



Bundesministerium
des Innern
und für Heimat



Schnittstellenbeschreibung

Zentrales Bürgerpostfach

27. Februar 2024



Überblick über das Dokument

Name des Dokuments	Schnittstellenbeschreibung Zentrales Bürgerpostfach
Dokument-Version	1.7
Release-Version	Release 2.3.0.0
Stand	27.02.2024

Nachdruck, auch auszugsweise, ist genehmigungspflichtig.

Inhaltsverzeichnis

Präambel	4
Erläuterung Begriffe	4
Authentifizierung	5
JSON Web Token (JWT)	5
ZBP PKI-Client-Zertifikat	6
Funktionsumfang der Empfangsschnittstelle	7
Funktionsliste (API v6)	7
Funktionsbeschreibung	8
Nachrichten einstellen	8
Validierung Nachrichten-Inhalt (erlaubte HTML-Tags)	11
Antragsstatusmeldung einstellen	12
Fehlercodes	17

Präambel

Die Schnittstellenbeschreibung des Zentrales Bürgerpostfach (ZBP) beschreibt zwei grundlegende Aspekte:

- **Authentifizierung**
→ Die Authentifizierung und Autorisierung erfolgt im ZBP mittels Security-Token (JWT), das mit Hilfe eines ZBP PKI-Client-Zertifikats (Public Key Infrastruktur) erstellt wird.
- **Funktionsumfang der ZBP-Schnittstelle**
→ Es werden nur die Funktionen aus der aktuellen API Version beschrieben. Für die Beschreibung älterer API Versionen dienen die Schnittstellenbeschreibungen der älteren Version.
→ Die aktuelle API Version ist: **API v6**

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

Erläuterung Begriffe

Begriff der Dokumentation	Synonyme	Kürzel	Erläuterung
Zentrales Bürgerpostfach		ZBP	
Drittanwendung	Fachverfahren, Fachdienst, Dienstleistungen, Online-Leistungen, Onlinedienst	DA	Bei Drittanwendung wird nicht unterschieden, welchen Dienst/Aufgabe die andere Anwendung hat. Es ist nur wichtig, dass diese Anwendung in irgendeiner Form in Kontakt mit dem ZBP steht.
Fachdienst	Dienstleistungen, Online-Leistungen, Onlinedienst	FD	Der Fachdienst ist die Webseite, auf der der Bürger seinen Antrag stellt.
OnlineDienst	Fachdienst, Dienstleistungen, Online-Leistungen, Onlinedienst	OD	Der Onlinedienst ist die Webseite, auf der der Bürger seinen Antrag stellt.

Fachverfahren	Fachanwendung, Behörde	FV	Das Fachverfahren ist die Anwendung, die in der Behörde läuft und von Sachbearbeitern der Behörde verwendet wird. Hier wird die Bearbeitung des Antrags durchgeführt.
Fachanwendung	Fachverfahren, Behörde	FA	Die Fachanwendung ist die Anwendung, die in der Behörde läuft und von Sachbearbeitern der Behörde verwendet wird. Hier wird die Bearbeitung des Antrags durchgeführt.
Nutzerkonto	BundID	NK	
Bürger	der Benutzer, der Anwender		
Vertrauensniveau	Stork QAAA Level	VN	

Authentifizierung

JSON Web Token (JWT)

Die Authentifizierung und Autorisierung erfolgt im ZBP mittels JSON Web Token (JWT). Dieses Security-Token muss mit einem RSA512 Algorithmus und einem ZBP PKI-Client-Zertifikat signiert sein. Die maximale Token-Lebenszeit (Ablaufdatum - Erstellungsdatum) ist auf 30 Minuten begrenzt.

