
| **Basisinformationen zum Behörden-Portalverbund** | **Information** |
|---|---|
| | **pv-info 2.0** |
| | **Ergebnis der Arbeitsgruppe** |

| | | |
|---|---|---|
| Kurzbeschreibung | Dieses Dokument stellt Basisinformationen zum Behörden-Portalverbund bereit und gibt einen Überblick über alle bisher erarbeiteten Konventionen zum Behörden-Portalverbund und deren Zusammenspiel.<br>Damit soll eine einheitliche Sicht auf die Rechte und Pflichten, der Vorgaben und Informationen für alle TeilnehmerInnen am Behörden-Portalverbund gewährleistet werden. | |
| Autor(en): | Mirjam Jilka,<br>Hannes Wittmann,<br>Alena Sirka,<br>Wilfried Connert | Projektteam / Arbeitsgruppe<br>AG Recht und Sicherheit |

| Stelle | Vorgelegt am | Angenommen am | Abgelehnt am |
|---|---|---|---|
| AG RS | 14.9.2010 | 24.9.2010 | |
| AB IZ | 14.9.2010 | 24.9.2010 | |

***Dokumentklasse:*** Konvention, Erläuterung, **Information**

***Doku-Stadium:*** Entwurf intern, **Entwurf öffentlich**, Empfehlung

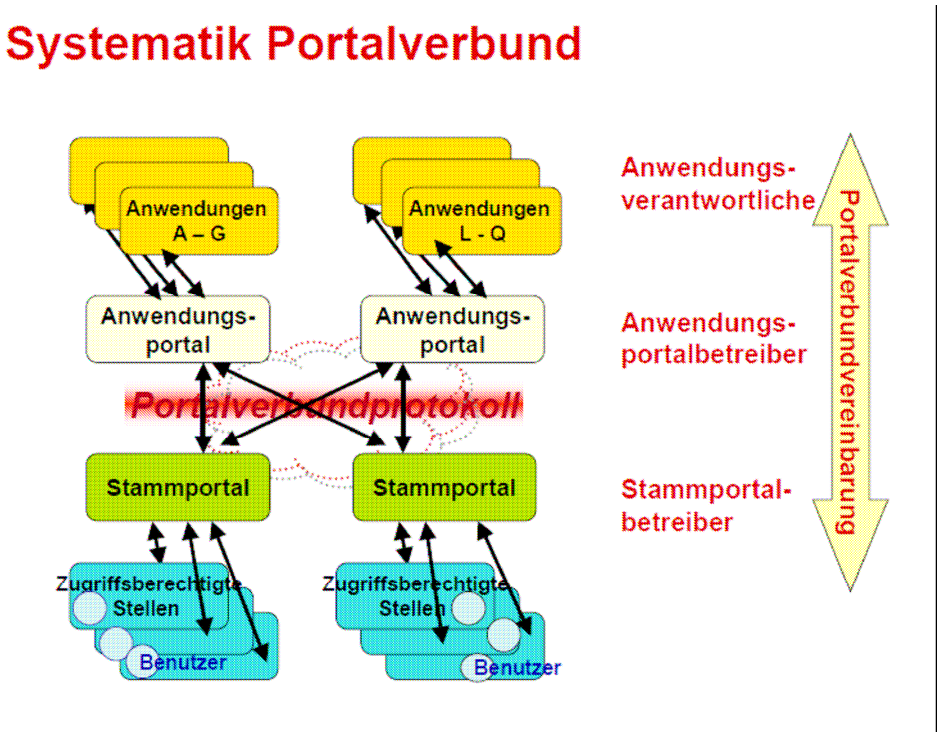
# INHALTSVERZEICHNIS

Basisinformationen zum Behörden-Portalverbund ..... 3
(1) Portalverbundvereinbarung – „pvv" ..... 4
(2) Beitritt zur PVV - „pvv-Beitrittserklärung" ..... 4
(2.1) Änderungen, Ergänzungen zu erfolgten Meldungen und weitere neue Meldungen zum Behörden-Portalverbund ..... 4
(2.2) Austritt (§ 13 (1) PVV) ..... 5
(3) Portalverbund-Protokoll - „pvp" ..... 5
(3.1) Zugriff auf ldap.gv.at über SOAP und PVP - „ldap-soap-pvp" ..... 5
(4) Vereinbarung über die Einräumung von Zugriffsrechten im Portalverbund – „pv-zugriff" 5
(5) Datensicherheitsmaßnahmen für Web Anwendungen – „pv-dasi" ..... 6
(6) Meldung der Benutzer- und Rechteverwalter im Stammportal – „pv-meld" ..... 6
(7) Sicherheitsklassen - „secClass" ..... 6
(8) Vereinbarung mit einem Dienstleister über den Betrieb eines Stammportals im Portalverbund – „pv-dl-stp" ..... 7
(9) Vereinbarung über die Einräumung von Zugriffsrechten im Portalverbund über einen Dienstleister – „pv-zugriff-DL" ..... 7
(10) Anwendungen Dritter – „pv-ext-anw" ..... 8
(11) Revisionsleitfaden – „rev-pv" ..... 8
(12) Revisionsabfrage – „pvp AuditQuery" ..... 8
(13) Testrollen – „pvp-Testrollen" ..... 8
(14) Sonstiges: ..... 9
(14.1) Standardportal ..... 9
(15) Ausblick: ..... 9
(15.1) PVP 2.0 ..... 9
