1

Portalverbund **Verwaltungsprozesse für zentrale Dienste**		**Konvention** **PVP2-ZD Policy 1.0** **Empfehlung**
Kurzbeschreibung	Diese Konvention definiert die Verwaltungsprozesse für die gemeinsamen Daten im Portalverbund. Damit wird sichergestellt, dass die Daten der Teilnehmer, ihrer befugten Vertreter und der Portale in vertrauenswürdiger und maschinenlesbarer Form zur Verfügung gestellt werden.	
Autor(en):	Rainer Hörbe (Wien) Harald Stradal (BMI)	Projektteam / Arbeitsgruppe **AG Integration und Zugänge (AG-IZ)** AG-Leiter: Michael Pellmann, MSc (Wien)
Beiträge von:	Caroline Müller, Peter Pichler, Peter Reif, Bernd Zwattendorfer	

2

Version 1.0:	**11.11.2015**	Angenommen: **27.1.2016 VSt-1712/535**

3

Inhaltsverzeichnis

1 Geltungsbereich

Zielgruppe. Die hier definierten Regeln und Beschreibungen richten sich an den Betreiber der zentralen Dienste des Portalverbunds sowie Portalbetreiber und Anwendungsverantwortliche.

Zweck. Die zentralen Dienste umfassen die Verwaltung der Teilnehmer und Kundmachungen des Depositars im zentralen Verzeichnisdienst und den SAML Metadaten der Verwaltung und allfälliger „(cross-)föderierter Verbünde“.

Die Kundmachungen des Depositars beinhalten alle Portale und alle anwendungsrelevaten Daten einschließlich der Betriebshandbücher.

Die PVV regelt den Teilnehmerkreis und den Abstimmungsprozess für die Teilnahme, lässt aber die Umsetzung der konkreten Verwaltungsprozesse offen. Für die geplante Umsetzung von PVP2 wird hiermit eine genauere organisatorische Regelung getroffen.

2 Begriffsbestimmungen

2.1.1 Rollen

Depositar
In der [PVV] definierte Rolle, die Meldungen der PV-Teilnehmer entgegen nimmt und kundmacht. Die Rolle wird von dem für die IKT-Koordination des Bundes verantwortlichen Ministerium (aktuell das Bundeskanzleramt) wahrgenommen. Der Depositar kann Aufgaben an die Portaladministratoren delegieren.

Portaladministrator

Die für den Betrieb eines PV-Portals zuständige natürliche Person, welche für die Meldung der technischen Konfigurationsdaten einschließlich der Zertifikate des Portals (impliziert auch deren Ajourierung) in den zentralen Diensten zuständig ist.

Anwendungsverantwortlicher

Der Begriff Anwendungsverantwortlicher ist in der Portalverbundvereinbarung [PVV] definiert. Im Kontext der hier beschriebenen Use-Cases stellt ein Anwendungsverantwortlicher den zugriffsberechtigten Stellen eine Anwendung im Portalverbund zur Nutzung zur Verfügung und meldet dafür die anwendungsrelevanten Daten an die PV-ZD. Anwendungsverantwortliche können PV-Teilnehmer oder extern sein.

PV-Teilnehmer

„Jene (Organe von) Gebietskörperschaften, anderen Körperschaften des öffentlichen Rechts oder sonstigen staatliche Aufgaben besorgenden Institutionen, die gemäß § 1 erklärt haben, als Portalbetreiber oder Anwendungsverantwortlicher am Portalverbundsystem teilzunehmen.“ [PVV]

Die Organisation schließt die Portalverbundvereinbarung ab und tritt dem Portalverbund bei.

Portalbetreiber

Jenes Organ eines Teilnehmers bzw. jene von einem Teilnehmer beauftragte Einrichtung, die ein Portal im Portalverbundsystem unterhält. Ein Portalbetreiber ist für den Betrieb eines Stamm- und/oder Anwendungsportals zuständig. Ein Portalbetreiber (ist eine Organisation) legt fest, welche Personen für diesen als Portaladministrator auftreten.

