Portalverbundprotokoll Version 2 **Allgemeiner Teil**		**Konvention** **PVP2 - 2.1.3** **Ergebnis der AG**
Kurzbeschreibung	Das Portalverbundsystem ermöglicht das Zusammenwirken von Stammportalen zur Registrierung von Benutzern mit ihren Zugriffsrechten einerseits und Anwendungsportalen zur Überprüfung des berechtigten Zuganges zu Anwendungen andererseits. Die Authentifizierung und Autorisierung kann delegiert werden. Der Aufwand für die Verwaltung der Benutzer wird reduziert und ein Single-Sign-On unterstützt. Die Version 2 des Portalverbundprotokolls unterstützt mehrere Profile, wie das Reverse-Proxy-Profil entsprechend der Versionen 1.x, und das SAML2 konforme „S-Profil".	
Autor(en):	Peter Pichler (LFRZ)	Projektteam / Arbeitsgruppe **AG Integration und Zugänge (AG-IZ)** AG-Leitung: Ing. Dipl.-Ing.(FH) Hannes Wittmann, MSc (Mag. Wien) Stellvertretung: Dipl.-Ing. Dominik Klauser, BSc (BKA)
Beiträge von:	Rainer Hörbe, Peter Pfläging, Joachim Minichshofer, Harald Stradal	

Version	2.1.3	:	**20.12.2017**	Angenommen: -
Version	2.1.2	:	**2.7.2015**	Angenommen: -
Version	2.1.1	:	**26.2.2015**	Angenommen: -
Version	2.1.0	:	**3.9.2013**	Angenommen: **21.11.2013** **VSt-1712/488**
Version	2.0.0	:	**31.8.2011**	Angenommen: **14.10.2011** **VST-1712/455**

Inhaltsverzeichnis

1 Über das Dokument und die Protokollversionen

PVP2 ist ein Standard für verteilte Autorisierungs- und Authentifizierungssysteme. Zum einen wird in Form von Attributdefinitionen ein Datenmodell beschrieben, mit der auf standardisierte Weise Informationen über Identitäten, organisatorische Zuordnung und zugeordnete Berechtigungen ausgetauscht werden können. Zum anderen wird über Profile festgelegt, wie diese Informationen zwischen Identity-Providern / Stammportalen und Service-Providern / Anwendung(sportal)en ausgetauscht werden.
Im auf PVP 1.x basierenden „Reverse-Proxy Profil" (PVP-2-R-Profil) wird jede Browseranfrage über Stamm- **und** Anwendungsportal (STP und AWP) geführt. Für die Authentifizierung der Portale werden TLS-Zertifikate verwendet. Die PVP Attribute werden in Form von HTTP Headern übertragen.
Das PVP2-S-Profil basiert auf dem „SAML 2.0 Web Single Sign On Profil" von OASIS und dem „Kantara eGovernment Implementation Profile". Dabei wird nur im Falle eines konkreten Authentifizierungserfordernisses der Browser zum Identity-Provider weitergeleitet. Nach Abschluss der Authentifizierung werden die PVP-Attribute wieder über den Browser zum Service-Provider (SP) geschickt. Bei der Benutzung einer S-Profil-Anwendung werden die Anfragen direkt zwischen Browser und SP ausgetauscht. (im Gegensatz zum R-Profil, indem alle Anfragen über die Portale geführt werden).

Dokumente der „PVP 2 Spezifikation":

- **PVP2-Allgemein** ist das Basisdokument, welches folgende Elemente enthält:
  a) Allgemeiner Teil mit Erklärungen und Zweckdefinition
  b) Die Beschreibung der notwendigen Nomenklatur und der Schreibweisen
  c) Die Architektur des Portalverbundprotokolls
  d) Die Anhänge
- **PVP2-Attribute Profile**
  Beschreibung der zwischen IdPs ausgetauschten Attribute
- **PVP2-R-Profil** ist die Weiterführung der „PVP 1.x Reverse Proxy Protokollvarianten". Das betrifft sowohl die HTTP/HTML-Bindung als auch die SOAP-Protokollbindung.
- **PVP2-S-Profil** konkretisiert die Verwendung der Basis-SAML-Profile.
- **PVP2-S-MD** (Metadaten Management) beschreibt die Prozesse der Verwaltung von SAML Metadaten

1.1 Versionsnummern für PVP2

In PVP2 wurden mehrere Profilvarianten auf einem gemeinsamen Datenmodell definiert. Daher ist es sinnvoll, die Versionsnummerierung dieser Tatsache anzupassen, da sonst bei minimalen Änderungen einzelner Profildefinitionen sämtliche anderen Spezifikationsdokumente neue Versionsnummern bekommen müssten, ohne dass es tatsächliche Änderungen gibt.