Übersicht der Angaben für die Erstellung des Security-Token:

createdDate	Erstellungsdatum
expiredDate	Ablaufdatum
Claim »signer«	Common Name (CN) des ZBP PKI-Client-Zertifikats
Claim »roles«	Der Inhalt »["THIRD_PARTY"]«

Beispiel Token-Erstellung

Third-Party Token

```
JWT.create()

    .withIssuedAt(createdDate) // createdDate = Erstellungsdatum

    .withExpiresAt(expiredDate) // expiredDate = Ablaufdatum

    .withClaim("signer", signer) // signer = CN (= common name) des ZBP PKI-Client-Zertifikats

    .withClaim("roles", List.of("THIRD_PARTY")) // roles = Rolle

    .sign(Algorithm.RSA512(publicKey, privateKey)); // Signierung des JWT
```

ZBP PKI-Client-Zertifikat

Die ZBP PKI-Client-Zertifikate werden zentral durch das Self Service Portal (SSP) ausgegeben, sobald dieses zur Verfügung steht. Um Zugang zum SSP zu erhalten, wird ein ELSTER-Organisationszertifikat benötigt.

Fachdienste und Fachverfahren können über das SSP neben produktiven ZBP Live-PKI-Client-Zertifikate auch Test-PKI-Client-Zertifikate (sog. Referenz-PK) beziehen und nutzen.

Jedes ZBP PKI-Client-Zertifikat muss durch das SSP über das ZBP Aussteller-CA erstellt worden sein und gewisse Vorgaben erfüllen. Die Verwendung eines nicht vom SSP erstellten PKI-Client-Zertifikats ist nicht möglich.

Das PKI-Client-Zertifikat wird ebenfalls als Client-Zertifikat für den Aufbau der SSL/TLS Verbindung verwendet und muss in jeder Anfrage an das ZBP als SSL Client Zertifikat mitgeschickt werden.

Funktionsumfang der Empfangsschnittstelle

Funktionsliste (API v6)

Funktion	HTTP-Methode + Endpunkt	Authentifizierung	Hinweise
Nachrichten einstellen	PUT /v6/mailbox/messages	ZBP PKI Client-Zertifikat und Security-Token (JWT)	Fachdienste und Fachverfahren können Nachrichten auf einer dedizierten Schnittstelle in einem Postkorb einstellen. Das Nutzerkonto wird über den Eingang einer neuen Nachricht informiert und kann im Folgenden den Bürger per E-Mail über den Eingang benachrichtigen.
Antragsstatusmeldung einstellen	POST /v6/applications/states	ZBP PKI Client-Zertifikat und Security-Token (JWT)	Fachdienste und Fachverfahren können Statusmeldungen zu einem Antrag mit Angabe der Antrags-ID einstellen. Es können mehrere Statusmeldungen desselben Status eingestellt werden. Dies dient dazu, um mittels der anderen Felder der Statusmeldung zusätzliche Informationen an den Bürger senden zu können (bspw. das Feld "Weitere Information").

Funktionsbeschreibung

Nachrichten einstellen

Um eine Nachricht in das ZBP einzustellen, muss der Sender über ein gültiges ZBP PKI-Client-Zertifikat verfügen. Mit dem Zertifikat kann der Sender einen entsprechenden Security-Token erstellen. 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 der Nachricht ist.

Ein Objekt zum Einstellen einer Nachricht besteht aus einem JSON-Objekt, welches mittels einer Checksumme signiert wird.

Dieses Objekt inkl. der Checksummen können beispielhaft folgendermaßen mithilfe gängiger Tools in der Linux-Shell berechnet werden:

```
# Checksummen aller Dateianhänge berechnen:
sha512sum <file-path>

# Dateigröße (contentLength) aller Dateianhänge ermitteln
ls -l <file-path>

# Checksumme des Nachrichteninhalts-JSONs (content) inkl. des Dateianhang-Arrays (attachments),
# die mit oben ermittelten Daten gefüllt wird
printf '{"mailboxUuid":"","stork_qaa_level":,"sender":"","title":"","content":"","service":"","retrievalConfirmationAddress":"","replyAddress":"","attachments":[{"filename":"<filename>","sha512sum":"<value-from-sha512sum-command>","contentLength":"<value-from-ls-command>"},"reference":"","senderUrl":""}] | openssl dgst -sha512 -sign <private-key-path> -out msg-digest.txt

# base64-Kodierung der Checksumme
base64 -w 0 msg-digest.txt

# Aufbau des Nachrichten-Objekts inkl. der Checksumme: Doppelte Anführungsstriche für Strings
# müssen mit einem \ "escaped" werden
curl -k -X 'PUT' \
  'https://<server-host>/v6/mailbox/messages' \
  -H 'accept: application/json' \
  -H 'Authorization: Bearer '<jwt-token>' \
  -H 'Content-Type: multipart/form-data' \
  -F 'json={"content":{"mailboxUuid":"","stork_qaa_level":"","sender":"","title":"","content":"","service":"","retrievalConfirmationAddress":"","replyAddress":"","attachments":[{"filename":"","sha512sum":"","contentLength":},"reference":"","senderUrl":"","sha512sum":"<output-from-base64-command>"}' \
  -F 'files=<file-path>@;type=<file-type>'
```


