Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ

Anhang 3 der Verordnung des Eidgenössischen Justiz- und Polizeidepartements (EJPD) über die Erstellung elektronischer öffentlicher Urkunden und elektronischer Beglaubigungen (EÖBV-EJPD; SR 211.435.11)

Technische Anforderungen zur Vermittlung des Zugriffs auf das UPReg

Version: 1

Inkrafttreten: 01.02.2018

Inhaltsverzeichnis

1. Allgemeines

1.1. Grundlage

Die vorliegenden Vorschriften bilden Anhang 3 der EÖBV-EJPD [2]. Sie stützen sich auf Artikel 10 Absatz 4 und Artikel 20 EÖBV [1] sowie auf Artikel 9 Absatz 1 und Artikel 10 EÖBV-EJPD [2].

1.2. Gegenstand

Der Kontakt zwischen dem von der Urkundsperson verwendeten Informatiksystem und dem UPReg kann durch Dritte vermittelt werden (Art. 10 Abs. 4 EÖBV [1]). Das Schweizerische Register der Urkundspersonen (UPReg) bietet Dritten die technische Möglichkeit, Zulassungsbestätigungen (Art. 2 Bst. a EÖBV [1]) abzurufen (Art. 9 Abs. 1 EÖBV-EJPD [2]). Dritte bedürfen dabei einer Bewilligung des Bundesamtes für Justiz (BJ).

Das vorliegende Dokument führt insbesondere die technischen Anforderungen auf, die zur Erteilung der Bewilligung nach Artikel 20 Absatz 1 Buchstabe b EÖBV-EJPD [2] erfüllt sein müssen (vgl. dazu Kapitel 1.4). Darüber hinaus enthält das vorliegende Dokument auch Informationen zur Funktionsweise der UPReg-Schnittstelle zur Ausgabe von Zulassungsbestätigungen an Urkundspersonen.

1.3. Geltungsbereich

Die im Kapitel 1.4 aufgeführten Vorgaben richten sich an Dritte, die den Zugriff auf das UPReg für den Abruf von Zulassungsbestätigungen zu vermitteln beabsichtigen. Im Folgenden ist zur Bezeichnung der Dritten der Einfachheit halber allgemein von «Gesuchsteller» die Rede.

1.4. Gegenstand der Prüfung im Rahmen des Bewilligungsverfahrens

Das Gesuch um Bewilligung, den Zugriff auf das UPReg zu vermitteln, muss die Angaben enthalten, wie die folgenden Vorgaben erfüllt sind (Art. 10 Abs. 2 EÖBV-EJPD [2]):

1. Den Nachweis der Erfüllung der Kriterien für den Betrieb nach Kapitel 2.
2. Die technische Implementation:
    a) der Grundanforderungen des Web-Services nach Kapitel 3;
    b) der *Representational State Transfer*-Schnittstellen (REST-Interfaces) für die Zulassungsbestätigung gemäss Kapitel 4.

Das BJ prüft das Vorliegen der technischen Anforderungen theoretisch und praktisch. Vor der produktiven Inbetriebnahme ist die Funktionsfähigkeit in der Praxis dem BJ anhand von elektronischen öffentlichen Urkunden mit Beispieltexten auf der Integrationsumgebung zu belegen. Das BJ stellt dazu einen Zugang auf das Testsystem zur Verfügung. Durch den Funktionstest wird sichergestellt, dass die Anforderungen der Kapitel 3 und 4 sowie 6 erfüllt sind.

Der Dritte prüft auf der Produktivumgebung nach Absprache mit dem BJ zum erstmöglichen Zeitpunkt die Funktionalität mit einer echten Urkundsperson und informiert das BJ umgehend über die Ergebnisse. Das Aufbieten einer Urkundsperson zum Ausführen einer Funktionsprüfung ist Sache des Dritten. Weiter ist durch den Dritten der Nachweis zu erbringen, dass die

Verfügbarkeit der Plattform einsehbar ist. Diese muss aktuell gehalten werden und das BJ ist periodisch zu informieren.

1.5. Kurzbeschreibung der Funktionsweise

Die Funktionalität wird über sogenannte *Representational State Transfer*–Services (kurz: REST–Services) angeboten. Die Urkundsperson ruft anhand von Informationen aus ihrer Signatur über einen Dritten die Zulassungsbestätigung beim UPReg ab. Die Ausgabe und das Anbringen der Zulassungsbestätigung richten sich nach den Artikeln 12 und 13 EÖBV-EJPD [2].