STP-Betreiber

Ein Stammportalbetreiber (STP-Betreiber) betreibt sein(e) Stammportal(e) immer für PV-Teilnehmer.

Es kann sein, dass der STP-Betreiber mehrere Stammportale für unterschiedliche PV-Teilnehmer betreibt.

STP-Dienstleister (nicht PV-Teilnehmer)

Ein STP-Dienstleister betreibt für eine zugriffsberechtigte Stelle ein Stammportal ohne selbst ein PV-Teilnehmer zu sein. In diesem Fall muss mit einem PV-Teilnehmer die Vereinbarung [pv-dl-stp] getroffen werden.

Zugriffsberechtigte Stelle (zbSt, Participant)

Zugriffsberechtigte Stellen sind alle jene Organisationseinheiten eines Teilnehmers (vgl. Punkt2.1.5), denen aufgrund rechtlicher oder vertraglicher Vorgaben Zugriffsrechte auf Anwendungen im Portalverbund einzuräumen sind.

Ist eine Zugriffsberechtigte Stelle nicht deckungsgleich mit dem Teilnehmer oder eine dem Teilnehmer untergeordnete Organisationseinheit, so müssen zwischen der Zugriffsberechtigten Stelle und dem Teilnehmer für den "indirekten Beitritt" die entsprechenden Rechte und Pflichten aus dem Portalverbund überbunden werden [pv-dasi].

Für die Gewährung von Zugriffsrechten sind darüber hinaus mehrere Ausprägungen möglich:
2.1.9.1 ZbSt mit eigenem Stammportal (NEU)
Die (Sub-)teilnahme am Portalverbund ist ausreichende Grundlage.
2.1.9.2 ZbSt mit vom Teilnehmer betriebenen Stammportal (NEU)
Zwischen Teilnehmer und Subteilnehmer ist die [pv-zugriff] abzuschließen.
2.1.9.3 ZbSt mit einem Stammportal bei einem Dienstleister (NEU)
Zwischen Teilnehmer und Subteilnehmer ist die [pv-zugriff-dl] abzuschließen UND zwischen Subteilnehmer und Dienstleister ist die pv-stp-dl abzuschließen.

2.1.2 Dienste und Konzepte

Portalverbund Zentrale Dienste (PV-ZD)

Jene Dienste im Portalverbund die gemeinsame Daten und Dienste bereitstellen. Dazu gehören im Kern:

- die Verwaltung der Verträge und Kundmachungen,
- die Einrichtung und Pflege der technischen Vertrauensstellungen,
- die Kundmachung von Portalen und ihrer technischer Daten,
- die Kundmachung von Anwendungen.

Es gibt noch weitere, hier nicht betrachtete Dienste wie z.B.

- die Verwaltungsprozesse für den Grundschutz und
- Testinfrastruktur zur Feststellung der Konformität von Portalen.

Zentraler Verzeichnisdienst

Hält die gemeinsamen Daten, die für den Betrieb des Portalverbunds erforderlich sind und im Verzeichnis ldap.gv.at geführt werden in einer strukturierten und automatisch verarbeitbaren Weise.

Diese Daten umfassen:

1. Teilnehmer, Anwendungsverantwortliche, zbSt., Dienstleister
2. Anwendungen und ihre Rechte
3. Stamm- und Anwendungsportale einschließlich ihrer technischen Attribute wie Identifier und Netzwerkadressen.

SAML Metadaten Verwaltung.

SAML Metadaten sind für den Betrieb mit den PVP2-S Protokoll erforderlich und in [1] spezifiziert. Die in den Daten enthaltenen Zertifikate werden auch für PVP2-R-Profil verwendet.

3 Verwaltungsprozesse

Die Prozesse der zentralen Dienste sind wie folgt gruppiert:

1. Vertragliche Rahmenbedingungen für den PV-Zugriff schaffen
2. Inbetriebnahme und Betrieb eines Portals
3. Inbetriebnahme und Betrieb einer PV Anwendung
4. Zentrale Dienste nutzen
5. Betrieb der zentralen Dienste

Die Beschreibung der Prozesse erfolgt in den Fällen wo mehrere Akteure beteiligt sind in Tabellenform. Zusätzliche Regeln werden im Text angegeben.