Im Folgenden wird alternativ der Aufbau einer Nachricht beispielhaft mit Java beschrieben:

Berechnung der Checksum der Anhänge:

sha512HexOfAttachments()

```
package org.apache.commons.codec.digest;

sha512HexOfAttachments(MultipartFile multipartFile) {
    String sha512Hex = DigestUtils.sha512Hex(multipartFile.getInputStream());
    return new CreateAttachmentDTO(multipartFile.getOriginalFilename(), sha512Hex, multipartFile.getSize());
}
```

Die Checksum über die gesamte Payload inkl. der Liste über die Anhänge mit ihren Checksums kann folgendermaßen berechnet werden:

signMessage()

```
package java.security;
package java.util;

signMessage(CertificateData certificateData, String message) {
    RSAPrivateKey key = (RSAPrivateKey) certificateData.getPrivateKey();
    Signature signature = Signature.getInstance("SHA512withRSA");
    signature.initSign(key);
    signature.update(message.getBytes(StandardCharsets.UTF_8));
    byte[] signed = signature.sign();
    return Base64.getEncoder().encodeToString(signed);
}
```

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 und erfüllt damit die Zustellfunktion.

Für neue Nachrichten werden jeweils eine Eingangsbenachrichtigungs-E-Mail über das Nutzerkonto an den betreffenden Bürger ausgelöst. Das ZBP verschickt selbst **keine** Eingangsbenachrichtigungen an Bürger. Das ist die Aufgabe des Nutzerkontos.

Die Menge der zugelassenen Anhänge ist derzeit prinzipiell beschränkt auf 25 MByte Gesamtgröße, in begründeten Ausnahmefällen kann nach Absprache mehr zugelassen werden. Die Anzahl der Anhänge darf nicht über 200 Stück liegen. Ein einzelner Anhang darf bis zu 25 MByte groß sein.

Eine Nachricht unterstützt folgende fachliche Parameter:

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

Beispiel Nachricht einstellen (mit Third-Party Token)

```
Request:
- 'accept: application/json'
- 'Content-Type: multipart/form-data'
- 'Authorization: Bearer {third-party token string}'

PUT {ZBP-URL}/v6/mailbox/messages
{
  "content":
  {
    "mailboxUuid":"dfc7[...]a0357b",
    "stork_qaa_level":1,
    "sender":"Test-Sender",
    "title":"Testnachricht 1",
```

```


    "content": "Testnachricht 1",
    "service": "Test-Service",
    "retrievalConfirmationAddress": "Test-Adresse",
    "replyAddress": "Test-Adresse",
    "attachments":
    [
      {
        "filename": "Test.pdf",

        "sha512sum": "f3b3ab3e6351e25b5c1882bea8d37efaddc0ea72bf153[...]c7fe93042d85b18b5b453e
        322d154bc55d5cc2754b0dfb4b2",
        "contentLength": 13264
      }
    ],
    "reference": "256100704",
    "senderUrl": "Test-URL",
    "applicationId": "i7j8k9l1[...]5g6h-1ab23c4f"
  },

  "sha512sum": "o7L9r1LIWhs61KdZnh[...]jOxDZmXo3sNxo/F8GwteoqjWOqmv2FaTrHNpGIBCI6yS4Y2
  S5QJ4PrGWyHjl6YM="
}

Response (HTTP 200):
{
  "mailboxHandle": "dfc7f[...]a0357b",
  "messageId": 170[...]12,
  "messageUuid": "0b385a[...]32abb8fba2"
}

