20. Juni 2012

Standardportal 2.0

Implementierung von PVP 2.0 für neue Wege im Federated Identity Management

Inhalt

- LFRZ GmbH
- Portalverbund
- PVP 1.x / Standardportal 1.0
- PVP 2.0 / SAML 2.0
- Standardportal 2.0
  - Funktionsumfang
  - Einsatz Open-Source-Produkte
  - PVP2 WebServices
  - Federation-Bridge
  - Sicherheit / Zertifizierung

LFRZ GmbH

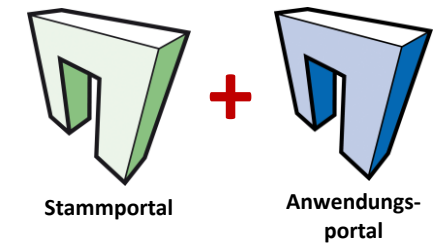
- LFRZ GmbH = Land, forst- und wasserwirtschaftliches Rechenzentrum GmbH
- IT-Dienstleister für die öffentliche Verwaltung
- 1968 als Verein gegründet, seit 2004 GmbH
- Eigentümer ist Verein, Mitglieder BMLFUW, BMF, AMA, ZAR und LWK (außerordentlich)
- MitarbeiterInnen: 40 interne und 10 externe
- Umsatz: € 7,6 Mio (2011)

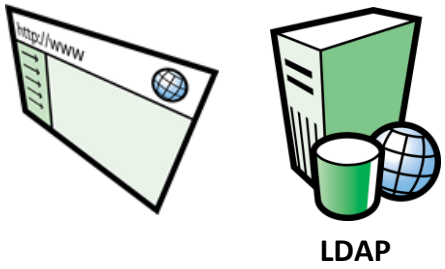
LFRZ Dienstleistungen und Lösungen

- E-Government Services
- Geografische Informationssysteme (GIS)
- Content Management Systeme
- Rechenzentrumsbetrieb
- Workflow Management Systeme
- SAP Dienstleistungen

E-Government Produkte & Services

- Standardportal
- Benutzer- u. Rechte-verwaltung (BRV)
- LDAP Behördenverzeichnis

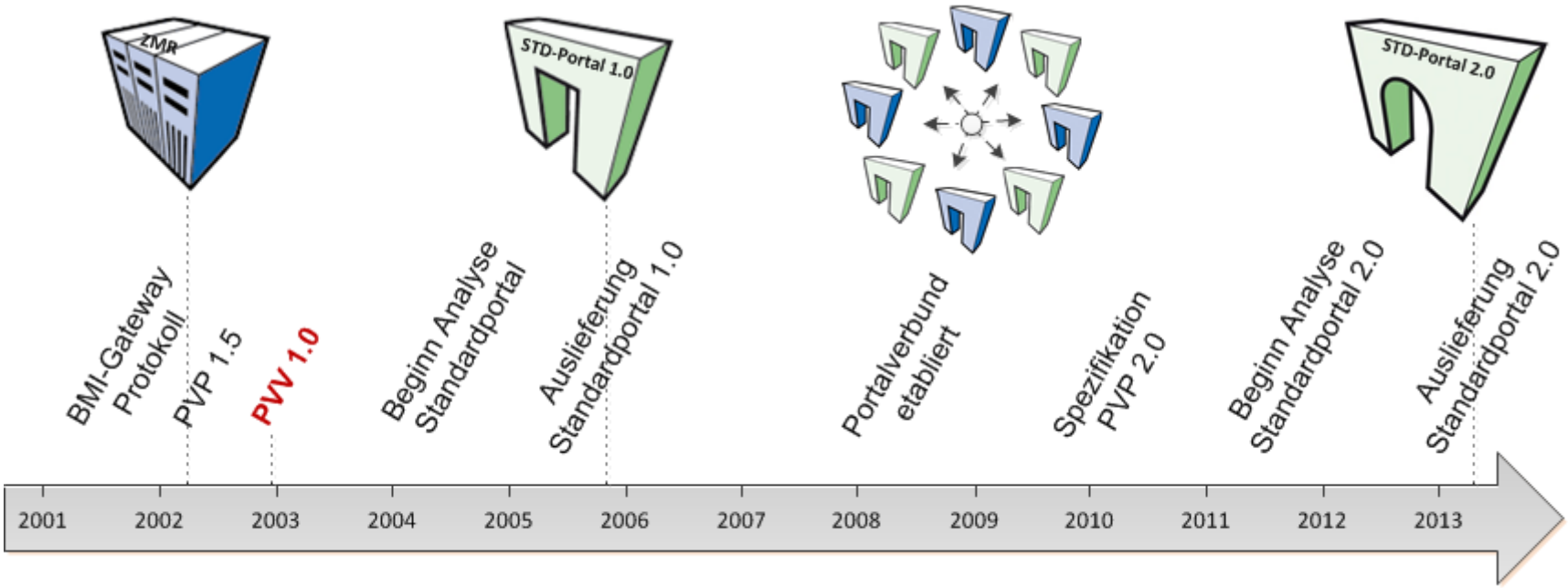




Was ist der Portalverbund?

