Schnittstellenbeschreibung - Zentrales Bürgerpostfach - Drittanwendungen

Stand: 17.04.2023

Dokumenten-Version: 1.2

Release-Version: Release 1.2.0.0

Autor: Antonius Dalezios (Entwicklungsleitung)

Präambel

Die Schnittstellenbeschreibung des "Zentrales Bürgerpostfach" (kurz ZBP) beschreibt, wie eine so genannte Drittanwendung (= Fachdienste, Fachverfahren, etc...) Nachrichten an das ZBP schicken können.

Dabei werden zwei grundlegende Aspekte beschrieben

- Authentifizierung
  Die Authentifizierung und Autorisierung erfolgt im ZBP mittels Security-Tokens (JWT).

- Funktionsumfang der Empfangsschnittstelle
  Es werden nur die Funktionen aus der aktuellste API Version beschrieben. Für die Beschreibung älterer API Versionen dienen die Schnittstellenbeschreibung in älterer Version.
  Die aktuelle API Version ist: **API v3**

Die technische Spezifikation der Schnittstelle wird als eine OpenAPI json Datei zur Verfügung gestellt und ist nicht Teil dieses Dokuments.

Authentifizierung

Die Authentifizierung und Autorisierung erfolgt im ZBP mittels Security-Tokens (JWT). Um ein Token zu erzeugen ist ein Client-Zertifikat notwendig. Dies wird teilweise auch als Berechtigungszertifikate bezeichnet.

Client-Zertifikat

Das Client-Zertifikat wird vom Betreiber des ZBPs nach Anmeldung ausgegeben. Das Zertifikat muss gewissen Vorgaben entsprechen und der public key des Zertifikats wird im Truststore des ZBPs hinterlegt. Die Verwendung eines nicht vom Betreiber des ZBP erstellten Zertifikats ist nicht möglich.
Das Client-Zertifikat wird **nicht** für den Aufbau der SSL/TLS Verbindung verwendet. Es dient ausschließlich der Erzeugung von Security Tokens und der Signatur von Nachrichten.

Security-Token

Überblick über die Arten der Autorisierung (= Security-Tokens) für Drittanwendungen:

Typ des Zertifikats	Typ des Security Tokens	Rolle
Drittanwendung (bspw. Fachverfahren)	Third-Party Token (engl. third-party token)	THIRD_PARTY (= der Verwender des Tokens ist eine Drittanwendung, die eine Nachricht ins ZBP einstellen möchte)

Code-Snippets (Java)

Third-Party Token

```
JWT.create()
        .withIssuedAt(createdDate) // createdDate = Erstellungsdatum
        .withExpiresAt(expiredDate) // expiredDate = Ablaufdatum
        .withClaim("signer", signer) // signer = CN (= common name) des Client-Zertifikats
        .withClaim("roles", List.of("THIRD_PARTY")) // roles = Rolle
        .sign(Algorithm.RSA256(publicKey, privateKey)); // Signierung des JWT
```

Funktionsumfang der Empfangsschnittstelle

Funktionsliste (API v3)

	Funktionsgruppe	Funktion	Security Token	Hinweise
	Nachrichten-Empfang	Über Drittanwendung	Third-Party Token	Drittanwendungen können Nachrichten auf einer dedizierten Schnittstelle in einem Postkorb einstellen. Das Nutzerkonto, welches die Hoheit über diesen Postkorb besitzt, wird über den Eingang einer neuen Nachricht informiert. Die Schnittstelle arbeitet mandanten-übergreifend: Ein Fachverfahren in Bundesland A kann eine Nachricht in einen Postkorb im ZBP einstellen, der organisatorisch zu einem Nutzerkonto aus Bundesland B gehört.

Funktionsbeschreibung

Nachrichten-Empfang

Über Drittanwendung

Um eine Nachricht in das ZBP einzustellen, muss der Sender über ein gültiges Client-Zertifikat verfügen. Mit dem entsprechenden Zertifikat kann der Sender dann ein entsprechendes Security Token erstellen. Das Token selbst enthält keine Parameter. Die Adressierung des Postkorbs erfolgt über die ein-eindeutige Postkorb-ID (auch Postkorb-Handle genannt). Die Postkorb-ID (engl. mailboxId) ist selbst Teil der Payload, damit diese auch Teil der Signatur ist.

