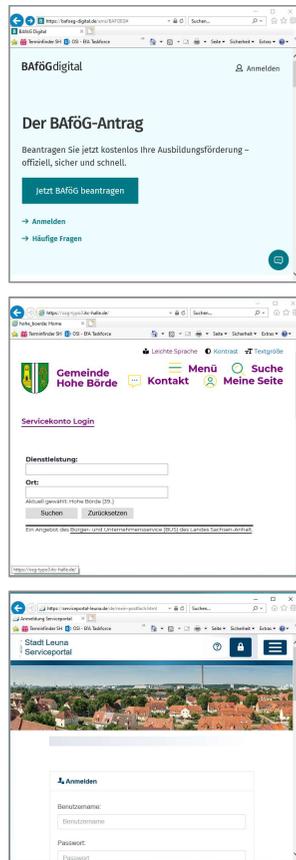


Identity Provider

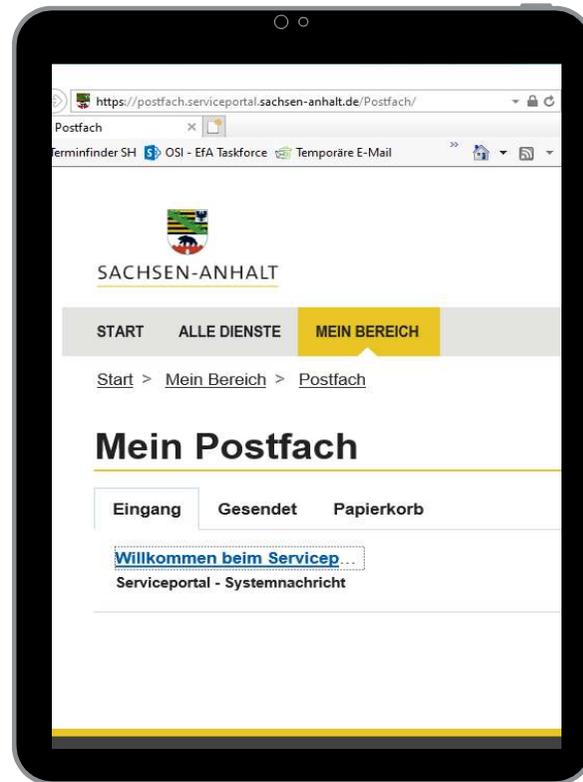
Verfügbare Funktionalitäten durch Anbindung an das OSI-Servicekonto

- Registrierung und Anmeldung unterschiedlichen Vertrauensniveaus
- Servicekonto Business
 - Benutzerverwaltung
 - Autorisierung

“MOTIVATION” - POSTFACH



Service Provider
(Kommunale) Portale, Online-Dienste

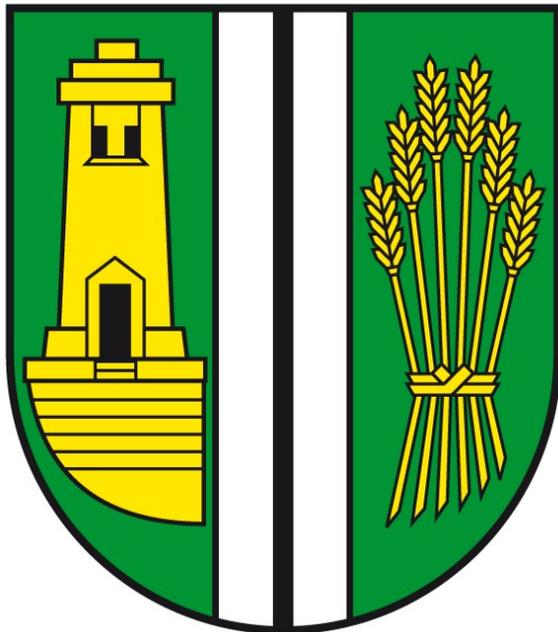


Identity Provider

Verfügbare Funktionalitäten durch Anbindung an das Postfach

- Senden einer Nachricht an ein Benutzer-Postfach
- Abrufen von Antwort-Nachrichten, die Nutzende für das angebundene System erstellt haben
- Löschen einer Antwort-Nachricht im OSI-Postfachsystem. Die Nachricht / der Vorgang bleibt für den Nutzer

