BundID Anleitung

Diese Anleitung soll eine Hilfe zur Anbindung an die BundID darstellen. Bei Fragen oder Rückmeldungen bitte an kadir.thal@dataport.de wenden.

Servicekonto

Welche grundsätzlichen Unterschiede gibt es gegenüber dem OSI Bürgerkonten?

- Die BundID ist als Fremdkonto am OSI Servicekonto angebunden.
- Es werden keinerlei Kontodaten im OSI Servicekonto gespeichert, sondern sie werden immer von der BundID abgerufen und an den Online-Dienst weitergegeben.
- Dadurch gibt es auch keinerlei Provisionierung hinsichtlich der Kontoerstellung, der Änderung oder der Löschung.
- Der Nachrichtenversand auf das BundID Postfach erfolgt über die Postfach Facade API die mittels OAuth abgesichert ist.
- Für die Zustellung in das BundID Postfach benötigt man die Postfachreferenz des Nutzerkontos, die als SAML-Attribut bei der Anmeldung vom OSI Servicekonto an den Online-Dienst übermittelt wird.
- Bei den Fremdkonten ist es unabdingbar, dass man die Kombination von NameIdentifier und NameQualifier aus der SAML-Assertion verwendet wird, um das Nutzerkonto eindeutig zu identifizieren. Diese Regel ist auch bei den OSI-Konten anwendbar.

Welche Anpassungen müssen im Online-Dienst vorgenommen werden?

Bei Online-Diensten, die über den Service Connector an das Servicekonto angebunden sind oder die bereits die Anmeldung mit den Interoperablen Servicekonten unterstützen, müssen für die Anmeldung mit der BundID keine Anpassung mehr vorgenommen werden.

Online-Dienste die direkt an das Servicekonto angebunden sind und bisher noch keine Anmeldung mit den Interoperablen Servicekonten unterstützen, müssen prüfen, wie sie ein Nutzerkonto eindeutig identifizieren und ggf. Änderungen vornehmen können.

Technische Details

Die Kombination aus der ID des Nutzerkontos aus `saml:Assertion/saml:Subject/saml:NameID` und dem Attribut `@NameQualifier` sollte verwendet werden.
Zudem gibt es einige Attribute, die bei der Anmeldung mit der BundID nicht unterstützt werden, wie z.B. der Username.

Wenn der Online-Dienst etwas in das BundID Postfach zustellen möchte, muss die Postfachreferenz (in der *SAML-Assertion* das Attribut *InboxReference*) mit an den Online-Dienst übermittelt werden.
Sollte der Online-Dienst im *SAML-AuthnRequest* einzelne Attribute anfordern, muss die Postfachreferenz mit aufgenommen werden. Wenn keine Attribute angefordert werden, liefert das OSI-Servicekonto einige Attribute automatisch zurück, wozu auch die Postfachreferenz zählt.

Für die Zustellung in das BundID Postfach muss die Postfach Facade API verwendet werden, die über OAuth abgesichert ist. Ein AccessToken kann über das OSI Servicekonto erzeugen werden, der dazu eine OpenID Connect Schnittstelle zur Verfügung stellt.

Die erforderliche ClientID und das ClientSecret kann vom FVM eingerichtet werden.
Des Weiteren können Online-Dienste, die an den Service Connector angebunden sind, auf bereits vorhandene APIs zurück greifen.

Wie wird die Anmeldemöglichkeit mit der BundID für den Dienst aktiviert?

Online-Dienste, die über den Service Connector an das Servicekonto angebunden sind, müssen in der AdminUI vom Service Connector die Option

"BundID-Anmeldung zulassen" für den Dienst aktivieren.

Online-Dienste, die direkt an das Servicekonto angebunden sind, müssen in der AdminUI vom Servicekonto im Serviceprovider oder im Dienst die Option "Service Provider ermöglicht Anmeldung via BundID" bzw. "Dienst ermöglicht Anmeldung via BundID" aktivieren.

Für Online-Dienste, die vor dem 25.10.2023 die Interoperabilität aktiviert haben, wird die Option automatisch aktiviert.

Die Aktivierung der jeweiligen Optionen in STAGE und PROD werden durch das FVM durchgeführt.

Was muss beim Gang auf PROD beachtet werden?

Die Verantwortung der Funktionsfähigkeit der Onlinedienste liegt bei den fachlichen Leitstellen. Die Konfigurationen und Einstellungen können durch die Administratoren der Onlinedienste vorgenommen werden. Das FVM kann durch einen formlosen Auftrag einer berechtigen Person bei der Anpassung unterstützen.