Die Signatur der Nachricht wird über die gesamte Payload berechnet. Die Payload enthält neben den eigentlichen Nachrichteninformationen auch die Checksums der Anhänge.

Die Schnittstelle selbst arbeitet synchron. Das heißt, dass der Empfang und die Prüfung der Signatur direkt durchgeführt werden. Antwortet die Schnittstelle mit Http-Status 200 (OK), gilt die Nachricht als empfangen und geprüft. Der Sender kann sich auf den erfolgreichen Empfang verlassen (um bspw. die 3-Tage-Zustellfiktion zu starten).

Die Menge der zugelassenen Anhänge ist beschränkt auf 100 MByte Gesamtgröße. Die Anzahl der Anhänge darf nicht über 200 Stück liegen. Ein einzelner Anhang darf bis zu 100MByte groß sein.

Eine Nachricht unterstützt folgende fachliche Parameter:

- Postkorb-ID/Postkorb-Handle (UUID)
- Absender (bspw. Bezeichnung der Drittanwendung oder Behörde)
- Betreff
- Nachrichtentext
- Dienste (bspw. Bezeichnung des Fachverfahren)
- Aktenzeichen (ein Frei-Text Referenz)
- Absender URL
- Adresse der Lesebestätigung
- Antwort-Adresse
- Anhänge
    - Dateiname

    - Größe in Byte (Content-Length)
    - Checksum der Datei
- Vertrauensniveau der Nachricht (storkQaaLevel).

Technische Bezeichnung	Schlüssel	Bezeichnung nach TR-03160-1 bzw. Beschluss der Projektgruppe eID Strategie von Juli 2021
STORK-QAA-Level-1	1	Basisregistrierung
STORK-QAA-Level-2	2	Niedrig
STORK-QAA-Level-3	3	Substantiell
STORK-QAA-Level-4	4	Hoch

Nach Empfang einer Nachricht von einer Drittanwendung wird das Nutzerkonto, welches das Konto des Empfängers (Bürgers) verwaltet, über den Neu-Eingang einer Nachricht informiert. Das Nutzerkonto kann mit dieser Information den Bürger daraufhin per (bspw.) E-Mail über den Neu-Eingang informieren.

Das ZBP verschickt selbst **keine** Eingangsbenachrichtigungen an Bürger. Das ist die Aufgabe des Nutzerkontos.

Fehlercodes

Hier werden die fachlichen Fehler-Codes der Schnittstellen des ZBP-Dienstes beschrieben.

Fehlercode	Fehlertext	Beschreibung	Schnittstellen
ZBP_400_001	Missing or incomplete message in body	Die zu übertragende Nachricht im Body der Anfrage fehlt oder ist unvollständig.	Nachricht einfügen, Nachricht migrieren
ZBP_400_002	multipart form ist malformed	Die Beschreibung der mehrteiligen Daten im multi-stream Format konnte nicht gelesen werden, da sie Fehler enthält.	Nachricht einfügen, Nachricht migrieren
ZBP_400_003	invalid attachment type	Der Dateityp des hochgeladenen Anhangs ist ungültig.	Anhang hochladen
ZBP_400_004	HTML contains forbidden tags or attributes.	Der Nachrichteninhalt enthält nicht erlaubte Tags oder Attribute.	Nachricht einfügen, Nachricht migrieren
ZBP_400_005	Attachment {filename} missing in json content.	Ein hochgeladener Anhang ist nicht im JSON der Nachricht referenziert.	Nachricht einfügen, Nachricht migrieren
ZBP_400_006	{field} missing for {filename} in Attachment in json content.	Ein Feld im Attachment-Teil der JSON Nachricht fehlt.	Nachricht einfügen, Nachricht migrieren
ZBP_401_001	malformed authorization token	Der Authorisierungs-Token für die spezifische Anfrage ist ungültig. Mögliche Ursachen: Der Token hat eine ungültige Form, oder enthält unzureichende Berechtigungen für den Zugriff auf die angeforderte Ressource.	Jeder Dienst
ZBP_403_001	access denied to mailbox	Der Zugriff zum angeforderten Postfach wurde verweigert.	Postfach löschen
ZBP_403_002	Given signature does not match with message content. Please re-sign and try again.	Die übertragene Prüfsumme stimmt nicht mit dem Nachrichteninhalt überein.	Nachricht einfügen, Nachricht migrieren
ZBP_403_003	Your current trust level is to low.	Der Trustlevel ist zu niedrig, um die Aktion erfolgreich durchzuführen.	Postfach löschen, Nachricht löschen
ZBP_404_002	Can't find this attachment.	Der Anhang konnte nicht gefunden werden.	Anhang herunterladen, Postfach löschen, Nachricht löschen
ZBP_404_003	Can't find this mailbox.	Das Postfach konnte nicht gefunden werden.	Nachricht abrufen, Nachrichten abrufen, Nachrichtenstatus festlegen, Nachrichten löschen, Zusammenfassung, Postfach löschen, Nachricht einfügen, Nachricht migrieren
ZBP_404_004	Can't find this message.	Die Nachricht konnte nicht gefunden werden.	Nachrichtenstatus festlegen, Nachricht abrufen, Mailbox löschen, Nachrichten löschen
ZBP_404_005	File does not exist.	Die Datei konnte nicht gefunden werden.	Anhang herunterladen
ZBP_409_001	no trust level	Es wurde kein Trustlevel angegeben.	Jeder Dienst
ZBP_409_002	no subject in token	Es wurde kein Subject (Nutzerkonto ID) im Token angegeben.	Jeder Dienst
ZBP_409_003	wrong trust level	Der angegebene Trustlevel ist ungültig.	Jeder Dienst
ZBP_409_004	User already has a mailbox with a different id.	Für die angegebene Nutzerkonto ID existiert bereits ein Postfach mit einer anderen ID.	Postfach erstellen, Postfach migrieren
ZBP_409_005	An id conflict occurred.	Es besteht ein Konflikt mit einer vorhanden ID.	Postfach erstellen, Postfach migrieren