DEMO HOHE BÖRDE / BAföG



<https://bafoeg-digital.de/ams/BAFOEG/login>

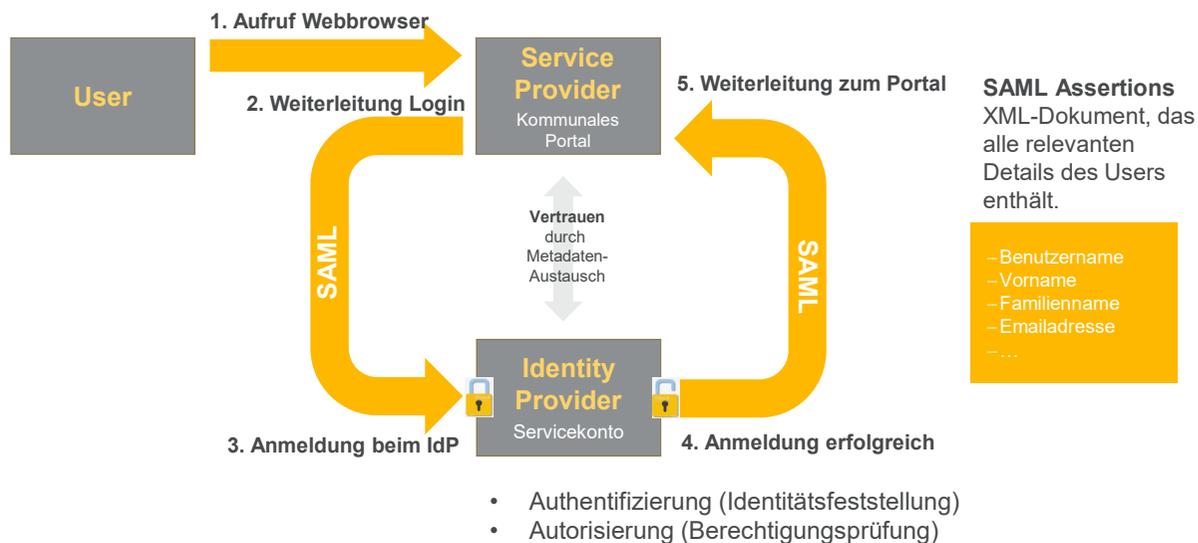


<https://serviceportal-leuna.de>



<https://ozg-typo3.itc-halle.de/anzeige-bus>

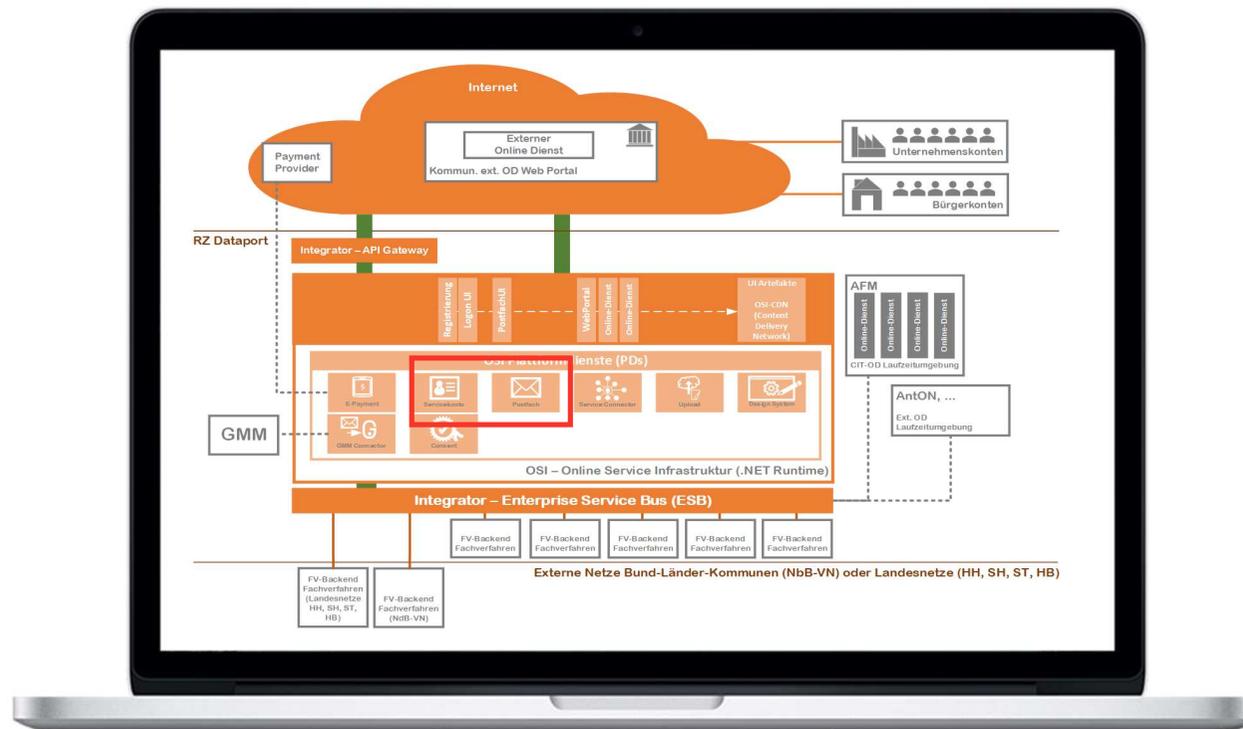
ALLGEMEINES ZU SAML



- **Security Assertion Markup Language (SAML)** ist ein offener Standard zum Austausch von Authentifizierungs- und Autorisierungsinformationen.
- Dies ermöglicht, dass man sich bei verschiedenen Websites mit einem Satz von Anmeldeinformationen anmelden kann.