1.6. Referenzen

[1] Verordnung über die Erstellung elektronischer öffentlicher Urkunden und elektronischer Beglaubigungen (EÖBV; SR 211.435.1)

[2] Verordnung des EJPD über die Erstellung elektronischer öffentlicher Urkunden und elektronischer Beglaubigungen (EÖBV-EJPD; SR 211.435.11)

2. Kriterienkatalog für die zur Vermittlung von Zulassungsbestätigungen aus UPReg durch Dritte

2.1. Vermittlung von Zulassungsbestätigungen durch Gesuchsteller

Bei der Vermittlung von Zulassungsbestätigungen authentisiert sich der Dritte gegenüber UPReg. Dabei werden Angaben aus der Signatur der Urkundsperson an UPReg übermittelt, welche eine zweifelsfreie Identifikation der Urkundsperson erlauben. UPReg übergibt dem Dritten die entsprechende Zulassungsbestätigung, welche nur im Zusammenhang mit der erwähnten Signatur der Urkundsperson verwendet werden kann.

2.2. Grundanforderungen für private Dienstleistungserbringer und Behörden

2.2.1. Management des Betriebs und der Kommunikation:

- Entwicklungs-, Test- und Produktionsplattformen müssen voneinander getrennt werden.

- Bei Verwendung von Passwörtern darf der Anbieter diese nicht auf Dauer speichern oder in Logfiles protokollieren. Ist die Speicherung der Passwörter von technischen Benutzern unvermeidbar, müssen diese Passwörter auf eine andere Weise gleichwertig und nachweislich wirksam geschützt werden.

- Die eingesetzten kryptografischen Verfahren und Systeme müssen dem Stand der Technik entsprechen und sich an der aktuellen Bedrohungslage orientieren. Vorzugsweise sind standardisierte Verfahren und Systeme einzusetzen.

- Um *Offline Password Guessing* zu verhindern, ist für die Übertragung eine Nachrichtenverschlüsselung mit Schlüsseln, die von Passwörtern abgeleitet werden, nicht zugelassen.

- Die Stärke der eingesetzten kryptografischen Verfahren und Systeme muss im Rahmen einer ganzheitlichen Sicherheitsarchitektur vollständig und nachvollziehbar beschrieben sowie periodisch überprüft und gegebenenfalls angepasst werden.

2.2.2. Zugriffskontrolle

- Der Zugriff auf die Plattform darf nur über starke Authentifikationsverfahren (z.B. digitale Zertifikate oder persönliche Tokens) erfolgen. Dabei sind starke Authentifikationsverfahren solche im Sinne von Kapitel 5.2 bis 5.5 der Ausführungsbestimmungen «Zugriffsmatrix» zu Kapitel 3.1 der Weisungen über die Informatiksicherheit in der Bundesverwaltung WIsB, vom 1. Juli 2015 zu verstehen. Insbesondere darf die Authentifikationsinformation nicht im Klartext übertragen werden, um nicht verwundbar gegenüber Abhorchungs- und Wiedereinspielungsangriffen zu sein.

- Werden im Authentifikationsverfahren Passwörter eingesetzt, müssen diese immer über verschlüsselte Verbindungen übertragen werden (z.B. im Rahmen einer SSL/TLS Session). Werden im Authentifikationsverfahren ausschliesslich Passwörter eingesetzt, müssen diese in Bezug auf die Passwortstärke den Anforderungen von Kapitel 8 des «IKT-Grundschutz in der Bundesverwaltung» vom 1. März 2017 zu Kapitel 3.1 der Weisungen über die Informatiksicherheit in der Bundesverwaltung WIsB genügen. Auf eine zeitliche Beschränkung der Gültigkeit von Passwörtern kann verzichtet werden.

2.2.3. Beschaffung, Entwicklung und Wartung von Plattformkomponenten

- Server, die vom Internet her erreichbar sind, müssen bedarfsgerecht gehärtet sein.

- Die bekannten Angriffe gegen Web-Anwendungen, wie sie z.B. vom Open Web Application Security Project (OWASP) dokumentiert werden, müssen erfolgreich abgewehrt werden können.