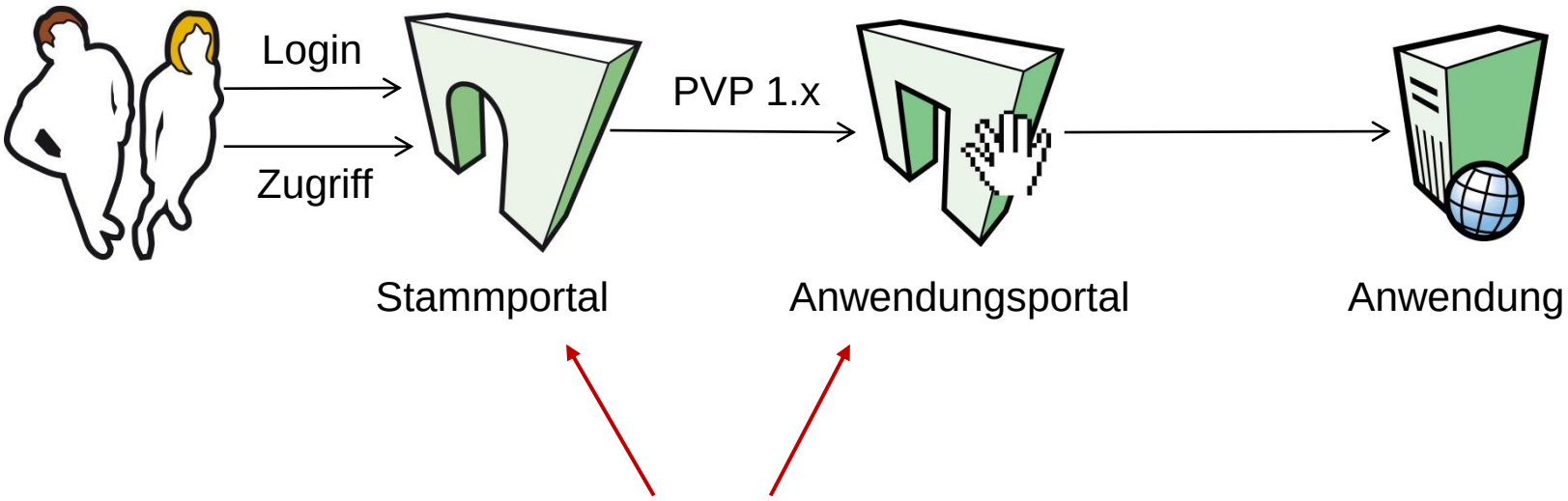
- Federated Identity Management für Behörden
- Benutzerverwaltung in verteilten Portalen *nicht* in den Anwendungen
- Rechtezuweisung durch zuständige Behörde (Ministerium, Land, Gemeinde)
- Rechtsgrundlage: Portalverbundvereinbarung (PVV 1.0)
- Technische Basis: Portalverbundprotokoll (PVP)

Entwicklung des Portalverbunds



Timeline Portalverbund / Standardportal

Portalverbundprotokoll Version 1



Standardportal 1.0 im Überblick

Rechteinhaber	LFRZ 2/3, BM.I 1/3
Gremien	Lenkungsausschuss und User-Group
Wartung	Durch LFRZ - regelmäßige Updates (bisher ~100 Builds)
Weiterentwicklung	Eigner Topf mit jew. 10% der Lizenzgebühr; jährliche Abstimmung der Erweiterungen in User-Group
Lizenznehmer	5 Ministerien, 8 Bundesländer (ausg. Tirol), HVB SV, Statistik, BEV, BBG, AGES, ÖGIZIN
Betrieb	Lizenznehmer oder als Shared Service (LFRZ)
Kosten Produktentwicklung	~ 1,5 Mio € in 7 Jahren