(15.2) Common Logfile format ..... 9
(15.3) Common Protocol File Format ..... 9
(15.4) Rechtemodellierung im Portalverbund ..... 9
(15.5) Bürger via Portalverbund - pvp-citizen ..... 10

# Basisinformationen zum Behörden-Portalverbund

Der Behörden-Portalverbund hat sich in den letzten Jahren als funktionierendes, gesichertes System für den Datenaustausch unter Behörden und Gebietskörperschaften sowohl technisch weiterentwickelt als den rechtlichen Rahmenbedingungen besser angepasst. Um allen TeilnehmerInnen am Behörden-Portalverbund einen Überblick über das gesamte Regelwerk zu gewährleisten, wurde dieses Dokument aktualisiert und erweitert.

Für die Umsetzung von e-Government müssen die Mitarbeiter der einzelnen Organisation auf für sie relevante Informationen in EDV-Systemen der eigenen Organisation, aber auch behördenübergreifend zugreifen können. Den Berechtigungssystemen kommt damit erhöhte Bedeutung zu. Berechtigungssysteme werden dazu nicht mehr in jeder Anwendung realisiert und gewartet, sondern den Anwendungen als Portal vorgelagert. Bei der behördenübergreifenden Zusammenarbeit zum Wohle der BürgerInnen kommt es zu einer Kommunikation zwischen Anwender und Anwendung über bzw. zwischen Portalen. Neben technischen Aspekten sind dafür auch verbindliche rechtlichen Rahmenbedingungen unter Beachtung des Datenschutzes notwendig. Diese werden in den nachfolgenden Konventionen geschaffen.



# (1) Portalverbundvereinbarung – „pvv"

Diese Konvention ist eine „Vereinbarung über die einzuhaltenden Rahmenbedingungen bei der Einrichtung und Benützung eines e-Government Portalverbundsystems", die unter Mitwirkung des Datenschutzbüros im Bundeskanzleramt entstanden ist. Damit werden die rechtlichen Rahmenbedingungen für den Behörden-Portalverbund geschaffen. Es werden darin insbesondere die Rechte und Pflichten von Anwendungsverantwortlichen, Anwendungsportalbetreibern, Stammportalbetreibern und zugriffsberechtigten Stellen festgelegt. Damit wird der Zugang zu Anwendungen der Verwaltung durch Benutzer aus der Verwaltung geregelt.

Basis der Vereinbarung ist das gegenseitige Vertrauen in das ordnungsgemäße Verhalten der Teilnehmer (trusted parties). Die Portalverbundvereinbarung stellt auch eine Vereinbarung über Datensicherheitsmaßnahmen nach dem DSG 2000 dar.