2.3. Anforderungen an das IT Service Management

2.3.1. Anforderungen

Für den zuverlässigen Betrieb von Plattformen muss nachgewiesen werden, dass die folgenden Betriebsprozesse dokumentiert, eingeführt, betrieben, permanent überwacht, periodisch geprüft, unterhalten und verbessert werden:

- Service Lieferprozesse
- Management von Serviceniveaus
- Service Berichtswesen
- Servicekontinuitäts- und -verfügbarkeitsmanagement
- Budgetierung und Verrechnung von Services
- Kapazitätsmanagement
- Prozesse zum Beziehungsmanagement
- Pflege der Beziehung zwischen Leistungserbringern und Kunden
- Lieferantenmanagement
- Prozesse zur Lösung von Störungen und Problemen
- Behandlung von Störungen (Vorfällen)
- Behebung von Problemen

- Steuerungs- und Überwachungsprozesse
- Konfigurationsmanagement
- Veränderungsmanagement
- Freigabe- und Bereitstellungsmanagement

Die Betriebsprozesse müssen sich an den internationalen Standards ISO/IEC 20000-1:2011 (Information technology – Service management – Part 1: Service management system requirements) und ISO/IEC 20000-2:2012 (Information technology – Service management – Part 2: Code of practice) oder an vergleichbaren Standards orientieren.

Zusätzlich muss ein professioneller Service Desk eingeführt, betrieben, permanent überwacht, periodisch geprüft, unterhalten und verbessert werden.

2.3.2. Verfügbarkeit

Grundsätzlich muss eine Plattform an allen Werktagen durchgängig mindestens während der gewöhnlichen Arbeitszeiten zur Verfügung stehen. Es sind Massnahmen zu ergreifen, dass die Ausfallzeit bei Störungen wenige Minuten nicht überschreitet. Allfällige Servicefenster sind ausserhalb der gewöhnlichen Arbeitszeiten zu planen. Die Verfügbarkeit einer Plattform muss protokolliert und das Protokoll über die Plattform veröffentlicht werden.

2.4. Zusatzanforderungen an die Informationssicherheit bei der Ausgabe von Zulassungsbestätigungen für private Dienstleistungserbringer

Die Informationssicherheit ist durch folgende Methode zu gewährleisten:

Durch Einrichtung, Implementierung, Betrieb, Überwachung, Überprüfung, Wartung und Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) nach ISO/IEC 27001:2013 (Information technology – Security techniques – Information security management systems – Requirements).

Der Anwendungsbereich des ISMS muss alle diejenigen Organisationseinheiten des Dritten umfassen, die rechtlich, administrativ und betrieblich für dessen Tätigkeit im Zusammenhang mit der Vermittlung des Zugriffs auf das UPReg für den Abruf von Zulassungsbestätigungen verantwortlich sind. Eine Beschränkung des Anwendungsbereichs auf den rein technischen Betrieb durch einen internen oder externen IT-Dienstleistungserbringer ist nicht zulässig.

Die Wirksamkeit und Angemessenheit des ISMS muss durch die Vorlage des durch eine Zertifizierungsstelle ausgestellten Zertifikats, das die Zertifizierung des ISMS nach ISO/IEC 27001:2013 bescheinigt, nachgewiesen werden. Die Zertifizierungsstelle muss durch die Schweizerische Akkreditierungsstelle (SAS) für die Durchführung von ISO/IEC 27001:2013 Audits akkreditiert sein.

3. Grundanforderungen des Web-Services

Die Web-Services sind allesamt als RESTful Web-Service definiert. Für das Messaging wird HTTP 1.1 und als Datenaustauschformat JSON verwendet.

3.1. Login und Berechtigung

Die clientseitige Authentisierung findet mittels Mutual Authentication auf Basis von HTTPS und X.509 Zertifikaten statt.

Eine Authentisierung findet bei jedem Server Round-Trip statt.

Für die Authentisierung gegenüber einem Client (Computersoftware, wie zum Beispiel Local-Signer) muss ein sicheres Identifikationsmittel verwendet werden. Als solche gelten ein zu einem qualifizierten Zertifikat gemäss ZertES gehörendes Authentisierungszertifikat (z. B. das Authentisierungszertifikat der SuisseID) oder ein anderes gemäss ZertES zugelassenes, geeignetes Identifikationsmittel. Bei allen Interaktionen mit dem Web-Service wird das Zertifikat mitgeschickt und ist für den Web-Service auslesbar. Weiter muss im HTTP Header das Feld „User-Agent“ vorhanden sein. Der Client Software Name und die Version müssen korrekt gesetzt sein.