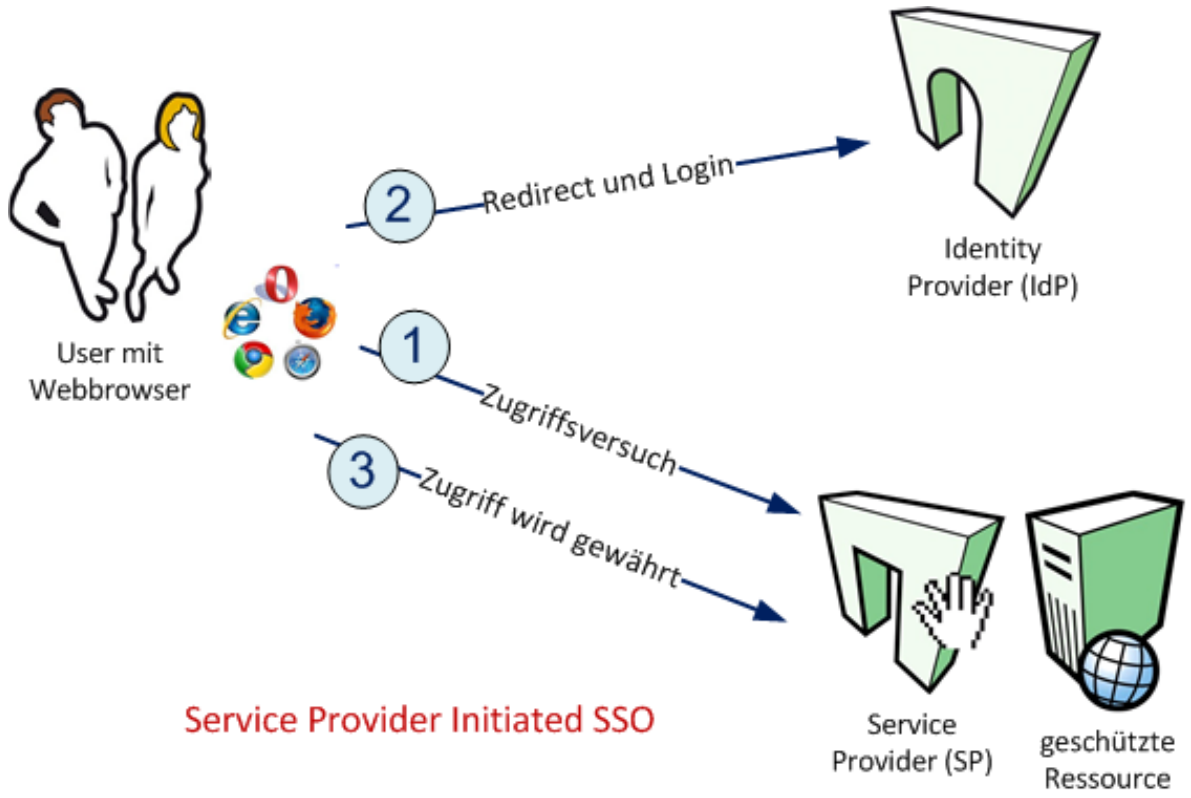
Datenbasis / Werkzeuge zur Portaladministration

- Datenmodell: LDAP-gv.at (aktuelle Versionen)
- Abstraktes Rechtemodell (PVP) als Grundlage für delegierte Benutzerverwaltung
- Benutzer- und Rechteverwaltung (BRV 2.0)
  - Version 2.0 mit neuem Design und erweiterter Suche
- Anwendungsportalverwaltung
  - Version 1.5 (Entwicklung des BM.I)
- LDAP Synchronisationstools

Portalverbundprotokoll Version 2

- PVP2 unterstützt folgende Profile
  - PVP2 R-Profil – Reverse-Proxy-Profil aufbauend auf PVP 1.x
  - PVP2 S-Profil – SAML 2.0 Web Browser SSO Profile
- SAML 2.0 (Security Assertion Markup Language)
  - Internationaler Standard zum Austausch von sicherheitsrelevanten Informationen über Identität und Eigenschaften von BenutzerInnen
  - Neue Begriffe –> Identity Provider (IdP), Service Provider (SP) und Attribute Provider