Die PV-Vereinbarung erspart zahlreiche bilaterale Vereinbarungen über den Zugang zu Anwendungen.
Sie ermöglicht eine Delegation der Zuweisung von Berechtigungen an jene Organisationseinheiten, in deren Bereich die Benutzer tätig sind, und wo daher die unmittelbare und aktuelle Kenntnis über Tätigkeit und notwendige Berechtigungen besteht.

Die standardisierten Regelungen werden durch den Beitritt der einzelnen Organisationen zwischen diesen wirksam.

**Siehe**: http://reference.e-government.gv.at/AG-IZ-PVV-pvv-1-0-Ergaenze.332.0.html

# (2) Beitritt zur PVV - „pvv-Beitrittserklärung"

Die PV-Vereinbarung kommt zur Anwendung, wenn Teilnehmer eine Beitrittserklärung beim Depositar (derzeit: BKA) abgeben. Dabei sind auch Angaben zum jeweiligen Portal und - wenn solche zur Verfügung gestellt werden - zu den jeweiligen Anwendungen erforderlich. Die Informationen der Anwendungsverantwortlichen zu ihren Anwendungen enthalten eine Festlegung der zugriffsberechtigten Stellen, der Rollen und der Zuordnung zu Sicherheitsklassen. Alle Beitrittserklärungen werden am Reference-Server kundgemacht.

**Siehe:**
http://reference.e-government.gv.at/uploads/media/pvv-Beitrittserklaerung_20050508_01.doc

## *(2.1) Änderungen, Ergänzungen zu erfolgten Meldungen und weitere neue Meldungen zum Behörden-Portalverbund*

Änderungen/Ergänzungen zur erfolgten Beitrittserklärung und zu bereits erfolgten Meldungen für Anwendungen/Portale sowie die Meldung/Einbringung weiterer neuer Anwendungen/Portale hat ebenfalls mit dem Musterformular „pvv-Beitrittserklärung" zu erfolgen.

### *(2.2) Austritt (§ 13 (1) PVV)*

Jeder Teilnehmer am Portalverbundsystem kann durch entsprechende schriftliche Erklärung aus dem Portalverbundsystem ausscheiden. Dieser Austritt wird 3 Monate nach Einlangen der Erklärung beim Depositar (§ 1 Abs. 3 PVV) wirksam.

## (3) Portalverbund-Protokoll - „pvp"

Das Portalverbundprotokoll (pvp) ermöglicht das Zusammenwirken von Stammportalen zur Authentifizierung und Autorisierung von Benutzern einerseits und Anwendungsportalen zur Überprüfung des berechtigten Zuganges zu Anwendungen andererseits. Optional wird noch eine Option zur Transaktionsverrechnung angeboten.

Im Portalverbund-Protokoll sind die technischen Standards festgelegt. Durch die Festlegung von Sicherheitsklassen samt Sicherheitsmaßnahmen (Vorgaben hierzu siehe unten die Konvention „sec class") und die Zuordnung von Anwendungen zu Sicherheitsklassen wird auch ein einheitlicher Rahmen von Sicherheitsmaßnahmen geschaffen.

**Siehe**: http://reference.e-government.gv.at/PVP-1-x.2331.0.html

### *(3.1) Zugriff auf ldap.gv.at über SOAP und PVP - „ldap-soap-pvp"*

Für andere Zugriffsarten als den öffentlichen Lesezugriff auf ldap.gv.at soll die Authentifizierung und Autorisierung über die Portalverbund-Infrastruktur erfolgen. Hier wird die dazu notwendige Protokollbindung spezifiziert.

**Siehe:**
http://reference.e-government.gv.at/AG-IZ-Zugriff-PVP-LDAP-SOAP-vo.1648.0.html

Die zugriffsberechtigten Stellen in Organisationseinheiten müssen selbst nicht Teilnehmer der PV-Vereinbarung sein (ausgenommen, wenn sie unmittelbar zu einer Organisation gehören, die zugleich auch Portalbetreiber oder Anwendungsverantwortlicher ist.) Sie treten dann der PV-Vereinbarung selbst nicht bei. Auf sie müssen die Pflichten aus dem Portalverbund durch den jeweiligen Portalbetreiber überbunden werden. Dafür wurden folgende Muster entwickelt (siehe **(4), (5)** und **(6)**):

## (4) Vereinbarung über die Einräumung von Zugriffsrechten im Portalverbund – „pv-zugriff"

§ 7 PVV regelt die Rechte und Pflichten der zugriffsberechtigten Stelle.