3.2. HTTP Status Codes

Der Web-Service liefert die folgenden Standard HTTP Status Codes zurück:

Status Code	Bedeutung
200	Die Operation ist vom Server verarbeitet worden.
400	Bad request (Syntaxfehler). Dies tritt z.B. bei einem nicht eingegebenen Parameter auf oder wenn der Parameter fehlerhaft ist (Format, Typ).
401	Unauthorized (Nicht autorisiert). Tritt auf, falls das Login fehlschlägt (das Benutzer-Zertifikat ist in der Datenbank nicht vorhanden) oder falls der Benutzer keine Berechtigungen hat, die aktuelle Operation auszuführen.
403	Forbidden (Zugang verboten). Es darf nicht auf die Ressource zugegriffen werden.
404	Not found (Ressource existiert nicht). Z.B. die Adresse ist falsch.
405	Method not allowed. Wird zurückgeliefert, wenn die falsche HTTP-Methode verwendet wird. Z.B. wenn der gesendete HTTP Request kein GET war, aber nur dies unterstützt wird.
500	Internal Server Error. Wird zurückgesendet, wenn serverseitig ein Fehler aufgetreten ist.

4. REST-Interface für die Zulassungsbestätigung

4.1. Methode *login*

Die Methode login dient zur Authentisierung eines Clients. Der Aufruf dieser Methode ist optional, da bei jedem Server-Round-Trip eine Authentisierung vorgenommen wird. Diese Methode dient der Clientsoftware als Test, ob eine eindeutige Identifikation möglich ist (über Authentisierungszertifikat; allenfalls über ein anderes Werkzeug gemäss Artikel 7 Absatz 1 Buchstabe i EÖBV [1] oder im Fall der Vermittlung des Registerzugriffs über einen Dritten, über dessen Identifikation), und ob die Urkundsperson im Register vorhanden ist. Im Folgenden wird der einfachen Lesbarkeit halber vom Authentisierungszertifikat gesprochen.

4.1.1. Aufruf

```
GET /CONTEXT-ROOT/nachweis/login
```

4.1.2. Antwort

Nur HTTP Status-Code ist relevant. Dieser hat folgende Bedeutung:

Status-Code	Bedeutung
200	Es besteht ein Benutzer mit einer momentan aktiven Funktion, welcher das zur Authentisierung verwendete Zertifikat zugeordnet ist und momentan verwendet wird.
401	Es besteht kein Benutzer mit einer momentan aktiven Funktion, welcher das zur Authentisierung verwendete Zertifikat zugeordnet ist und momentan verwendet wird.

4.2. Methode *rt1-generate* (RT1)

Beim ersten Round-Trip wird dem Server das PKCS#7-Objekt der Signatur geliefert, für welche eine Zulassungsbestätigung angebracht werden soll. Auch werden alle für die Identifikation der Urkundsperson benötigten Informationen und untenstehenden Daten übermittelt.

Diese Methode liefert die gerenderte, einzubettende Grafik der Zulassungsbestätigung und zusätzliche Informationen zurück.

4.2.1. Aufruf

```
POST /CONTEXT-ROOT/nachweis/rt1-generate
```

Es wird ein JSON im HTTP Body übermittelt. Im Header muss folgendes stehen:

```
Content-Type: application/json
```

JSON Attribut	For-mat	Defau lt Wert	Beschreibung
pkcs7	String /PKC S7/PE M		Das PKCS#7 enthält das PDF Signatur Zertifikat mit dem signierten Hash. PKCS#7 im PEM Format. Es muss die gesamte Zertifikatskette vorhanden sein. Und zusätzlich noch ein Zeitstempel eines TSAs. Das PEM darf keine Steuerzeichen (z.B. newlines) aufweisen.
hash	String		Wert der kryptografischen Hashfunktion der unsignierte PDF Datei (wird in den Verordnungen als «kryptographische Prüfsumme» bezeichnet). Er liegt in Form einer hexadezimalen Zeichenfolge vor. Die PKCS#7 Struktur (Parameter pkcs oben) wurde unter Verwendung dieses Wertes erstellt.
revision	Inte-ger		Revisionsnummer des PDF Dokuments, für welches ein Funkti-onsnachweis erstellt werden soll. Es handelt sich um eine natür-liche Zahl. Die Zulassungsbestätigung ist nur für die angege-bene Revision gültig.
domain	String		Filter für die Domäne, welche verwendet werden soll. Z.B. „up-reg“.
canton	String		Filter für den Kanton, welcher verwendet werden soll. Z.B. „BE“ oder „VD“.
au-thCert-Base64	String		Optional. Falls ein Client eine Zulassungsbestätigung vermitteln möchte. Base64 Certificate DER/Binary.

4.2.2. Antwort

Die Antwort wird als JSON mit dem HTTP Status-Code 200 zurückgeliefert.