```

-  Die Schnittstelle kann für dieselbe Nachricht mehrfach aufgerufen werden. Durch Prüfung der Signatur stellt das ZBP fest, ob exakt dieselbe Nachricht bereits im System des ZBP persistiert wurde. In diesem Fall antwortet die Schnittstelle mit HTTP-Status 200 (OK). Die Nachricht wird nur einmal im ZBP hinterlegt und kommt nicht mehrfach vor.

Validierung Nachrichten-Inhalt (erlaubte HTML-Tags)

Alle empfangenen Nachrichten werden inhaltlich auf enthaltene HTML-Tags validiert. Das ZBP lehnt Nachrichten ab, die unerlaubtes HTML enthalten. Die Felder, die validiert werden, sind:

- Absender (sender)
- Titel (title)
- Nachrichten-Text (content)
- Service (service)
- Referenz / Aktenzeichen (reference)

Die erlaubten HTML-Tags sind:

- Text Formatierung: b, i, u, strong, em, span, p
- Überschriften: h1, h2, h3, h4
- Listen: ul, ol, li
- Links & Bilder: a (mit "href", "rel", und "target" Attributen), img (mit "src" Attribut), button (mit "href" Attribut)
- Tabellen: table, td, tr
- Layout & Struktur: div, center, br, form, style, title, html, head, body


Werden nicht erlaubte HTML-Tags im Nachrichten-Inhalt identifiziert, erhält der Sender den Error-Response "ZBP_400_004: HTML contains forbidden tags or attributes." zurück.

Die Definitionen für die Validierung der HTML-Inhalte können mithilfe einer HTML-Policy XML-Datei angepasst und per Konfigurationsparameter auch ausgeschaltet werden.

Antragsstatusmeldung einstellen

Um eine Statusmeldung zu einem Antrag in das ZBP einzustellen, muss der Sender über ein gültiges ZBP PKI-Client-Zertifikat verfügen. Mit dem Zertifikat kann der Sender einen entsprechenden Security-Token erstellen. Die Adressierung des Postkorbs erfolgt über die ein-eindeutige Antrags-ID (engl. applicationId).

Mögliche Statuswerte für eine Statusmeldung

Statuswert in der Antragsfortschrittanzeige	String	Verpflichtend zu setzen	Zu setzen von	Erläuterung
Ausfüllen des Antrags begonnen	INITIATED		Onlinedienst	Gedacht für Onlinedienste, die Anträge zwischenspeichern können. Der begonnene Antrag ist nach Senden, dann bereits dem Bürger in der Antragsliste ersichtlich.

Antrag bei der Behörde eingereicht	SUBMITTED	✗	Onlinedienst	Gedacht für Onlinedienste; Sollte der Antrag vom Onlinedienst asynchron an das Fachverfahren übergeben werden oder der Antrag aus unbekanntem Grund nicht im Fachverfahren eingehen, kann man so aber erkennen, dass der Bürger den Antrag erfolgreich begonnen hat.
Antrag bei der Behörde eingegangen	RECEIVED	✓	Fachverfahren	Obligatorischer Status, der vom empfangenen Fachverfahren gesetzt werden soll, sobald der neue Antrag eingegangen ist.
Antrag wird geprüft	PROCESSING	✗	Fachverfahren	Der Bürger wird beim Antragsstatus "Eingegangen" annehmen, dass sein Antrag auch irgendwann bearbeitet wird. Eine Bestätigung, dass sich jetzt konkret ein Sachbearbeiter um den Antrag kümmert, ist jedoch ein großer Gewinn in Sachen Komfort und Akzeptanz der digitalen Behördenleistungen. Daher wird empfohlen, den Status zu verwenden.