Soweit Stammportalbetreiber und zugriffsberechtigte Stelle nicht in einer Organisationseinheit zusammenfallen, ist es erforderlich, zwischen dem Stammportalbetreiber und der zugriffsberechtigten Stelle eine Vereinbarung über die Einhaltung der Pflichten aus der Portalverbundvereinbarung und die Tragung allfälliger Kosten für die Nutzung von Anwendungen zu treffen.

Dieses Dokument enthält ein Muster für eine Vereinbarung zwischen dem Stammportalbetreiber und einer zugriffsberechtigten Stelle.

Dabei wurde der Text aus dem vorgelegenen Anlassfall soweit abstrahiert, dass nur mehr die Bezeichnungen für die Rollen „Teilnehmer" und „zugriffsberechtigte Stelle" eingesetzt werden müssen

**Siehe:** http://reference.e-government.gv.at/AG-IZ-Zugriff-02-05-2005.897.0.html

## (5) Datensicherheitsmaßnahmen für Web Anwendungen – „pv-dasi"

Für die Anleitung und Verpflichtung der einzelnen zugriffsberechtigten Stellen auf die Einhaltung konkreter Datensicherheitsmaßnahmen ist ein allgemein abgestimmtes Muster vorteilhaft.
Dieses Dokument enthält ein solches Muster, das einer Vereinbarung zwischen Stammportalbetreiber und zugriffsberechtigter Stelle angeschlossen werden soll.

**Siehe:** http://reference.e-government.gv.at/Portalverbund-Datensicherheit.640.0.html

## (6) Meldung der Benutzer- und Rechteverwalter im Stamm-portal – „pv-meld"

Eine Organisationseinheit muss ihre Rechte- und Benutzerverwalter mittels Verpflichtungserklärung verpflichten und diese an Stammportalbetreiber melden; ebenso jede Änderung.

Dieses Dokument enthält ein Muster einer Verpflichtungserklärung sowie einer Meldung der Rechte- und Benutzerverwalter.

**Siehe:**
http://reference.e-government.gv.at/AG-IZ-Meldung-Stammportal-02.895.0.html

Darin ist auch die Verpflichtung enthalten, allfällige Entgelte für die Nutzung von Anwendungen direkt zu tragen.

## (7) Sicherheitsklassen - „secClass"

Die Definition und Abbildung von Sicherheitsklassen ermöglicht es einer Anwendung zu prüfen, ob ein Benutzer die für die Nutzung der Anwendungsfunktion erforderlichen Sicherheitsauflagen erfüllt, auch wenn für Benutzer und Anwendungsbetreiber unterschiedliche Sicherheitsnormen gelten.
Der Schutzbedarf von Anwendungen einerseits und Sicherheitsmaßnahmen der Benutzer und ihrer Systeme andererseits wird in einem Schema mit 4 Sicherheitsklassen kategorisiert, welches Auflagen im Bereich der Authentifizierung, der Netzsicherheit, der räumlichen Sicherheit und anderen Bereichen beinhaltet.

Wenn eine zugriffsberechtigte Stelle nicht durch eigene Mitarbeiter sondern durch Vertragspartner als Dienstleister tätig wird, trägt sie die Verantwortung für diese. Die muss den Vertragspartner entsprechend verpflichten und darf nur selbst die genannten Mitarbeiter berechtigen.

**Siehe**: http://reference.e-government.gv.at/AG-IZ-Sicherheitsklassen-Sec.1719.0.html

## (8) Vereinbarung mit einem Dienstleister über den Betrieb eines Stammportals im Portalverbund – „pv-dl-stp"

Nach § 10 PVV muss ein Teilnehmer am Portalverbundsystem, der sich eines Dienstleisters bedient, diesen zur Einhaltung aller Bestimmungen und Datensicherungsmaßnahmen verpflichten und dies auch in geeigneter Weise kontrollieren. Dieses Dokument enthält ein Muster für eine Vereinbarung mit einem Dienstleister über den Betrieb eines Stammportals.