Video zu SAML: <https://www.youtube.com/watch?v=SvppXbpv-5k&feature=youtu.be>

EINORDNUNG OSI



ALLGEMEINES ZUR ANBINDUNG

OSI - Nutzerkonto



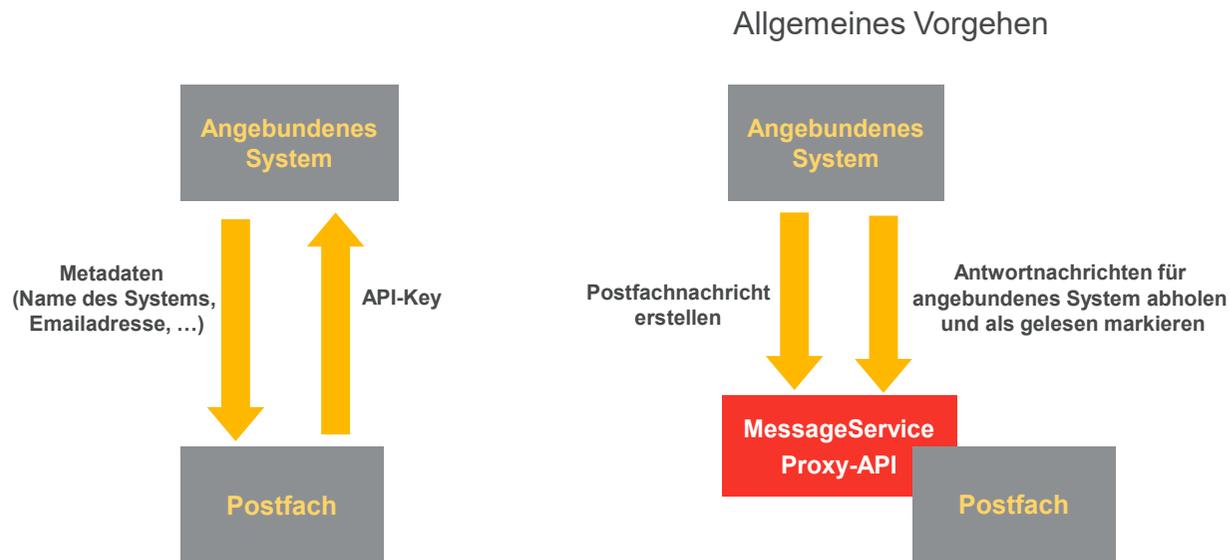
Zur Anbindung Dritter an das OSI-Servicekonto müssen Metadaten zwischen dem Service Provider (kommunales Portal) und dem Identity Provider (OSI-Servicekonto) ausgetauscht werden



SAML bietet hierfür einen sicheren Datenaustausch zwischen Service Provider und Identity Provider