Das Hauptdokument **PVP2-Allgemein** behält die normale aus drei Zahlen bestehende Versionsnummerierung.
Format: H.U.F
(H…Hauptversion, U...Unterversion, F…Nummer für Fehlerkorrekturen und kompatible Erweiterungen);
z.B. 2.1.1

Die **PVP-...-Profil**-Dokumente haben dieselbe Versionsnummer wie das zugehörige PVP2-Allgemein – Dokument.
Die Änderung der Haupt- und Unterversion muss in allen Profil-Dokumenten berücksichtigt werden und führen auch dort zu einer neuen Versionsnummer.

Der komplette Dokumentensatz soll als ZIP-Archiv zur Verfügung gestellt werden. In dieser ZIP Datei sollte eine ReadMe-Datei die aktuelle Version anführen. Die ZIP-Datei soll die Versionsnummer im Dateinamen enthalten.

2 Zweck

Das Portalverbundsystem ermöglicht die Delegation von Identitätsprüfung, Authentifizierung und Autorisierung.
Das PV-Protokoll erweitert die Kommunikation zwischen Stamm- und Anwendungsportalen, indem vertrauenswürdige Aussagen über Authentizität, Autorisierung und Verrechnungsdaten getroffen werden (können).
Autorisierung bedeutet in diesem Zusammenhang, dass einem Benutzer für den Zugriff auf eine bestimmte Ressource („Anwendung") bestimmte Zugriffsrechte eingeräumt werden.
Die Kommunikation zwischen den Portalen muss Integrität und Vertraulichkeit gewährleisten.
Der Portalverbund (PV) im Sinne von [PVV 1.0] ist zur Kommunikation zwischen Körperschaften öffentlichen Rechts vorgesehen. Für den Verbund sind rechtliche, organisatorische und technische Betrachtungsweisen relevant, daher sind neben dieser technischen Protokollspezifikation weitere Dokumente wie die Portalverbundvereinbarung [PVV 1.0] und Sicherheitsklassen [SecClass] zu beachten.
Das Protokoll kann aber in einem anderen rechtlichen Kontext für weitere Zwecke verwendet werden:

- Kommunikation zwischen Behörden und Nicht-Behörden auf Grund bilateraler Vereinbarungen
- Kommunikation zwischen internen Stamm- und Anwendungsportalen
- Kommunikation zwischen Anwendungsportalen und Anwendungen
- Kommunikation in anderen Verbünden (z.B. Kammerportalverbund, Wirtschaftsportalverbund, etc.)

3 Schreibweise

3.1 Normative und nicht-normative Teile

Beispiele und Fußnoten sind nicht Teil der Spezifikation.

3.2 Begriffsbestimmung

Die Begriffe sind in [PVV 1.0] definiert.

Ergänzend dazu wird festgelegt:

3.2.1 Application Chaining

Das ist der Fall, wenn der Zugriff eines Benutzers auf eine Anwendung (implizit) aufgrund der Verwendung einer anderen Anwendung erfolgt. Diese „Verkettung" von Anwendungen wird englisch „chaining" bezeichnet.

3.2.2 Subteilnehmer

Bezeichnet eine Organisation (zugriffsberechtigte Stelle), die dem Portalverbund „indirekt" mittels einer Vereinbarung ([pv-zugriff] bzw. [pv-zugriff-dl]) mit einem Stammportalbetreiber beitritt. Die Vereinbarung inkludiert die Verpflichtung zur Einhaltung der Datensicherheitsmaßnahmen für Webanwendungen [pv-dasi] und Vorgaben für die Verwaltung von Zugangskonten und die Zuordnung von Anwendungsrechten ([pv-meld])

3.2.3 Participant

Beschreibt einen (Sub-)Teilnehmer aus technischer Sicht.

3.2.4 Verrechnungsdaten

Verrechnungsdaten bestehen aus der Identifikation des Rechnungsempfängers und der Liste der möglichen Kostenstellen und Gebührenstufen des Anwenders. Die Auswahl der konkreten Kostenstelle und Gebührenstufe einer Transaktion erfolgt in der Anwendung, nicht im PVP.

3.2.5 Identity-Provider (IdP), Service-Provider (SP), Attribute-Provider

Sind in **Fehler! Verweisquelle konnte nicht gefunden werden.**definiert.