JSON Attribut	Format	Bescheibung
uuid	String	UUID Version 4 (zufällig generierte UUID). Wird bei der Me-thode *rt2-sign* benötigt.
signatureReason	String	String, welcher im PDF als SignatureReason bei der Signatur übereinstimmend hinterlegt werden muss (siehe unten).
certChain	PEM	Zertifikatskette der Server-Signatur (X.509 Zertifikate). Mit die-sem Zertifikat wird in *rt2-sign* signiert.
imageB64	Base64	Gerendertes, einzubettendes Bild der Zulassungsbestätigung im PNG-Format Base64 kodiert.
layout	Objekt	Anweisungen für die Platzierung der Signatur.
leftPos	Integer	Abstand vom linken Seitenrand in Pixel bei 72dpi.

topPos	Integer	Abstand vom unteren Seitenrand in Pixel bei 72dpi
page	Enumeration	Seite, auf der die Zulassungsbestätigung angebracht werden muss: FIRST: auf der ersten Seite; PENULTIMATE: auf der vorletzten Seite; ULTIMATE: auf der letzten Seite.

4.2.3. Von Dritten vermittelter Abruf von Zulassungsbestätigungen

Eine Besonderheit ergibt sich für von Dritten vermittelte Abrufe von Zulassungsbestätigungen. Hierbei können von einem Dritten Zulassungsbestätigungen für eine Urkundsperson beantragt werden. In diesem Fall wird nicht das Authentifizierungszertifikat von der Mutual Authentication für die Zulassungsbestätigung verwendet, sondern das Zertifikat, welches bei RT1 in der Property *authCertBase64* übermittelt wird. Dieses Zertifikat wird dann wie das Authentisierungszertifikat des Standardfalls behandelt.

Da der Abruf der Zulassungsbestätigung für Dritte einer Bewilligung des BJ bedarf (Art. 20 Abs. 1 Bst. b EÖBV [1]), muss das Zertifikat, welches für die Mutual Authentication verwendet wird, in der Datenbank von UPReg eingetragen sein.

4.2.4. SignatureReason

Die *SignatureReason* (Grund für die Signatur) sind Informationen, welche unter dieser Bezeichnung beim Signieren des PDFs hinterlegt werden müssen. Der entsprechende String muss buchstabengetreu hinterlegt werden. Beim String muss es sich um eine JSON Datenstruktur handeln, die maschinell ausgewertet werden kann.

4.2.4.1. Aufbau

JSON Tag		Beschreibung
v		Die momentane Version dieser Struktur.
c3p		Optional. Issuer und Seriennummer des Authentication Certificates. Wird nur gesetzt, wenn ein Drittanbieter eine Zulassungsbestätigung für eine Urkundsperson erstellt.
c		Seriennummer des Signaturzertifikates (aus PKCS#7-Struktur des RT1).
t		Transaktions-UUID. Die Transaktion besteht aus den Operationen RT1 und RT2.
h		SHA-256 Hash des generierten Bildes bei RT1.
f		Liste der momentan gültigen Funktionen dieser Person, denen das verwendete Zertifikat zugeordnet ist.
	fd	Domäne, in welcher die Funktion gültig ist.

	fi	Funktions-ID.
	fk	Kanton, in welchem die Funktion gültig ist, z.B. *BE.*
	fb	Volle Funktionsbeschreibung, z.B. *Notar / Notaire.*
	fo	UID der Organisation, an welche die Funktion gebunden ist.
	fp	Personen-ID der Person, welcher diese Funktion zugeordnet ist.

4.2.4.2. Personen- und Funktionsidentifikator

Die vom liefernden Register stammenden Personen- und Funktionsidentifikatoren sind nur innerhalb des liefernden Registers und (allenfalls) der entsprechenden Domäne eindeutig. Damit die Identifikatoren über alle liefernden Register eindeutig werden, wird in der signatureReason dem Identifikator des liefernden Registers das Kantonskürzel des Standorts des liefernden Registers vorangestellt. Identifikator und Kantonskürzel sind mittels Schrägstrich getrennt.

```
Kantonskürzel/ Identifikator des Registers
```

Beispiele für IDs:

```
BE/1d32b4bc-b923-4615-9233-8bcbc5223a77

VD/19837

TI/a:12-kjv
```