Aktivität erforderlich	ACTION_REQUIRED	✗	Fachverfahren	<p>Das Fachverfahren sollte dem Bürger immer eine Nachricht im ZBP hinterlegen (inkl. der damit verbunden E-Mail-Benachrichtigung), wenn eine Aktivität seinerseits notwendig ist. Eine zusätzliche Visualisierung am Antrag selbst kann dies aber noch deutlicher hervorheben. Des Weiteren wird der Bürger damit auch daran erinnert, dass eine Aktivität seinerseits ggf. immer noch aussteht.</p> <p>Nach erfolgreicher Aktivität des Bürgers (bspw. Nachreichen von Dokumenten) sollte der Status wieder zurück auf "Antrag wird geprüft" gestellt werden.</p>
Antrag Abgeschlossen	COMPLETED	✓	Fachverfahren	<p>Der Status "Abgeschlossen" steht für die Beendigung des Antrags. Er stellt keine Aussage drüber dar, ob der Antrag des Bürgers "erfolgreich" war.</p>

Die Antrags-ID ist selbst Teil der Payload, damit diese auch Teil der Signatur der Statusmeldung ist. Die Signatur der Statusmeldung wird über die gesamte Payload berechnet.

Ein Objekt zum Einstellen einer Statusmeldung besteht aus einem JSON-Objekt, welches mittels einer Checksumme signiert wird.

Die Nachricht inkl. der Checksummen der Statusmeldung können beispielhaft folgendermaßen mithilfe gängiger Tools in der Linux-Shell berechnet werden:

Statusmeldung signieren

```
# Checksumme der Statusmeldung-JSON (content)
printf '{"applicationId":"93bc2fce-0242-43fa-8d1a-5a847edfc02a","status":"RECEIVED","additionalInformation":{"de":"Test 1"},"statusDetails":{"de":"Test 1"},"reference":"Test 1","publicServiceName":{"de":"Bundeswahlscheinverfahren"},"senderName":"Bundeswahlscheinverfahren","createdDate":"2024-01-14T12:23:21.223Z"}' | openssl dgst -sha512 -sign <Pfad-zum-privaten-Schlüssel> -out msg-digest.txt
```

```
# base64-Kodierung der Checksumme
base64 -w 0 msg-digest.txt
```

```
# Aufbau der Nachricht inkl. der Checksumme: Doppelte Anführungsstriche für Strings müssen mit
# einem \"escaped\" werden
curl -X 'POST' \
  'https://<server-host>/v6/mailbox/applications/states' \
  -H 'accept: application/json' \
  -H 'Authorization: Bearer <jwt-token>' \
  -d '{"content":{"applicationId":"93bc2fce-0242-43fa-8d1a-5a847edfc02a","status":"RE-
CEIVED","additionalInformation":{"de":"Test 1"},"statusDetails":{"de":"Test 1"},"refer-
ence":"Test 1","publicServiceName":{"de":"Bundeswahlscheinverfahren"},"sender-
Name":"Bundeswahlscheinverfahren","createdDate":"2024-01-
14T12:23:21.223Z"},"sha512sum":"<output-from-base64-command>"}
```

Im Folgenden wird alternativ der Aufbau einer Nachricht beispielhaft mit Java beschrieben:

signState()

```
package java.security;
package java.util;

signStateMessage(CertificateData certificateData, String stateMessage) {
    RSAPrivateKey key = (RSAPrivateKey) certificateData.getPrivateKey();
    Signature signature = Signature.getInstance("SHA512withRSA");
    signature.initSign(key);
    signature.update(stateMessage.getBytes(StandardCharsets.UTF_8));
    byte[] signed = signature.sign();
    return Base64.getEncoder().encodeToString(signed);
}
```

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 Statusmeldung als empfangen und geprüft. Der Sender kann sich auf den erfolgreichen Empfang verlassen und erfüllt damit die Zustellfiktion.