3.1 Vertragliche Rahmenbedingungen für den PV-Zugriff schaffen

3.1.1 PV beitreten

	Beitrittswerber	Depositar	Alle PV-Teilnehmer
1	fertigt die Beitrittserklärung zum Portalverbund der Behörden rechtsgültig und übermittelt diese an den Depositar.		
2		prüft den Beitritt formal, • ob die Beitrittserklärung vollständig und korrekt ist, und • dass die für PV-ZD benötigten Informationen des Beitrittswerbers (Organisationsdaten) zur Verfügung stehen	
3		informiert die PV-Teilnehmer über die Beitrittsbewerbung.	
4			prüfen, ob der Beitrittswerber die notwendigen Voraussetzungen erfüllt und können Einspruch erheben.
5		wartet die Einspruchsfrist ab und entscheidet ob (a) ob Einsprüche eingebracht wurden oder (b) dem Beitritt stattgegeben wird.	
6a		informiert Beitrittswerber wird über den Einspruch.	
6b		Beitritt wird kundgemacht und in den PV-ZD eingetragen. □	

3.1.2 PV austreten

Die Meldung des Austritts erfolgt an den Depositar, der alle Rechte und alle vertraglichen Vereinbarungen, welche der Organisation im Zusammenhang mit der PV-Teilnahme entstanden sind wieder aufgelöst werden.

	PV-Teilnehmer	*Depositar*
1	meldet den Austritt an den Depositar	
2		prüft bestehende Verträge und Rechte der Organisation und aktualisiert die Daten in den PV-ZD entsprechend.
3		Austritt wird kundgemacht ☐

3.1.3 Dienstleistervertrag Stammportalbetrieb abschließen [pv-dl-stp]

Es wird die rechtliche Grundlage geschaffen, damit ein STP-Dienstleister, der selbst nicht PV-Teilnehmer ist, zugriffsberechtigten Stellen den Zugriff auf Services des Portalverbundes einrichten darf. AWP-Betreiber sollen über die PV-ZD abfragen können, welche Organisationseinheiten Stammportal-Dienstleister sind, und mit welchen PV-Teilnehmern ein Dienstleistervertrag [pv-dl-stp] besteht.

Vorbedingungen:

- Das STP des Dienstleisters ist in den PV-ZD registriert
- AWP-Betreiber und Depositar sind berechtigt auf Dienstleistervereinbarungen in den PV-ZD lesend und schreibend zuzugreifen.

	PV-Teilnehmer	*STP-Betreiber*	*AWP-Betreiber (im Auftrag des Depositars) oder Depositar*
1	schließen eine Dienstleistervereinbarung [pv-dl-stp] ab		
2	übermitteln den Vertrag wird dem ersten AWP-Betreiber, der den Zugriff einräumen soll.		
3			prüft formale Richtigkeit des Vertrags
4			trägt nach erfolgreicher Prüfung das Vorhandensein einer Dienstleistervereinbarung zwischen PV-Teilnehmer und STP Betreiber [pv-dl-stp] wird in den PV-ZD ein. ☐

Zusatzregel: Ist die Vereinbarung beendet, meldet einer der beiden Vertragspartner die Löschung an den Depositar, der sie löscht.

3.1.4 Zugriffsvereinbarung abschließen (pv-zugriff bzw. pv-zugriff-dl)

Schafft die vertragsrechtliche Grundlage für den Zugriff einer zugriffsberechtigten Stelle über den Portalverbund mithilfe eines STP-Betreibers.