4.2.4.3. Beispiel

Beispiel der JSON Struktur. Hier ist das Attribut *c3p* vorhanden, es handelt sich also um das Beispiel einer Zulassungsbestätigung:

```
{
  "v":   2,
  "c3p": "CN=SwissSign SuisseID Platinum CA 2010 - G2,O=SwissSign AG,C=CH-
          68e7efa97226563b26865495db53d2",
  "c":   "a38913a67b137b91",
  "t":   "41fd7eca-9bf6-48ff-82e6-eb049260f162",
  "h":
"f0f5db86868e794679c7251475bbf63ed029d2dcc49a1987b1f5ecb2df0f898d",
    "f":   [
      {
        "fd": "upreg",
        "fi": "BE/10001",
```

```
            "fk": "BE",

            "fb": "Notar/in - Notaire",

            "fo": "CHE-107450801"

            "fp": "BE/1d32b4bc-b923-4615-9233-8bcbc5223a77",


        }

   ]

}
```

4.3. Methode *rt2-sign* (RT2)

Diese Methode signiert den übergebenen Hashwert. Die zurückgegebene Signatur (PKCS#7 Struktur) enthält Informationen (Transaktions-ID, Informationen über verwendetes Signaturzertifikat etc.), welche sich auf die Signatur der Urkundsperson beziehen. Diese Informationen werden vom Validatorsystem (Art. 17 EÖBV-EJPD [2]) ausgewertet, um die Gültigkeit der Zulassungsbestätigung zu überprüfen.

4.3.1. Aufruf

```
GET /CONTEXT-ROOT/nachweis/rt2-sign
```

Im HTTP Body muss ein JSON mit folgenden Attributen vorhanden sein.

Parameter	Parametertyp	Beschreibung
revision	Integer	Muss gleich dem Parameter *revision* + 1 in RT1 sein.
uuid	String	Ist die UUID, welche der Client bei der Antwort von RT1 erhalten hat.
hash	String	Wert der kryptografischen Hashfunktion der aktuellen PDF Revision.
freeOfCharge	String	Optional. Falls ein Client eine Zulassungsbestätigung vermitteln möchte; bei Präsenz des Parameters wird die angeforderte Zulassungsbestätigung von Gebühren befreit.

4.3.2. Antwort

Die Antwort wird als JSON mit dem HTTP Status-Code 200 zurückgeliefert.

Attribut-Name	Format	Beschreibung
pkcs7	PKCS7/PEM	PKCS#7 Struktur im PEM Format; enthält die Serverzertifikate sowie den signierten Hashwert aus dem Request.

4.4. Fehlercodes

Sofern auf einen Request kein HTTP Status-Code 200 zurückgeliefert wird, wird eine JSON-Struktur zurückgeliefert, welche den Fehler genauer spezifiziert. Dies erfolgt mit einem eindeutigen Fehlercode, welchen der Client auswertet und somit benutzerfreundlich auf dem UI visualisieren kann.

Diese Fehlercodes können bei den Methoden login, RT1 und RT2 auftreten und müssen dementsprechend behandelt werden.

4.4.1. Antwort

Parameter	Parameter-typ	Beschreibung
httpStatus	Integer	Entspricht dem HTTP Status-Code. Grundsätzlich: 4xx: Entspricht einem Client-Fehler; das Problem sollte ohne Support vom Betreiber lösbar sein; 5xx: Entspricht einem Server-Fehler; Support vom Betreiber notwendig.
errorCode	String	Definierter Fehler; über ein Mapping kann der Fehlercode in eine benutzerfreundliche Nachricht gewandelt werden.
description	String	Eine Beschreibung des Fehlers; diese sollte nicht direkt dem Benutzer angezeigt werden, da diese meistens Exception.get-Message() entspricht.
exception Class	String	Name der Exception-Klasse, von welcher der Fehler ausgelöst wurde.

4.4.2. Fehler-Codes

Es kann nicht garantiert werden, dass eine der untenstehenden Angaben geliefert werden kann. Sofern bei einem Fehler (HTTP Status Code ≠ 200) der Content-Type `application/json` gesetzt ist, kann der Inhalt ausgelesen (geparst) werden. Wird jedoch z.B. das Zertifikat vom Reverse Proxy oder Applikationsserver von UPReg nicht akzeptiert, dann wird dementsprechend eine Fehlermeldung dieser Software generiert, welche keine JSON Informationen enthält.

Folgende Tabelle beschreibt mögliche Fehler. Der Wert in der Spalte Name entspricht dem Wert im Feld `errorCode` der Antwort, der Wert in der Spalte Status Code entspricht dem Wert im Feld `httpStatus`.