Für neue Statusmeldungen werden jeweils eine Eingangsbenachrichtigungs-E-Mail über das Nutzerkonto an den betreffenden Bürger ausgelöst. Das ZBP verschickt selbst **keine** Eingangsbenachrichtigungen an Bürger – das ist die Aufgabe des Nutzerkontos.

Eine Statusmeldung unterstützt folgende fachliche Parameter:

- Antrags-ID (Pflicht)
- Status (Pflicht)
- Antragsbezeichnung (Pflicht, maximal 100 Zeichen)
- Absender (Pflicht, maximal 100 Zeichen)

- Erstellungszeitpunkt (Pflicht)
- Details zum Status (Optional, maximal 50 Zeichen)
- Weitere Information (Optional, maximal 100 Zeichen)
- Referenz (Optional, maximal 50 Zeichen)

Es ist möglich eine Statusmeldung zu schicken, ohne den Status des Antrags zu verändern. Das ist bspw. der Fall, wenn die Behörde dem Bürger weiterführende Informationen mitteilen möchte, ohne den Status des Antrags selbst zu ändern.

Alle empfangenen Statusmeldungen werden inhaltlich auf enthaltenes HTML geprüft. Das ZBP lehnt Statusmeldungen ab, die HTML in einem der Felder enthalten. Wird HTML in einem der Felder identifiziert, erhält der Sender die Fehler-Response ZBP_400_001 "Value of the field 'de' in 'StatusDetailsDTO' is invalid (The value contains HTML)." zurück.

Beispiel Antragsstatusmeldung einstellen (mit Third-Party Token)

Request:

- 'accept: */*'
- 'Content-Type: application/json'
- 'Authorization: Bearer {third-party token string}'

POST {ZBP-URL}/v6/mailbox/applications/states

```
{
  "content":
  {
    "status":"ACTION_REQUIRED",
    "applicationId":"93bc2fce-0242-43fa-8d1a-5a847edfc02a",
    "additionalInformation":
    {
      "de":"Test 1"
    },
    "statusDetails":
    {
      "de":"Test 1"
    },
    "reference":"Test 1",
    "publicServiceName":
    {
      "de":"Bundeswahlscheinverfahren"
    },
    "senderName":"Bundeswahlscheinverfahren",
    "createdDate":"2024-01-14T12:23:21.223Z"
  },
  sha512sum:"PXBzslsrortU0AMQ[...]vNFSJ9ZOJdUk0FFews="
}
```

Response:

- HTTP 200

Fehlercodes

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

Fehlercode	Fehlertext	Beschreibung	Schnittstellen
ZBP_400_001	Invalid request body.	Die zu übertragende Nachricht im Body der Anfrage fehlt oder ist unvollständig.	Nachricht einstellen, Antragstatusmeldung einstellen
	Value of the field '{field-name}' in '{dto-name}' is invalid ({reason}).	Wert des Feldes '{field-name}' in '{dto-name}' is invalide ({reason}).	Nachricht einstellen, Antragstatusmeldung einstellen
ZBP_400_002	Multipart form is malformed.	Die Beschreibung der mehrteiligen Daten im multi-stream Format konnte nicht gelesen werden, da sie Fehler enthält.	Nachricht einstellen
ZBP_400_003	Invalid attachment type : {attachment-type}.	Der Dateityp {attachment-type} des hochgeladenen Anhangs ist ungültig.	Nachricht einstellen
ZBP_400_004	HTML contains forbidden tags or attributes.	Der Nachrichteninhalt enthält nicht erlaubte Tags oder Attribute.	Nachricht einstellen
ZBP_400_005	Attachment {filename} missing in json content.	Ein hochgeladener Anhang ist nicht im JSON der Nachricht referenziert.	Nachricht einstellen
ZBP_400_006	{field} missing for {filename} in Attachment in json content.	Ein Feld im Attachment-Teil der JSON Nachricht fehlt.	Nachricht einstellen
ZBP_400_007	Can't find {header-name} in Header.	{header-name} wurde nicht im Header gefunden.	Nachricht einstellen