Vorbedingung:

Die zbSt ist in den PV-ZD eingetragen

	zugriffsberechtigte Stelle	*STP-Betreiber*	*Anwendungsverantwortlicher (im Auftrag des Depositars)*
1	schließen eine Zugriffsvereinbarung [pv-zugriff] oder [pv-zugriff-dl] ab		
2	übermitteln den Vertrag dem ersten Anwendungsverantwortlichen, der den Zugriff einräumen soll.		
3			nimmt die Eintragung in den PV-ZD vor, sodass die zbSt als Participant (mindestens) eines bestimmten STP hinterlegt ist. ☐

Ergebnis:

Für die zbSt werden in den PV-ZD folgende Daten eingetragen:

- Name, UserID und Organisationseinheit des Prüfers (=Eintragenden)
- Datum der Eintragung und Art der Vereinbarung ([pv-zugriff] oder [pv-zugriff-dl])

3.1.5 Zugriffs- oder Dienstleistervereinbarung widerrufen

Ist die Vereinbarung (pv-zugriff, pv-zugriff-dl, pv-dl-stp) beendet, meldet einer der beiden Vertragspartner die Löschung an den Depositar, der sie aus dem zentralen Verzeichnisdienst löscht. Das Zertifikat des Dienstleisters ist vom Depositar zu widerrufen.

	zugriffsberechtigte Stelle	*STP-Betreiber*	*PV-Teilnehmer*	*Depositar*
1a	beenden eine Zugriffsvereinbarung			
1b		beenden eine Dienstleistervereinbarung		
2	benachrichtigen den Depositar			
3				löscht die Vereinbarung aus dem zentralen Verzeichnisdienst
4				im Fall einer Dienstleistervereinbarung[1]: widerruft das Zertifikat des Dienstleisters

[1] Ein Dienstleister hat nur eine pv-dl-stp Vereinbarung und das STP-Zertifikat sollte nicht anderweitig verwendet werden

3.2 Inbetriebnahme und Betrieb eines Portals

3.2.1 Portaladministrator melden

Die Berechtigungen für Portaladministratoren werden in den PV-ZD verwaltet. Eintragung und Freigabe erfolgen immer durch die Portalbetreiber im Auftrag des Depositars auf Grund von Anträgen, die über einen sicheren, vom Portalverbundsystem unabhängigen Kanal übermittelt werden.

Ablauf:

Der Portalbetreiber übermittelt die Daten des Portaladministrators vorzugsweise persönlich, oder mittels RSa Brief bzw. durch gleichwertige elektronische Verfahren und pflegt sie in der Berechtigungsverwaltung der PV-ZD ein.

Resultat:

In der PV-ZD-Rechteverwaltung sind für den Portaladministrator folgende Daten hinterlegt:

- Name und Organisationszuordnung
- Daten seiner Bürgerkarte (bPK:PV oder Zertifikat) zur Authentifizierung

Jeder Portalbetreiber kann den Stand aller gemeldeten Portaladministratoren abfragen.

3.2.2 Wurzelzertifikate beziehen und prüfen

Die im Portalverbund verwendeten Wurzelzertifikate werden vom Depositar bekannt gemacht und außerhalb des Systems vertrauenswürdig übermittelt.

Die Wurzelzertifikate sind

1. das TLS-Zertifikat für die PV-ZD und
2. das selbst-signierte Signaturzertifikat des Metadaten-Aggregators.

Vorbedingungen:

- Die Wurzelzertifikate wurden vom Depositar bereitgestellt.

	Depositar oder sein Vertreter	*Portaladministrator*
1	stellt Wurzelzertifikate am Referenceserver bereit	
2		bezieht die Wurzelzertifikate

3	übergibt Prüfdaten (Fingerprints) für Wurzelzertifikate persönlich an den Portaladministrator. Alternativ findet eine persönliche Übermittlung durch einen anderen PV-Teilnehmer, z.B. ein Land, oder eine (elektronische) Übermittlung in gleichwertiger Sicherheit statt. Die Übergabe wird dokumentiert. Best Practice ist der persönlich übergebene Ausdruck.	
		überprüft, dass die von ihm erzeugten Fingerprints der Wurzelzertifikate identisch mit den vom Depositar übernommenen sind. Nach erfolgreicher Prüfung werden die Wurzelzertifikate im Portal konfiguriert. ☐

3.2.3 Portalkundmachung übermitteln

Änderungen am Stamm- bzw. Anwendungsportal, welche auch Änderungen an den zentralen Daten nach sich ziehen, werden in der Portalkundmachung den anderen Teilnehmern bekannt gegeben. Zusätzlich müssen von den Portalbetreibern jene Personen festgelegt werden, die für die Meldung der Portaladministratoren zuständig sind.