Name	Status-Code	Beschreibung
ERR_MISSING_REQUIRED_PARAM	402	Ein benötigter Parameter fehlt.
ERR_INVALID_DATA	404	Mindestens ein Parameter weist einen ungültigen Wert

		auf. Z.B. PKCS#7 Struktur im falschen Format.
ERR_INVALID_HASH	405	Bei RT1: Der Hashwert stimmt nicht mit dem Hashwert in der PKCS#7 Struktur überein.
ERR_SIGN_CERT_NOT_FOUND	406	Das Signaturzertifikat wurde in der PKCS#7 Struktur nicht gefunden.
ERR_FN_MANY_PERSON_FOR_CERTIFICATE	408	Konsistenzfehler. Das gleiche Zertifikat ist mehreren Personen zugeordnet.
ERR_FN_NO_PERSON_ WITH_THIS_CERTIFICATE	409	Es existiert keine Person mit diesem Zertifikat.
ERR_FN_NO_RELEVANT_ RELATIONSHIPS_ACTIVE	410	Es existiert keine aktive Funktion mit diesem Zertifikat.
ERR_FN_PERMISSION_DENIED	411	Zertifikat vom Server akzeptiert. Jedoch ist der Benutzer nicht in der Datenbank registriert. Oder nicht aktiviert zum aktuellen Zeitpunkt.
ERR_TIMEOUT_BETWEEN_RT1_RT2	412	RT2 muss in einem Zeitfenster nach RT1 aufgerufen werden. Dieser Fehler tritt auf, wenn das Zeitfenster überschritten wurde, also zu viel Zeit zwischen RT1 und RT2 verstrichen ist.
ERR_UNKOWN_UUID_AT_RT2	413	Der UUID Parameter, welcher bei RT2 übergeben wurde, ist nicht bekannt. Problem: RT1 wurde nicht aufgerufen oder es wird eine falsche bzw. modifizierte UUID benutzt. Es muss die UUID bei RT2 übergeben werden, welche bei RT1 vom Server geliefert wurde.
ERR_INVALID_REVISION_NUMBER	414	Die Revisionsnummer, welche in RT1 angegeben wurde, wurde in RT2 nicht genau einmal inkrementiert.
ERR_MISSING_RT1_CALL_BEFORE_RT2	415	RT2 wurde aufgerufen, ohne vorgängig RT1 aufzurufen.
ERR_FN_PDF_SIGN_CERT_NOT_KNOWN_FOR_USER	416	Das Zertifikat, mit welchem das PDF signiert wurde (bei RT1 übergeben), wurde nicht bei der Person gefunden. Das Signaturzertifikat gehört nicht zu der Person, welche

		den Service RT1 aufgerufen hat.
ERR_FN_DISCRETE_VALIDATOR_NOT_VALID	417	Die bei RT1 in der PKCS#7 Struktur gelieferte Signatur ist nicht qualifiziert gemäss ZertES.
ERR_SIGDATE_BEFORE_REGISTER_ACTIVATION	419	Das Signaturdatum liegt vor dem Inkrafttreten der EÖBV für das entsprechende Register.
ERR_SIGCERT_AUTHCERT_MISMATCH	420	Die Signatur der Autorisierung und der Signatur gehören nicht zu derselben Funktion.
ERR_INT_UNKOWN	500	Es ist ein interner Serverfehler aufgetreten. Fehler ist nicht genauer spezifiziert.
ERR_INT_SERVICE_CALL_FAILED	502	Der Service Call warf eine Exception, die auf einen Konfigurationsfehler von upreg.ch schliessen lässt. Z.B. ungültige URL, Proxy, Authentication etc. Die Konfiguration von upreg.ch muss angepasst werden.
ERR_INT_SERVER_DOWN	503	Der Server ist überlastet.

4.5. Methode *ping*

Diese Methode dient ausschliesslich dazu, um die Mutual Authentication / 2Way SSL Funktionalität zu prüfen. Es ist ein Test, ob das Client Zertifikat (Mutual Authentication) vom Reverse Proxy und vom Applikationserver von UPReg akzeptiert werden bzw. ob diese korrekt in die Truststores von upreg.ch eingefügt wurden.

4.5.1. Aufruf

```
GET /CONTEXT-ROOT/nachweis/ping
```

4.5.2. Antwort

Nur der Status Code ist relevant. Es wird kein Content zurückgeschickt. Falls der Service antwortet, wird mit dem HTTP Status-Code 200 geantwortet.