3.3 Vergleiche zu anderen Nomenklaturen

PVP1	**SAML**	**RFC 2904**	**PVP2**
Anwendung	Service-Provider	Service Equipment	Service-Provider
Anwendungsportal		AAA-Server (Org1)	
Portalverbund	Circle of Trust	(agreement)	Portalverbund
Benutzer	Client	User	Principal
Stammportal	Identity-Provider	AAA-Server (Org2)	Identity-Provider, Attribute Provider
(Sub-)Teilnehmer		User Home Organization	Stammorganisation

Im **Fehler! Verweisquelle konnte nicht gefunden werden.**sind weitere Referenzen auf andere Standards dokumentiert.

4 Architektur

4.1 Basisprofile

Die Versionen des Portalverbundprotokolls beginnend mit Version 2.0 spezifizieren unterschiedliche Basisprofile in denen die Attribute der authentifizierten Benutzer und Systeme (Organisationszugehörigkeit, zugewiesene Rechte, transaktionsbezogene Verrechnungsdaten) kompatibel abgebildet werden.
Was sich jedoch ändert ist die Art des Transports der Informationen und das Kommunikationsmuster.
Es sind derzeit die Basisprofile „R-Profil" und „S-Profil" spezifiziert:

4.1.1 Basisprofil R (Reverse Proxy Profil)

Das „R-Profil" im PVP ist eine Fortführung des klassischen PVP1-Protokolls, in dem ein Stammportal den Benutzer authentifiziert, seine Rechte definiert und anschließend den HTTP-Request in einer „Reverse Proxy" Methode weiterreicht.

4.1.2 Basisprofil S (SAML Web-SSO Profil)

Das „S-Profil" implementiert eine Variante des SAML 2 Web-SSO Profils. Die Authentifizierung erfolgt an einem Identity-Provider (IdP). Nachrichten zwischen IdP und Service-Provider (SP) werden im Wesentlichen über den Browser der anfragenden Person ausgetauscht. (SAML sieht dafür die Varianten „Post-Binding", „Redirect-Binding" und „Artifact-Binding" vor).
Nach erfolgreicher Anmeldung übermittelt der IdP die PVP-Attribute in Form einer „SAML Assertion" (XLM-Datenstruktur).
Danach adressieren alle Browseranfragen direkt den SP. (Im Gegensatz zum R-Profil, wo alle Anfragen über Stamm- und Anwendungsportal zur Anwendung geführt werden)

Vor- und Nachteile der Basisprofile

Feature	R-Profil	S-Profil
Einbindung über VPN/IP-Adresseinschränkung	Einfacher durch beschränkte Anzahl von Stammportalen	Clients müssten über eigenes VPN oder Ähnliches gehen
Datenschutz	Stammportal liest Verkehr (Inhalt) mit	IdP erfährt nur die Authentifizierungsanfragen
Application Proxy	Für Sicherheit von DMZ sinnvoll	Müsste extra konfiguriert werden
Starkes Key Binding	nein	möglich
Anwendungskompatibilität	Relative ULRs, definierter Namespace	Keine speziellen Erfordernisse
Anwendungsschnittstelle	PVP	SAML

4.2 Akteure

Im Kontext des Portalverbunds besteht die Rechtsbeziehung nur zwischen IdP und SP (PVP1: Stamm- und Anwendungsportal). Die im PVP definierten Attribute beziehen sich auch auf Principals (Endbenutzer).
Für das Protokoll sind folgende Entitäten erforderlich:

- Principal (User- oder System Principal)
- IdP (Stammportal)
- SP (Anwendungsportal)

4.3 Message Sequenz

Der Portalverbund ist grundsätzlich neutral gegenüber dem Modell der Interaktionen zwischen Benutzern, Portalen und Anwendungen.
Für das „PVP R-Profil" ist derzeit jedoch ein Reverse-Proxy-Modell vorgesehen, wie es im RFC 2904 Abschnitt 3.1.1 als „agent sequence" definiert ist.
Das PVP S-Profil dagegen orientiert sich am SAML 2.0 WEB-SSO-Profil und implementiert daher eine Front-Channel Methode für die Anmeldungssequenz.

5 Bedingungen zur Konformität

Folgende Dokumente sind zu beachten, um einen technisch kompatiblen und den Sicherheitsanforderungen gemäßen Einsatz einer Einheit im Portalverbund (z.B. eines Portals, IDPs, SPs) zu gewähren.

5.1 Verbindliche Dokumente für das Portalverbundprotokoll V2

Prinzipiell sind alle Dokumente der PVP Spezifikation (dieses Dokument und seine Unterdokumente) einzuhalten, um Konformität mit dem PVP Protokoll zu erreichen.
Ein IdP bzw. ein SP ist auch dann kompatibel, wenn er nur R-Profil oder S-Profil umsetzt. Für die Kommunikation mit anderen Einheiten ist er in diesem Fall möglicherweise auf ein Gateway angewiesen.