ALLGEMEINES ZUR ANBINDUNG

OSI - Postfach



- Anbindung aus dem Internet ist über eine proprietäre Schnittstelle möglich

Anbindungsprozess



METADATEN - Template

Name der Kommune		Zum Beispiel „Landkreis xyz“
Name der Umgebung (Bitte geben Sie die Umgebung an, für die Sie eine Anbindung wünschen.)		Zum Beispiel „Stage-Umgebung Sachsen-Anhalt“
Kontakt Daten zum IT-Dienstleister		
Fachlicher Ansprechpartner	Name	Zum Beispiel „Frank Mustermann“
	E-Mail	Zum Beispiel „mustermann@firmaabc.de“
	Telefonnummer	Zum Beispiel „040 1234 1234“
Technischer Ansprechpartner	Name	Zum Beispiel „Sabine Test“
	E-Mail	Zum Beispiel „test@firmaabc.de“
	Telefonnummer	Zum Beispiel „040 1234 5678“
E-Mail für geplante Maßnahmen an OSI (Bitte geben Sie eine E-Mailadresse für Informationen zu geplanten Maßnahmen an der OSI-Infrastruktur an.)		Zum Beispiel „serviceportal@kommunexyz.de“
Bezeichnung des SAML Service Providers (In der Regel handelt es sich hierbei um den Namen des Portals. Die Bezeichnung muss global eindeutig sein.)		Zum Beispiel „Serviceportal Kommune xyz“
Beschreibung des Nutzens (Bitte geben Sie kurz an, warum Sie eine Anbindung an das OSI-Servicekonto wünschen.)		Zum Beispiel „Für den Online-Dienst xyz soll die Authentifizierung über das OSI-Servicekonto erfolgen.“
SAML SP entityID		Zum Beispiel „urn:dienstleisterabc:portalxyz:osi:servicekonto:prod“

Signaturzertifikat	Zum Beispiel „siehe Zertifikat im Anhang“
Verschlüsselungszertifikat (optional)	Zum Beispiel „siehe Zertifikat im Anhang“
Endpunkte	
1. URL für den AssertionConsumerService (via POST-Binding/https)	Zum Beispiel „https://testportal.de/ws/auth/saml/2.0/AssertionConsumerServiceViaPost“
2. URL für den SingleLogoutService (via Redirect-Binding/https) (für Logout-Request und –Response)	Zum Beispiel „https://testportal.de/ws/auth/saml/2.0/SingleLogoutServiceViaRedirect“
3. Als Alternative zu 2. (nur gemeinsam mit 4.): URL für SingleLogoutService (via POST-Binding/https) (für Logout-Response)	Zum Beispiel „https://testportal.de/ws/auth/saml/2.0/SingleLogoutServiceViaPost“
4. Als Alternative zu 2. (nur gemeinsam mit 3.): URL für SingleLogoutService (via SOAP-Binding/https) (für Logout-Request)	Zum Beispiel „https://testportal.de/ws/auth/saml/2.0/SingleLogoutServiceViaPost“

WARTUNG

Vorgehen bei Zertifikataustausch



Vor geplanten Maßnahmen an der OSI-Stage- und -Produktionsumgebung (z.B. Zertifikatstausch) erfolgt eine Information an einen definierten Verteiler



Sofern Sie in den Metadaten eine E-Mailadresse bei „E-Mail für OSI-Updates/-Änderungen“ angeben, werden Sie in den Verteiler aufgenommen



Bei einem Zertifikatstausch können Sie entsprechend der Ihnen zugeleiteten Information ab einem bestimmten Zeitpunkt das öffentliche Zertifikat unter einem definierten Link abrufen.

AUSBLICK

OAuth2.0/OpenID Connect

- OAuth2.0/OpenID Connect als weiterer Standard und Alternative zu SAML
- liefert weitere Funktionen zur M2M Kommunikation
- „OSI als API“
 - Erweiterte Postfachfunktionalität
 - ePayment
 - Consent-Funktionalität (Signatur-Dienst)
 - Anbindung GMM (Governikus Multi Messenger)



WEITERGEHENDE INFOS

LEITFADEN ZUR ANBINDUNG

https://ozg.sachsen-anhalt.de/fileadmin/Bibliothek/Politik_und_Verwaltung/MF/OZG/Bilder/Leitfaden/2020-06-19_Leitfaden_zur_Anbindung_kommunaler_Online-Dienste_an_OSI_v1.3.pdf

TEMPLATE METADATENAUSTAUSCH

https://ozg.sachsen-anhalt.de/fileadmin/Bibliothek/Politik_und_Verwaltung/MF/OZG/Bilder/Leitfaden/2020-07-10_Template-Metadatenaustausch.docx

SAML-SCHNITTSTELLENBESCHREIBUNG SERVICEKONTO

https://ozg.sachsen-anhalt.de/fileadmin/Bibliothek/Politik_und_Verwaltung/MF/OZG/Bilder/Leitfaden/2020-06-18_SAML-Schnittstellenbeschreibung_Servicekonto.pdf