Die Kundmachungsinhalte können online oder außerhalb des PV-Systems eingebracht werden. Die Kundmachungsinhalte sind:

- Stammportal (z.B.: Bezeichnung, URL, Verfügbarkeit)
- Mindestens alle Informationen der Kundmachung der Portale [Kundmachung-Portale]
- Anwendungsportal (wie Stammportal)

	Portalbetreiber	*Depositar*
1	meldet die Portaldaten online oder im Zuge des Beitritts als Teil der Beitrittserklärung an den Depositar.	
2		prüft die Kundmachung formal
3		aktualisiert die PV-ZD
4		stellt sicher, dass der Portalbetreiber das Recht hat, über den PV eigene Metadaten zu aktualisieren und seine Portalkundmachung aktuell zu halten. Portalbetreibern, die auch ein Anwendungsportal betreiben, wird auch das Recht eingeräumt Anwendungskundmachungen zu aktualisieren und - sofern der Portalbe-

		treiber PV Teilnehmer ist - auch PV Anwendungen erstmalig zu melden.
5		publiziert die Kundmachung – siehe 3.5.3. ☐

Für die Anwendungen der zentralen Dienste, mit denen online Kundmachungen verwaltet werden, müssen dem Portalbetreiber Zugriffsrechte eingeräumt werden.

3.2.4 Eigene Metadaten aktualisieren

Für den Austausch von Zertifikaten im PV und die Konfiguration von Portalen im PVP2-S-Profile sind die SAML Metadaten in den zentralen Metadaten zu pflegen und zu publizieren.

	Portaladministrator	*Depositar*
1	erstellt neue/aktualisierte SAML Metadaten	
2	übermittelt die mit der Bürgerkarte signierten Metadaten an die Metadatenregistratur, wodurch sie automatisch geprüft werden.	
3		überprüft die Signatur des Portaladministrators und seine Berechtigung.
4		prüft die Metadaten werden nach folgenden Regeln: 1. Im Attribut Subject Name der Zertifikate dürfen keine widersprüchlichen Daten enthalten sein; etwa der Name einer fremden Organisation. 2. Sind die Hostnamen von Endpoint-URLs der meldenden Organisation zuzuordnen. D.h., dass Portale nur in einer Domäne des Portalbetreibers betrieben werden dürfen. (Überprüfung mittel Whois-Abfrage oder schriftlicher Bestätigung über das Verfügungsrecht über die Domäne) 3. Ist die Entity Category (pvp/egovtoken, pvp/egovtoken-charge) dem Verwendungszweck der Anwendung entsprechend? (So sollen z.B. diese Kategorien nicht für Bürger-Anwendungen verwendet werden.) 4. Bereits widerrufene oder abgelaufene Zertifikate sind abzulehnen.
4		Bei positiver Prüfung werden die Metadaten publiziert, bei negativer Prüfung an den Portaladministrator zurückgewiesen. ☐

3.2.5 Wechsel des Portalzertifikats in den Metadaten (Zertifikats-Rollover)

Dieser Prozess ist ein Sonderfall von 3.2.4 Eigene Metadaten aktualisieren.