**Siehe**:
http://reference.e-government.gv.at/AG-IZ-DL-Stammportal-09-05-2.947.0.html

**Beispiel:**
Länder schließen Vereinbarungen mit Providern als Dienstleiter über den Betrieb von Stammportalen für den Zugang von Gemeinden ab. Die Länder sind Teilnehmer am Portalverbund, die Provider Dienstleister, die Gemeinden zugriffsberechtigte Stellen.
Provider müssen dazu die technische Infrastruktur eines Stammportales nicht selbst betreiben, sondern können sich dafür eines Dienstleisters bedienen, der dann ev. mehrere Stammportale hostet. Diese treten im Portalverbund als getrennte Stammportale mit jeweils eigenem Zertifkat in Erscheinung. Eine Revision der technischen Installation erfolgt jedoch nur durch jenes Land, im dem diese installiert ist.
Vereinbarungen mit den zugriffsberechtigten Stellen werden an das Amt der Landesregierung des jeweiligen Bundeslandes weitergeleitet. Eine Liste der Adressen mit den zuständige Abteilung wird aufgelegt.
Auf dieser Basis können auch Vereinbarungen zwischen anderen Teilnehmern und Dienstleistern (zB Bundesministerium und Bundesrechenzentrum GmbH) abgeschlossen werden.

## (9) Vereinbarung über die Einräumung von Zugriffsrechten im Portalverbund über einen Dienstleister – „pv-zugriff-DL"

§ 7 PVV regelt die Rechte und Pflichten der zugriffsberechtigten Stelle.

Soweit Stammportalbetreiber und zugriffsberechtigte Stelle nicht in einer Organisationseinheit zusammenfallen, ist es erforderlich, zwischen dem Stammportalbetreiber und der zugriffsberechtigten Stelle eine Vereinbarung über die Einhaltung der Pflichten aus der Portalverbundvereinbarung und die Tragung allfälliger Kosten für die Nutzung von Anwendungen zu treffen.

Dieses Dokument enthält ein Muster für eine Vereinbarung zwischen dem Stammportalbetreiber, der sich eines Dienstleisters bedient und einer zugriffsberechtigten Stelle.

Dabei wurde der Text aus dem vorgelegenen Anlassfall soweit abstrahiert, dass nur mehr die Bezeichnungen für die Rollen „Teilnehmer", „Dienstleister" und „zugriffsberechtigte Stelle" eingesetzt werden müssen

**Siehe**: http://reference.e-government.gv.at/AG-IZ-Zugriff-DL-02-05-2005.898.0.html

## (10) Anwendungen Dritter – „pv-ext-anw"

Private Anbieter von Anwendungen, die für Mitarbeiter der öffentlichen Verwaltung von Interesse sind, können nicht Teilnehmer des Behörden-Portalverbundes werden.
Diese Empfehlung regelt, wie einerseits den privaten „Externen Anwendungsverantwortlichen" ermöglicht wird, ihre Anwendungen zugriffsberechtigten Stellen, die ihre Berechtigungen an Stammportalen verwalten zur Verfügung zu stellen, andererseits sicherstellt, dass nur ausgehende Zugriffe möglich sind.

**Siehe**:
http://reference.e-government.gv.at/AG-IZ-PV-Anwendungen-Dritter.2140.0.html

## (11) Revisionsleitfaden – „rev-pv"

Gemäß § 6 (6) PVV haben Stammportalbetreiber mindestens einmal jährlich eine Sicherheitsrevision durchzuführen oder zu veranlassen.
Um einen einheitlichen Standard bei allen Portalverbundteilnehmern zu erreichen, sind in diesem Revisionsleitfaden, der benutzerfreundlich in Form einer Checkliste gestaltet wurde, alle Verpflichtungen der Portalbetreiber (Stamm- und Anwendungsportalbetreiber) so aufgearbeitet, dass damit eine regelmäßige Revision erleichtert werden soll.