ZBP_409_006	Missing case reference number	Dies bedeutet, dass Ihre Fallreferenz-ID als null oder leer gesendet wird	Nachricht einfügen, Nachricht migrieren
ZBP_409_007	Invalid characters in case reference number	Dies bedeutet, dass Ihre Fallreferenz-ID-Zeichenfolge eine nicht unterstützte Zeichencodierung enthält.	Nachricht einfügen, Nachricht migrieren
ZBP_409_008	Case reference number is too long	Dies bedeutet, dass Ihre Fallreferenz-ID-Zeichenfolge mehr als 255 Zeichen hat.	Nachricht einfügen, Nachricht migrieren
ZBP_413_001	Number of allowed attachments exceeded.	Die Anzahl der erlaubten Anhänge wurde überschritten.	Nachricht einfügen, Nachricht migrieren
ZBP_413_002	Sum of attachments size exceeded limit.	Die erlaubte Summe der Dateigrößen der Anhänge wurde überschritten. Es wird hier die Gesamtgröße aller Anhänge zusammengerechnet.	Nachricht einfügen, Nachricht migrieren
ZBP_429_001	Rate limit was exceeded.	Die erlaubte Zugriffsrate wurde überschritten.	Jeder Dienst
ZBP_500_003	An Error occurred while streaming the attachment.	Beim Herunterladen des Anhangs ist ein Fehler aufgetreten.	Anhang herunterladen
ZBP_500_004	There was an error deleting the mailbox. Not all messages and attachments were deleted.	Beim Löschen des Postfachs ist ein Fehler aufgetreten. Es konnten nicht alle Nachrichten und Anhänge erfolgreich gelöscht werden.	Postfach löschen
ZBP_500_005	There was an error deleting the message.	Beim Löschen der Nachricht ist ein Fehler aufgetreten.	Nachricht löschen
ZBP_500_006	error processing request	Beim Verarbeiten der Anfrage ist ein Fehler aufgetreten.	Nachricht einfügen, Nachricht migrieren
ZBP_500_007	error validating the message content	Beim Überprüfen des Nachrichteninhalts auf unerlaubtes HTML ist ein interner Fehler aufgetreten	Nachricht einfügen, Nachricht migrieren
ZBP_500_011	internal servlet error occurred	Ein interner Serverfehler ist aufgetreten.	Jeder Dienst
ZBP_500_012	Please check logs for more information	Bitte überprüfen Sie die Logs für weitere Informationen.	Jeder Dienst
ZBP_503_001	error uploading to file storage	Beim Hochladen der Datei zum Dateiserver ist ein Fehler aufgetreten.	Nachricht einfügen, Nachricht migrieren