Postfach

Der Postkorb der BUND ID steht seit 1.10.2023 zur Verfügung. Aufgrund des Reifegrads 3 wird ab dem 1.8.2023 die Postfachreference mit jedem Antrag mitgeschickt werden können. Eine Ausbaustufe das für OSI fremde FV das Postkorbhandle ausgegeben wird ist in Arbeit.

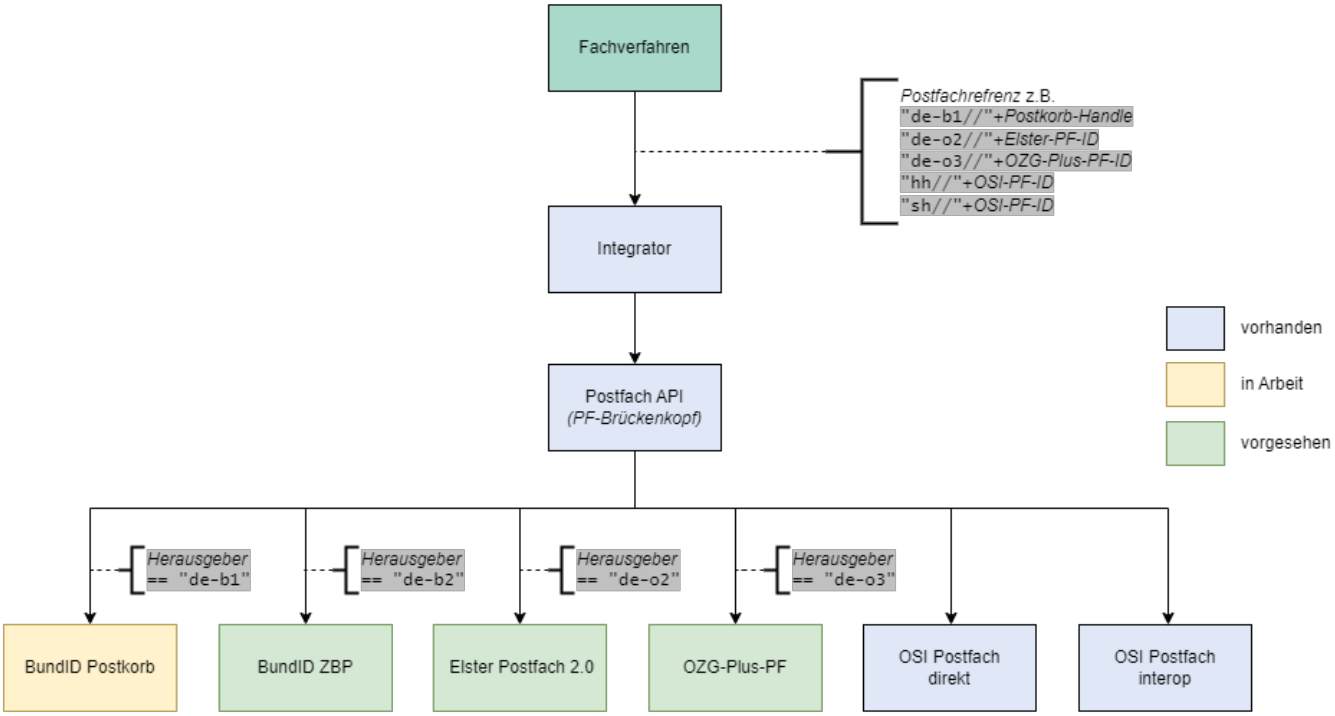
Die Anbindung der ZBP Schnittstelle ist aktuelle noch in Klärung und zeitlich noch nicht eingeplant.
Grundsätzlich werden zur Nutzung des Postkorb der BUND ID keine Anpassungen von Seiten der OD benötigt, wenn bereits einer der unten aufgeführten Schnittstellen angebunden sind.

Wie funktionierts?

1. Der OD muss die *Postfachreferenz* vom Servicekonto bekommen.
    - Dies erfolgt im Feld "InboxReference" der User-Informationen.
2. Der OD muss die *Postfachreferenz* an das Fachverfahren (zusammen mit den Antragsdaten) übermitteln.
3. Das FV muss die *Postfachreferenz* (bei Aufruf der PF-MessageExchange-Schnittstelle über den Integrator) angeben.