	Portaladministrator	*Metadatenaggregator*
1	bezieht ein neues Portalzertifikat von einer für den PV akkreditierten CA und erstellt damit aktualisierte Metadaten	
2	aktualisiert Metadaten wie in 3.2.4 beschrieben.	
3	wartet bis alle Portale durch den Metadaten-Refresh das neue Zertifikate haben sollten.	
4	stellt eigenes Portal auf das neue Zertifikat um.	
5		kann nach 30 Tagen das alte Zertifikat löschen. ☐

3.2.6 Zertifikat widerrufen

Das Zurückziehen eines Zertifikates muss im Verbund unmittelbar bekannt gemacht werden. Es erfolgt durch einen Zertifikatstausch, bei dem das alte Zertifikat sofort entfernt wird. Inwieweit eine Betriebsunterbrechung erfolgt unterliegt der Risikoeinschätzung des Portalbetreibers.

Sperre durch den Portaladministrator

	Portaladministrator	*Depositar*
1	deaktiviert das Zertifikat im eigenen Portal.	
2	Ersetzt das Zertifikat in den eigenen Metadaten durch ein neues Zertifikat.	
3	aktualisiert die zentralen Metadaten.	
4		Die Metadaten-Registry speichert die widerrufenen Zertifikate in einer internen Sperrliste. ☐

Sperre durch den Depositar

	Melder	*Depositar*
1	meldet das zu widerrufende Zertifikat dem Depositar	

	über einen vom System unabhängigen Kanal.	
2		entfernt das Zertifikat aus den zentralen Metadaten.
3		Die Metadaten-Registry speichert die widerrufenen Zertifikate in einer internen Sperrliste.
		Verständigt die Portalbetreiber☐

Meldungen können von jedermann, der vom PV betroffen ist, eingebracht werden. Die Plausibilität ist vom Depositar im Kontext zu bewerten, um DoS-Angriffe zu unterbinden.

3.3 Inbetriebnahme und Betrieb einer PV Anwendung

3.3.1 Anwendungskundmachung erstellen / aktualisieren

Vorbedingung

Der Anwendungsverantwortliche ist entweder PV-Teilnehmer oder hat eine Vereinbarung als externer Anwendungsanbieter.

Ablauf:

Der Anwendungsverantwortliche meldet entweder über die Anwendung PAI oder formlos schriftlich die Anwendungsdaten. Die Daten umfassen:

- Die Einträge gvApplication und gvApplicationRights laut dem LDAP-Schema einschließlich des Betriebshandbuches und
- die SAML Metadaten einschließlich der Zertifikate.

Ergebnis:

Die Daten liegen vollständig und korrekt in den PV-ZD vor, womit die Kundmachung der Anwendung durch den Depositar nach § 1 Abs. 3 der Portalverbundvereinbarung erfolgt.

3.3.2 Verpflichtungserklärung für externe Anwendungen abschließen

Dieser Prozess erfolgt sinngemäß wie der Beitritt (3.1.1), wobei Beitritt durch Verpflichtungserklärung zu ersetzen ist.

3.4 Zentrale Dienste nutzen

Portale, die PVP2 verwenden, *MÜSSEN* ihre Konfigurationsdaten einschließlich der Zertifikate von den zentralen Diensten beziehen und diese daher auch dort aktuell halten. Die Daten sind im Falle von Änderungen umgehend im lokalen Portal zu aktualisieren, um die Sperrung von Zertifikaten und Zugriffsrechten zeitnahe umzusetzen. SAML-Metadaten sind periodisch und automatisiert über die Schnittstelle des Metadaten-Feeds zu importieren.

Portale *können* ihre Zertifikate für den Betrieb von PVP1 über die zentralen Dienste verteilen.

3.5 Datenpflege und Betrieb der zentralen Dienste

3.5.1 Organisation in den PV-ZD registrieren und aktualisieren

Um eine neue Organisation einzutragen, die für eine der oben angeführten Rollen benötigt wird, ist deren Verwaltungskennzeichen notwendig.

.

3.5.2 Wurzelzertifikate etablieren

Die im Portalverbund verwendeten Wurzelzertifikate müssen bekannt gemacht und außerhalb des Systems vertrauenswürdig übermittelt werden. Die Wurzelzertifikate sind

1. das TLS-Zertifikat für den LDAP-Verzeichnisdienst der PV-ZD und
2. das selbst-signierte Signaturzertifikat des Metadaten-Aggregators.