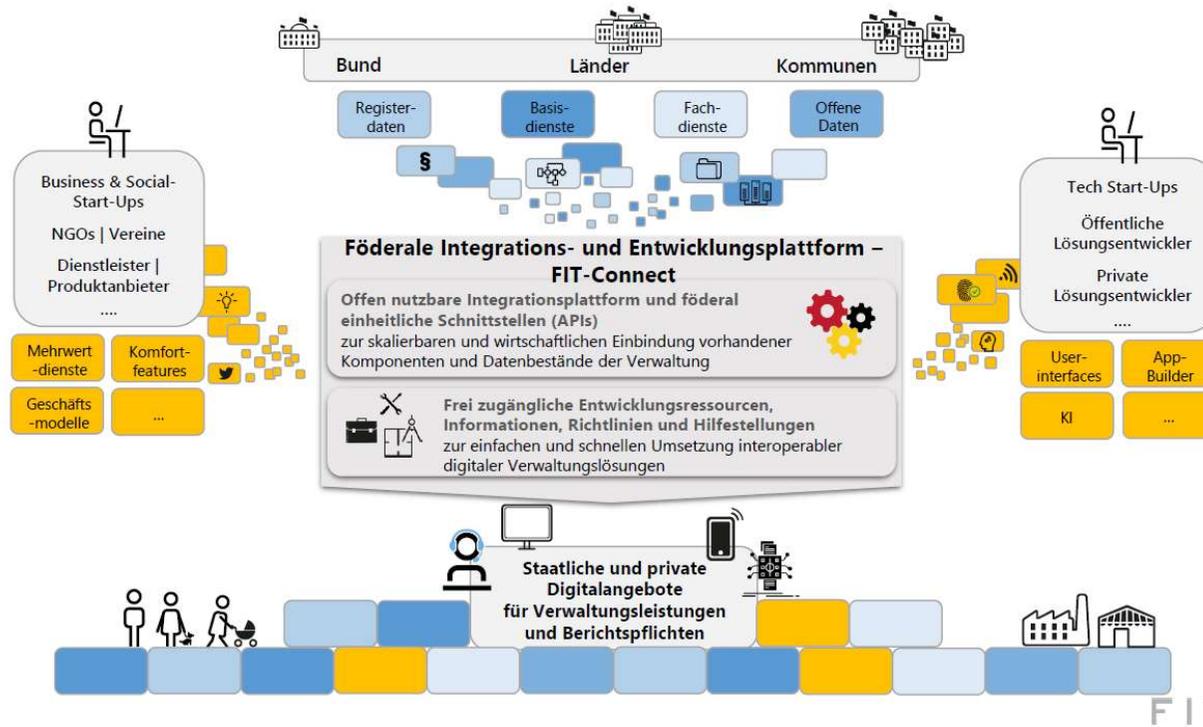
SAML-SCHNITTSTELLENBESCHREIBUNG POSTFACH

https://ozg.sachsen-anhalt.de/fileadmin/Bibliothek/Politik_und_Verwaltung/MF/OZG/Bilder/Leitfaden/2020-06-18_Schnittstellenbeschreibung_Postfach_MessageService_ProxyAPI.pdf