- Dies erfolgt im Feld *{mailboxId}* des Webservice-Aufrufs `/MessageExchange/v1/Send/{mailboxId}` bzw. `/MessageExchange/v1/Send/MessageWithAttachments/{mailboxId}`

4. Das Postfach (genauer: die Postfach API a.k.a. PF-Brückenkopf) muss die *Postfachreferenz* analysieren:
   - 4.1. Ist der Herausgeber "de-b1", so handelt es sich bei der *Id* um das Postfach-Handle eines BundID-Postkorbs.
     - 4.1.1. Dann wird die Nachricht dorthin zugestellt.



Welche Schnittstelle?

Anwendungsfall	Schnittstelle	Protokoll	Zone	Authentifizierung für diesen Service	Link zu technische Dokumentation	Anmerkungen

externe Onlinedienste und Fachverfahren die aus dem Internet auf das Postfach zugreifen möchten.
• Persönliche Postfächer
• Funktionspostfächer
• Anhänge (optional)
• Interoperable Postfächer FINK V0.6
• BUND ID Postkorb
• Mein Unternehmenskonto (Mittelfristig)
	Facade Postfach über den Integrator	REST	Internet	Provisionierung über ServiceKonto (OAuthToken)	osi_postfach - Integrator - OSI Confluence (dataport.de)
					
					PF-Facade - OSI Postfach - OSI Confluence (dataport.de)
					
					Swagger UI (dataport.de)
						externe Onlinedienste die aus dem Internet auf das Postfach zugreifen möchten, ist es zwingend der Integrator dazwischen zu schalten.
						
						Folgende Konfigurationseinstellung müssen in der Konfigurationsdatei (bei ASP.NET Core/.NET & und höher wäre das die appsettings.json) hinterlegt werden, damit über die Facade eine Nachricht an z.B. die BundID gesendet werden können:
						
						"**PostfachSettings**": {
						
						"**BaseUrl**": "https://api-gateway-dev.dataport.de:443/api/osi_postfach/1.0.0/",
						
						// OD spezifisch (muss über den **Betrieb** im Servicekonto AdminTool über den Bereich OpenId-Clients eingestellt werden
						
						"**ClientId**": "<clientid>",
						
						"**Secret**": "<secret>",
						
						"**Scopes**": "<scope>",
						
						// Generell
						
						"**Authority**": "https://idp-hh-002.ositest.dataport.de/webidp2/", //Identity Provider **Servicekonto**
						
						"**Resources**": "<resource>"
						
						}

interne Onlinedienste und Fachverfahren die aus dem Intranet auf das Postfach zugreifen möchten.
 	
• Interoperable Postfächer FINK V0.6
• BUND ID
• Persönliche Postfächer
• Funktionspostfächer
• Anhänge (optional)
	Facade Postfach	REST	Intranet	Provisionierung über ServiceKonto (OAuthToken)	PF-Facade - OSI
					Postfach - OSI
					Confluence (dataport.de)
					
					Swagger UI (dataport.de)
						Folgende Konfigurationseinstellung müssen in der Konfigurationsdatei (bei ASP.NET Core/.NET & und höher wäre das die appsettings.json) hinterlegt werden, damit über die Facade eine Nachricht an z.B. die BundID gesendet werden können:
						
						"**PostfachSettings**": {
						
						"**BaseUrl**": "https://api-gateway-dev.dataport.de:443/api/osi_postfach/1.0.0/",
						
						// OD spezifisch (muss über den **Betrieb** im Servicekonto AdminTool über den Bereich OpenId-Clients eingestellt werden
						
						"**ClientId**": "<clientid>",
						
						"**Secret**": "<secret>",
						
						"**Scopes**": "<scope>",
						
						// Generell
						
						"**Authority**": "https://idp-hh-002.ositest.dataport.de/webidp2/", //Identity Provider **Servicekonto**
						
						"**Resources**": "<resource>"
						
						}

interne Onlinedienste und Fachverfahren die aus dem Intranet auf das Postfach zugreifen möchten. • Persönliche Postfächer • Funktionspostfächer • Anhänge (optional) • Interoperable Postfächer FINK V0.6 • BUND ID Postkorb • Mein Unternehmenskonto (Mittelfristig)	**MessageExchange Micro Service 2.0**	REST	Intranet	Provisionierung über Service Conector	https://docs.osi.dataport.de/x/9SLL	