5.2 Verbindliche Dokumente für den Verwaltungsportalverbund

Dokument-ID	*Titel*
[PVV 1.0]	Portalverbundvereinbarung (referenziert die Spezifikation der Sicherheitsklassen [SecClass])
[PVRechte]	Rechtemodellierung für Portalverbundanwendungen
[PV-GS]	Portalverbund Grundschutz
[PVP2-ZD-Policy]	Verwaltungsprozesse für zentrale Dienste

5.3 Empfohlene Dokumente (Best Practice)

Dokument-ID	*Titel*
[PVP2 BP]	PVP V2 Best Practice
[PVP-SMA]	PVP Sicherheitsmaßnahmen (Algorithmen)

Anhang A Referenzen

Sofern nicht anders angegeben findet man die referenzierten Dokumente unter http://reference.e-government.gv.at (http://www.ref.gv.at)

[AG-IZ Glossar]
Hörbe: Identity Management Glossar der AG-IZ

[pv-dasi]
Hafner, Wittmann: Datensicherheitsmaßnahmen für Webanwendungen

[PV-GS]
Reif: Portalverbund Grundschutz

[pv-meld]
Connert, Springer-Knam: Meldung der Benutzer- und Rechte-verwalter im Stammportal

[pv-zugriff]
Connert, Aichberger: Vereinbarung über die Einräumung von Zugriffsrechten im Portalverbund

[pv-zugriff-dl]
Connert, Aichberger: Vereinbarung über die Einräumung von Zugriffsrechten im Portalverbund über einen Dienstleister

[PVP-SMA]
Reif: Portalverbund Sicherheitsmaßnahmen (Algorithmen)

[PVP2 BP]
Lenz: PVP V2 Best Practice

[PVP2-ZD-Policy]
Hörbe, Stradal: Portalverbund Verwaltungsprozesse für zentrale Dienste

[PVRechte]
Stradal, Freidl, Gritschenberger, Pichler, Reif: Rechtemodellierung für Portalverbundanwendungen

[PVV 1.0]
Connert, Grandits, Kotschy, Posch, Siegl: Vereinbarung über die einzuhaltenden Rahmenbedingungen bei der Einrichtung und Benützung eines E-Government Portalverbundsystems (21.11.2002)

[SecClass]
Hörbe: Sicherheitsklassen für den Zugriff von Benutzern auf Anwendungen

Anhang B Änderungshistorie

PVP 2.1.0

- Einleitungstexte überarbeitet
- Kurzbeschreibung S-Profil überarbeitet
- Heraustrennen des PVP2-Attribute Profils
- Entfernen von Ideen zu in Zukunft geplanten Profilen
- Versionsnummerierung: Die Erstversionen der Profil-Dokumente haben jetzt dieselbe Versionsnummer wie PVP2-Allgemein. Erst bei Änderungen in Profil-Dokumenten werden Unterversionen gemacht, die mit einem Buchstaben gekennzeichnet sind. (z.B. PVP2-S-Profil 2.1.0.a)
- Kapitel "Key Bindings" gestrichen
- Kapitel Änderungshistorie ergänzt

PVP 2.1.1

- Keine technischen Änderungen
- Referenzen aktualisiert
- Formulierungen für bessere Verständlichkeit überarbeitet

PVP 2.1.2

- Vereinfachung der Konvention zur Versionierung der PVP Dokumente
- Neu: Kapitel 5 „Bedingungen zur Konformität"

PVP 2.1.3

- Div. Anpassungen in Sub-Dokumenten – Neue Versionsnummer
- Entfernen nicht mehr aktueller bzw. referenzierter Referenzen (PV-Whitepaper, PortalV-PKI, LDAP.gv.at, LDAP.gv.at-PV, RFC2616, VKZ), ergänzen fehlender Referenzen
- Entfernen des Verweises die schon in vorhergehenden Versionen gestrichene SOAP spezifische PVP-R-Profil Variante
- Ergänzen von PVP2-S-MD als Dokument der PVP-Spezifikation
- Vereinfachung der Beschreibung der verbindlichen PVP Dokumente (Beseitigung von Redundanzen mit dem Einleitungskapitel)
- Entfernen des Vermerkes, das an PV-GS und PV-ZD Policy noch gearbeitet wird.
- Ergänzungen in der Definition des Begriffes Subteilnehmer
- Dokumentreferenzen an die im jeweiligen Spezifikationsdokument verwendeten Schreibweise angepasst.