AUSBLICK FIT - CONNECT

Zielvision der FIT-Connect Plattform



FIT-Connect möchte eine Konnektierungsplattform bereitstellen

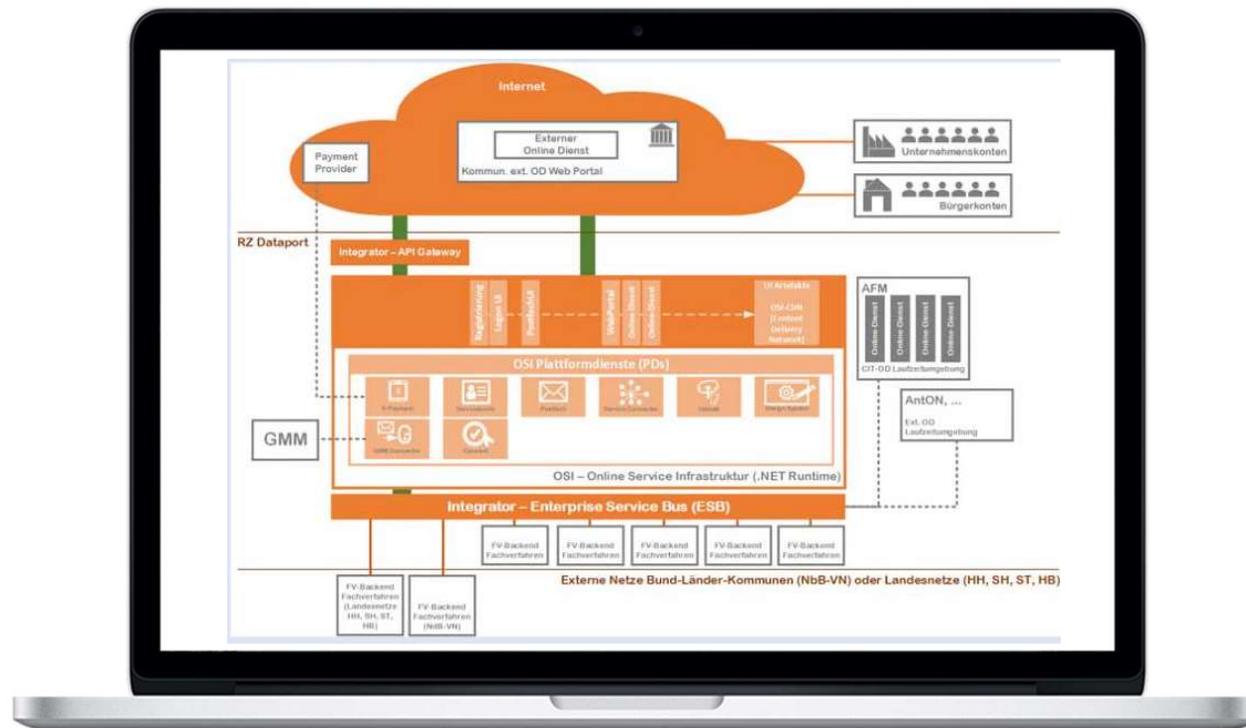


SACHSTAND ZU BASISDIENST ePAYMENT

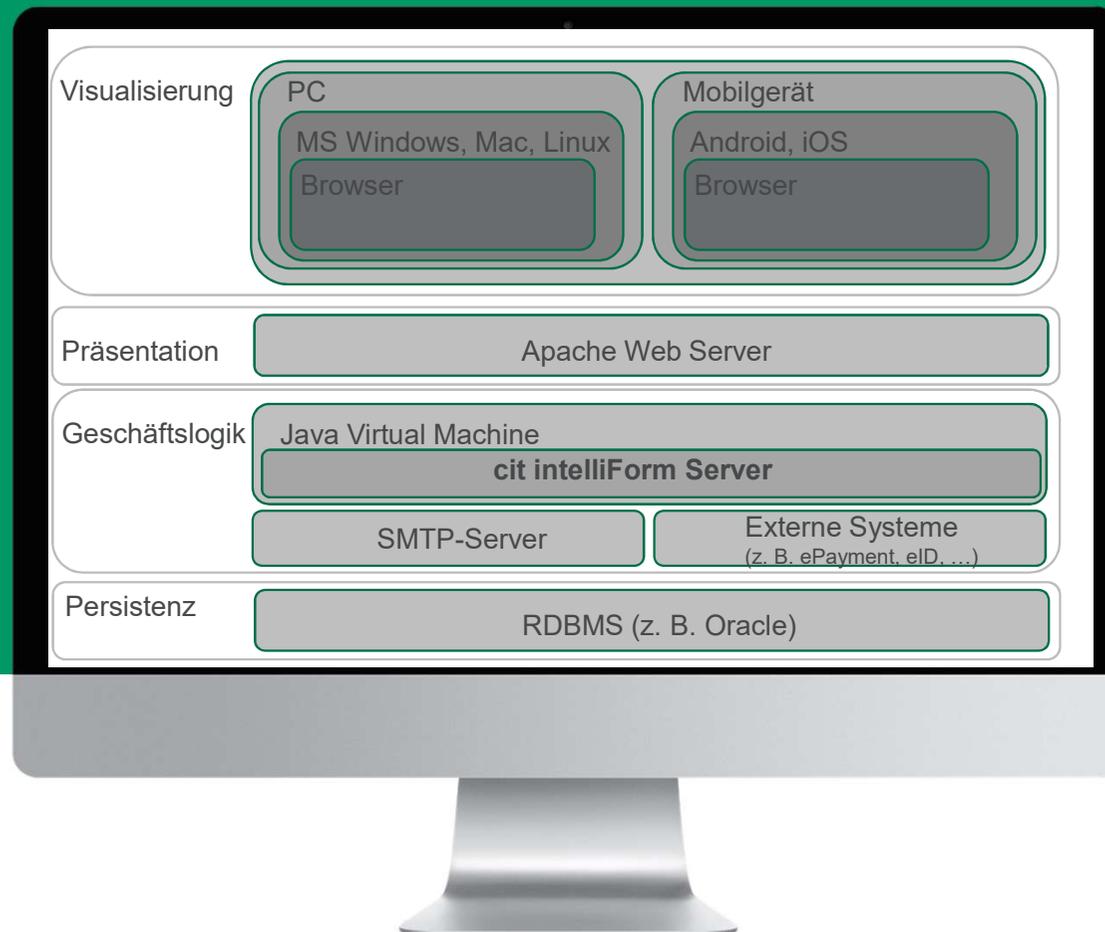
- Arbeiten, den Basisdienst ePayment anzubieten, laufen
- Es wird geplant, der Entwicklergemeinschaft ePayBL beizutreten
- Folgende Fragen haben sich dazu ergeben:
 - Bieten Sie bereits elektronische Bezahlungsmöglichkeiten an?
 - Wie ist die Kassenzeichenstruktur der Kommunen?
 - Gibt es Gemeinsamkeiten bei der Vergabe?
 - Haben Sie Bezahlterminals die zum Einsatz kommen?
 - Gibt es eine Arbeitsgemeinschaft der Kämmerer an die wir herantreten können?