ZBP_400_008	Duplicate filename in message: {filename}.	Die Nachricht enthält unerlaubt gleiche Anhangsdateien.	Nachricht einstellen
ZBP_400_012	Missing or incomplete message in body.	Die Validierung der Felder in einer Nachricht ist gescheitert.	Nachricht einstellen
ZBP_400_013	Unable to create Envelope / DTO object from the body, Incorrect json content.	Das JSON der Nachricht ist technisch nicht korrekt und konnte deshalb nicht geparkt werden.	Nachricht einstellen
ZBP_400_014	Message content is too long, allowed max length: %s.	Der Nachrichtentext ist in der Zeichenlänge zu lang, als der Wert der maximal erlaubten Zeichenlänge für Nachrichten, welcher in der ZBP-Konfiguration definiert ist.	Nachricht einstellen
ZBP_401_001	Malformed authorization token.	Der Autorisierungs-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.	Nachricht einstellen, Antragstatusmeldung einstellen
ZBP_401_002	Client token could not be validated.	Das Zertifikat für die spezifische Anfrage ist ungültig. Mögliche Ursachen: Das Zertifikat stammt nicht von der PKI oder das Zertifikat wurde von der PKI zurückgezogen.	Nachricht einstellen, Antragstatusmeldung einstellen
ZBP_403_001	Access Denied.	Der Token hat keine Berechtigung diese Ressource zu benutzen.	Nachricht einstellen, Antragstatusmeldung einstellen
ZBP_403_002	Given signature does not match with message content. Please re-sign and try again.	Die übertragene Prüfsumme stimmt nicht mit dem Nachrichteninhalte überein.	Nachricht einstellen

ZBP_404_003	Can't find this mailbox.	Das Postfach konnte nicht gefunden werden.	Nachricht einstellen,
ZBP_404_008	Can't find this application.	Der Antrag konnte nicht gefunden werden.	Nachricht einstellen, Antragsstatusmeldung einstellen
ZBP_409_001	No trust level.	Es wurde kein Trustlevel angegeben.	Nachricht einstellen, Antragstatusmeldung einstellen
ZBP_409_002	No subject in token.	Es wurde kein Subject (Nutzerkonto-ID) im Token angegeben.	Nachricht einstellen, Antragstatusmeldung einstellen
ZBP_409_003	Wrong trust level.	Das angegebene Trustlevel ist ungültig.	Nachricht einstellen, Antragstatusmeldung einstellen
ZBP_409_007	Invalid characters in case reference number.	Dies bedeutet, dass Ihre Fallreferenz-ID-Zeichenfolge eine nicht unterstützte Zeichencodierung enthält.	Nachricht einstellen
ZBP_409_008	Application reference number is too long.	Dies bedeutet, dass Ihre Fallreferenz-ID-Zeichenfolge mehr als 255 Zeichen hat.	Nachricht einstellen
ZBP_409_009	This state transition is not allowed.	Der übertragene Status ist zwar prinzipiell gültig, der Wechsel zu diesem Status ist aber nicht erlaubt.	Antragsstatusmeldung einstellen
ZBP_413_001	Number of allowed attachments exceeded.	Die Anzahl der erlaubten Anhänge wurde überschritten.	Nachricht einstellen
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 einstellen

ZBP_500_006	Error processing request.	Beim Verarbeiten der Anfrage ist ein Fehler aufgetreten.	Nachricht einstellen
ZBP_500_007	Error validating the message content.	Beim Überprüfen des Nachrichteninhalts auf unerlaubtes HTML ist ein interner Fehler aufgetreten.	Nachricht einstellen
ZBP_500_011	Internal server error occurred.	Ein interner Serverfehler ist aufgetreten.	Nachricht einstellen, Antragstatusmeldung einstellen
ZBP_500_012	Please check logs for more information.	Bitte überprüfen Sie die Logs für weitere Informationen.	Nachricht einstellen, Antragstatusmeldung einstellen
ZBP_503_001	Error uploading to file storage.	Beim Hochladen der Datei zum Dateiserver ist ein Fehler aufgetreten.	Nachricht einstellen