5. Updateservice für Kantons- und Domänenliste

5.1. Methode *update*

In RT1 muss der Kanton und die Domäne angegeben werden, für welche die Zulassungsbestätigung ausgestellt werden soll. Die Liste der Kantone wird sich wohl eher selten ändern, diejenige der Domänen hingegen öfters. Damit bei der Einführung einer neuen Domäne nicht alle Clientsysteme manuell informiert und aktualisiert werden müssen, wird ein Service zur automatischen Aktualisierung dieser Liste bereitgestellt.

5.1.1. Aufruf

```
GET /CONTEXT-ROOT/list/update
```

5.1.2. Antwort

Als Antwort wird als *application/xml* die Datei mit den beiden Listen Kantone und Domänen zurückgeschickt. Diese UTF-8 kodierte XML Datei entspricht folgender Definition.

```
<?xml version="1.0"?>

<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
    targetNamespace="http://www.glue.ch/localsigner/zulabconfiguration"
    xmlns="http://www.glue.ch/localsigner/zulabconfiguration" elementFormDefault="qualified">

    <xs:element name="config">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="comment" type="xs:string" minOccurs="0"/>
                <xs:element name="cantons" type="cantonsType"/>
                <xs:element name="domains" type="domainsType"/>
            </xs:sequence>
            <xs:attribute name="version" type="xs:dateTime"/>
        </xs:complexType>
    </xs:element>

    <xs:complexType name="cantonsType">
        <xs:sequence>
            <xs:element name="canton" type="entryType" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="domainsType">
        <xs:sequence>
            <xs:element name="domain" type="entryType" minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="entryType">
        <xs:sequence>
            <xs:element name="value" type="xs:string"/>
            <xs:element name="translations" type="i18nType"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="i18nType">
        <xs:sequence>
            <xs:element name="german" type="xs:string"/>
            <xs:element name="french" type="xs:string"/>
            <xs:element name="italian" type="xs:string"/>
        </xs:sequence>
    </xs:complexType>
</xs:schema>
```

6. Zulassungsbestätigung

6.1. Datenstruktur Zulassungsbestätigung Version 1 & 2

Im `Reason`-Feld der Signatur der Zulassungsbestätigung ist eine JSON-Struktur eingebettet, die Metainformationen über die Person und deren Funktionen gibt, an welche das für die Signatur verwendete Zertifikat gebunden ist.

JSON Schlüssel		Beschreibung
`v`		Wert: „`1`“. Die Version dieser Struktur.
`c3p`		Optional. Issuer und Seriennummer des IAC. Wird nur gesetzt, wenn für einen Drittanbieter eine Zulassungsbestätigung für einen Notar erstellt wird.
`c`		Seriennummer des Signaturzertifikates (aus RT1Request PKCS#7 Struktur).
`p`		Personen-UUID der Person, für welche die Zulassungsbestätigung erstellt wird.
`t`		Transaktions-UUID. Die Transaktion ist RT1 und RT2.
`h`		SHA-256 Hash des generierten Bildes bei RT1.
`f`		Liste der momentan gültigen Funktionen.
	`fd`	Funktions-Domain (ist der Wert der Domain, welcher bei RT1 übermittelt wurde (z.B. UPReg).
	`fi`	Funktions-ID.
	`fk`	Kanton oder Bundesbehörde, wo die Funktion gültig ist (z.B. BE).
	`fb`	Funktionsbeschreibung (z.B. Notar).
	`fo`	Organisations-UID der Organisation, an welche die Funktion gebunden ist.

6.2. Personen- und Funktionsidentifikator

Es ist zu beachten, dass die ID der Person und der Funktion nicht mehr die des UPReg ist, sondern diejenige des liefernden Registers. Diese Identifikatoren sind nur innerhalb des Kantons oder der Bundesbehörde und der Domäne eindeutig.

Diese ID wird aus dem Kantonskürzel bzw. dem Kürzel der Bundesbehörde und der ID des Registers zusammengestellt. Die beiden Werte sind mittels Schrägstrich getrennt.

```
Kantonskürzel/Kantonaler-Identifikator
```

Beispiele für IDs:

```
BE/1d32b4bc-b923-4615-9233-8bcbc5223a77

VD/19837

TI/a:12-kjv
```

6.3. Layout der Signatur

Wie in der in die Signatur eingebetteten Datenstruktur, wird in der Zulassungsbestätigung jedem Identifikator das Kantonskürzel bzw. das Kürzel der Bundesbehörde vorangestellt. In der folgenden Abbildung ist dies beim Identifikator der Person (Wert im Feld `Name/Nom/Nome`) zu erkennen.