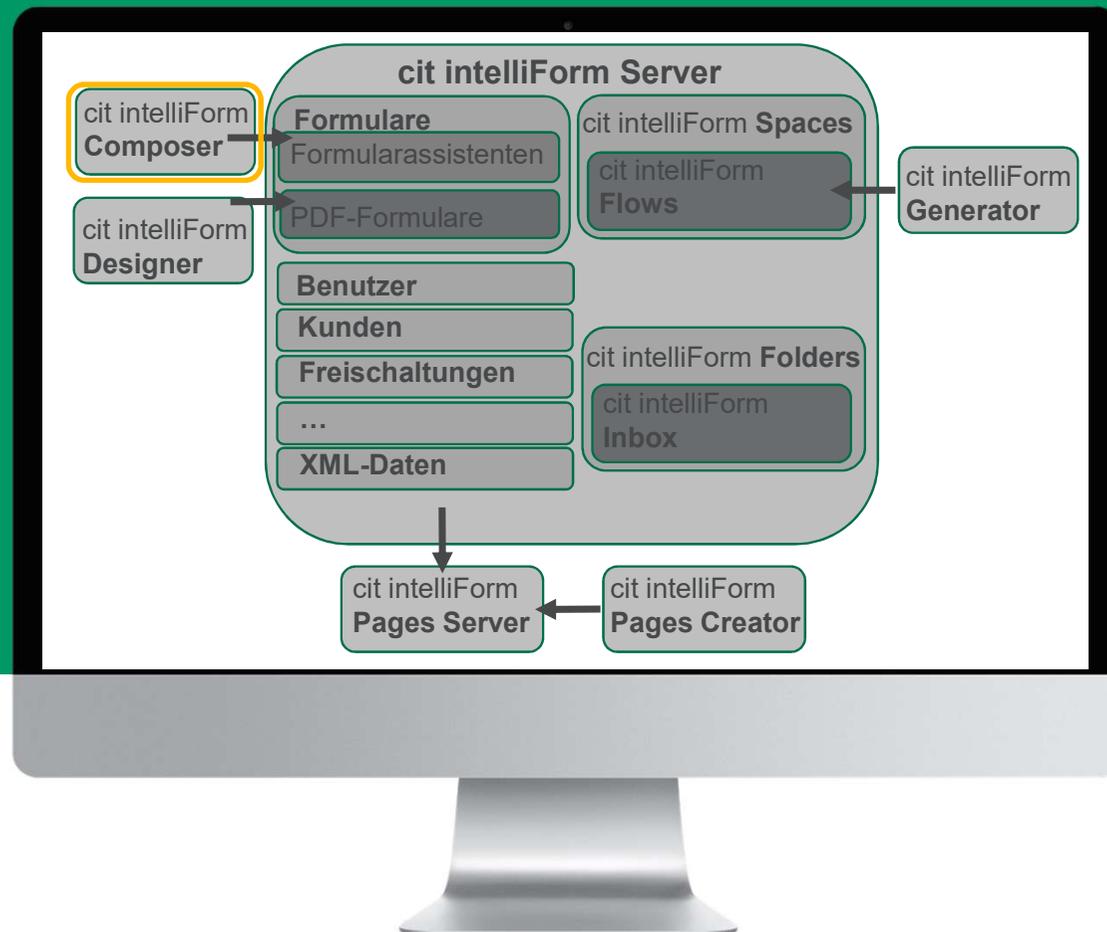
AFM - PLATTFORM



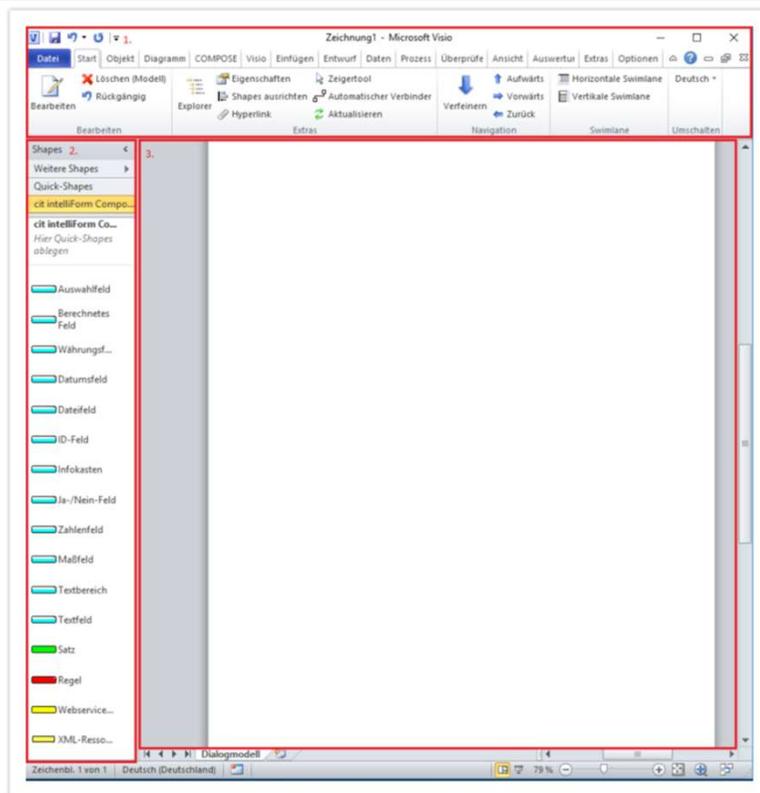
AFM - SERVERARCHITEKTUR



AFM - KOMPONENTEN



AFM - COMPOSER



- basiert auf SemTalk
- Microsoft® Office Visio-Basis
- Voraussetzungen:
 - Betriebssystem Microsoft Windows 7 Service Pack 1 oder Microsoft Windows 10, 32-Bit / 64-Bit
 - Microsoft Office Visio 2010, 2013 oder 2016,
 - Microsoft .NET Framework 4 oder neuer (in Windows 10 standardmäßig enthalten)
 - Microsoft Visual Studio 2010-Tools für Office-Laufzeit
 - Administrationsrechte (nur zur Installation)

AFM - VORGEHEN

- Bedarfsmeldung über MF
- Prüfung der OZG-Konformität
- Dataport führt Qualitätscheck durch und deployed auf der Stageumgebung
- Nach erfolgreichem Test → Überführung in Produktivumgebung
- Dataport entwickelt derzeit technische Spezifika für die Entwicklung der AFM-Antragsassistenten



3. OZG-Sprechstunde