	Depositar	*Portaladministrator*
1	publiziert Wurzelzertifikate am Referenzserver ohne erhöhte Sicherheit.	
2	erstellt Fingerprints	
3	Weiter mit Ablauf 3.2.2 Wurzelzertifikate beziehen und prüfen	

3.5.3 Kundmachung und Betrieb von Verzeichnisdaten und Metadaten-Feed

Mit der Einführung von PVP V2 werden die gemeinsamen Daten nur mehr in strukturierter Form verwaltet, wodurch die Verteilung automatisiert erfolgen kann. Für diesen Zweck werden vom Depositar folgende Dienste zur Verfügung gestellt[2]:

- Zentraler Verzeichnisdienst mit folgendem Inhalt:
  - Organisationen (PV-Teilnehmer, zbSt, Portalbetreiber, Dienstleister, und Anwendungsanbieter
  - Portale
  - Vorhandensein von Zugriffs- und Dienstleistungsvereinbarungen
  - Vorhandensein von Verpflichtungserklärungen externer Anwendungsanbieter
  - Anwendungen und Anwendungsrechte
  - Betriebshandbücher

[2] Diese Forderung ist das Ergebnis des Architekturkonzepts. Die zeitliche Umsetzung und Finanzierung sind an einer anderen Stelle zu bestimmen.

- SAML Metadaten, diese enthalten:
  - SAML IDP und SP, bzw. Platzhalter für R-Profil-Portale mit ihren Zertifikaten
- Rechteverwaltung der zentralen Dienste für:
  - Portaladministratoren

Für diese Dienste sind folgende Publikationsmechanismen vom Depositar zur Verfügung zu stellen:

- Die jeweiligen maschinenlesbaren Formate für den zentralen Verzeichnisdienst, SAML Metadaten und die ZD-Rechteverwaltung;
- Ein benutzerfreundlicher Publish/Subscribe-Mechanismus, der auch die einfache Kenntnisnahme der durchgeführten Veränderungen zulässt, etwa in Form eines RSS Feeds;
- Die aktuelle Gesamtsicht im PDF- oder HTML-Format.

4 Referenzen

Referenz	Dokument
[PV-Best Practice]	„PVP V2 Best Practice“, Ergebnis der Arbeitsgruppe, 22.5.2015 (Zur Abstimmung mit PVP 2.1.2)
[pvv]	http://reference.e-government.gv.at/uploads/media/pvv1.0-21112002.pdf
[pv-zugriff]	http://reference.e-government.gv.at/uploads/media/pv-zugriff-1-0-1-20050621.pdf
[pv-zugriff-dl]	http://reference.e-government.gv.at/uploads/media/pv-zugriff-dl-1-0-0-20050502.pdf
[pv-ext-anw]	http://reference.e-government.gv.at/uploads/media/pv-ext-anw__1-0-2_20080821.pdf
[pv-dl-stp]	http://reference.e-government.gv.at/uploads/media/pv-dl-stp_1-1-0_20060509.pdf
[PVP-SMA]	Portalverbund Sicherheitsmaßnahmen (Algorithmen)
[pvv-beitritt]	http://www.ref.gv.at/Beitrittserklaerung.966.0.html
[PVP2-S-MD]	SAML Metadata Management Spezifikation
[AG-IZ-IDM-Glossar]	http://www.ref.gv.at/uploads/media/AG-IZ-IDM-Glossar_1_0_0-2011-08-31.pdf
[Kundmachung-Portale]	https://ref.gv.at/cms/uploads/media/20141016_Portale-PV-Kundmachung.pdf
[LDAP-gvat_PV]	Spezifikation LDAP-gv.at für Portalverbund http://reference.e-government.gv.at/AG-IZ-LDAP-Dokumente-Spezifi.2258.0.html

Anhang A Änderungshistorie

Version 1.0.0

Dokument neu erstellt