**Siehe:** http://reference.e-government.gv.at/Revisionsleitfaden.auditcheck.0.html

Die technischen Spezifikationen des Protokolls bestehen darüber hinaus aus folgenden Dokumenten (Punkt **(12)** bis **(13)**):

## (12) Revisionsabfrage – „pvp AuditQuery"

Mit der Revisionsabfrage wird die Schnittstelle spezifiziert, die gemäß § 4 (8) PVV pro Stammportal umzusetzen ist. Diese Schnittstelle ist so gestaltet, dass sie auch für die interne Revision eines Stammportals verwendet werden kann.

**Siehe**: http://reference.e-government.gv.at/Revisionsabfrage.auditquery.0.html

## (13) Testrollen – „pvp-Testrollen"

Für Test und Unterstützung der Benutzer durch Anwendungsbetreuer und IT-Supporter, denen aus rechtlicher Sicht kein Zugang zu Daten einer Anwendung zusteht, soll eine Lösung gefunden werden, mit der die Funktionen im gesetzlichen Rahmen getestet werden können.
Durch die Definition einer Testrolle und der Bereitstellung von Testdaten sollen die Testmöglichkeiten gegeben werden.

**Siehe**: http://reference.e-government.gv.at/Testrollen.2334.0.html

# (14) Sonstiges:

## *(14.1) Standardportal*

Mit dem Projekt „Standardportal" wurde in Zusammenarbeit zwischen dem BMI, dem LFRZ und weiteren Partnern eine Softwarelösung für Stamm- und Anwendungsportal nach den Vorgaben des Portalverbundes realisiert. Diese kann von den Projektpartnern nach den getroffenen Vereinbarung genutzt werden. Daneben bestehen weiterhin auch Portal auf anderer Softwareplattformen, die den Konventionen gemäß implementiert sind.

# (15) Ausblick:

Derzeit sind einige Dokumente und Konventionen in Arbeit, bzw. bestehen Projektgruppen zur Weiterentwicklung des Behörden-Portalverbundes. Diese werden hier aufgezählt und bei der nächsten Versionierung übernommen.

## *(15.1) PVP 2.0*

Mit PVP 2.0 werden international standardisierte Protokolle wie SAML 2.0 zur Kommunikation im Portalverbund eingesetzt. Über das in PVP 2.0 definierte SAML-Profil soll eine Kompatibilität zum PVP 1.x über Gateways ermöglicht werden.

**Siehe**: http://reference.e-government.gv.at/PVP-2-x.2332.0.html

## *(15.2) Common Logfile format*

Spezifikation eines einheitlichen Protokollierungsformats für alle Portale im Portalverbund.

**Siehe**: http://reference.e-government.gv.at/Common-Logfile-Format.2335.0.html

## *(15.3) Common Protocol File Format*

Spezifikation eines einheitlichen Protokollierungsformats für alle Applikationen im Portalverbund: Für die Durchführung einer Revision bzw. der Überprüfung der Zulässigkeit von Zugriffen auf eine Anwendung im Einzelfall sind gewisse Mindestanforderungen für ein Protokoll für die im Portalverbund definierten Zwecke erforderlich.

## *(15.4) Rechtemodellierung im Portalverbund*

Dieses Dokument wird als Konvention Vorgaben und Empfehlungen für die Modellierung von Rechtesystemen für den Portalverbund der österreichischen Verwaltung beschreiben. Die Modellierung von Zugriffsrechten zielt auf die einfache

Integration der Rechte in den Stamm- und Anwendungsportalen und deren einfache Verwaltung ab.

**Siehe**: http://reference.e-government.gv.at/Rechtemodellierung.2328.0.html

### *(15.5) Bürger via Portalverbund - pvp-citizen*

Um Bürger, welche sich an einem Portal authentifiziert haben, an eine entfernte Applikation oder ein entferntes Portal via PVP weiterreichen zu können, bedarf es über das PVP hinaus gehende Definitionen. Dieses Dokument soll diese festlegen, um sie dann später in ein erweitertes PVP Konzept zu integrieren.

**Siehe:**
http://reference.e-government.gv.at/uploads/media/pvp_citizen_1-0_2009-1103.pdf