Am 09.12.2020

Alle 3 Wochen

immer mittwochs 13 - 14 Uhr

VIELEN DANK

Für Ihre Aufmerksamkeit



Sachsen-Anhalt
#moderndenken



WEITERE INFORMATIONEN UND ANTWORTEN ERHALTEN SIE HIER

Ministerium der Finanzen des Landes Sachsen-Anhalt

 **ADRESSE:**
Editharing 40
39108 Magdeburg

 **E-MAIL:**
ozg-mf@sachsen-anhalt.de

 **TEL.:**
+49 391 567 1030

 **WEBSEITE:**
ozg.sachsen-anhalt.de

Quellen und Bilder

Bildquellen:

Folie 4: https://www.google.com/search?q=hohe+B%C3%B6rde+wappen&tbm=isch&ved=2ahUKEwixj5PSw4ntAhVO4oUKHacxAmcQ2-cCegQIABAA&oq=hohe+B%C3%B6rde+wappen&gs_lcp=CgNpbWcQAzIECCMQJzoECAAQHjoGCAAQBRAeOgQIABAYUMANWlwXYI0aaABwAHgAgAHKAYgBhQeSAQUyLjQuMZgBAKABAaoBC2d3cy13aXotaW1nwAEB&sclient=img&ei=I7uzX_HxJ87ElwSn44i4Bg&bih=501&biw=1056&client=firefox-b-d#imgrc=pe0T6jTaviQ_WM

Folie 14: <https://picjumbo.com/webdesigners-sticky-notes/>

Folie 21: <https://unsplash.com/photos/0CvHQ62gwY8>