SAML Web Browser SSO Profile



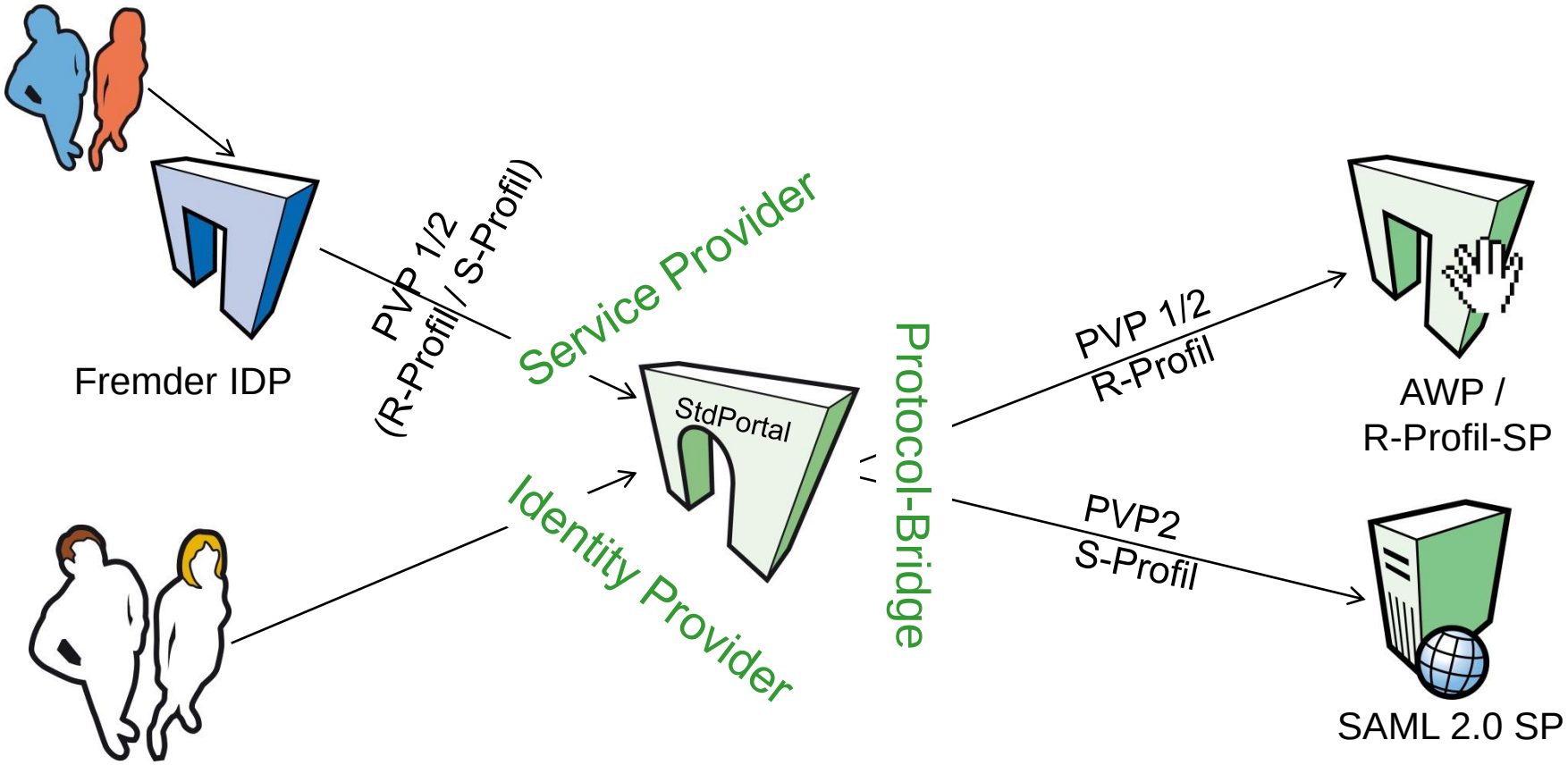
Vorteile von SAML 2.0

- Etablierter internationaler Standard (OASIS)
  - Vereinfachte Anbindung von Standardsoftware (SAP, Oracle, MS, ..)
  - Einfache Kopplung mit anderen SAML-Federations (z.B. UNIs, USP, ..)
  - Verwendung in europäischen Federations (z.B. STORK)
- Direkte Kommunikation von Browser mit Webanwendung
  - Geringere Anforderungen an Anwendungen u. weniger technische Risiken (z.B. bei Java-Applets, Office-Integrationen, Ajax-Apps,..)
  - Sprechende Zieladressen für Anwendungen
- Login bei Bedarf (Auswahl Identity Provider)
  - Anonymer Besuch der Webangebote, Anmeldung erst für Transaktion

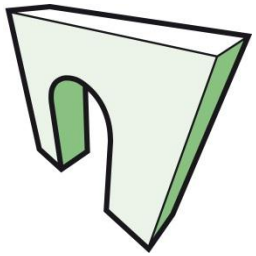
Standardportal 2.0 – Implementierung von PVP2

- SAML 2.0 Identity Provider (IdP)
- SAML 2.0 Service Provider (SP)
- Standardportal als Protocol-Bridge
- Multifederation Use-Cases z.B. Federation-Bridge
- PVP2 WebServices
- Sicherheitsüberprüfung u. Zertifizierung nach ÖNORM A7700

Standardportal 2.0 Java-Webapplikation für alle Funktionen



Open-Source-Produkte als Basis für SAML 2.0 Features

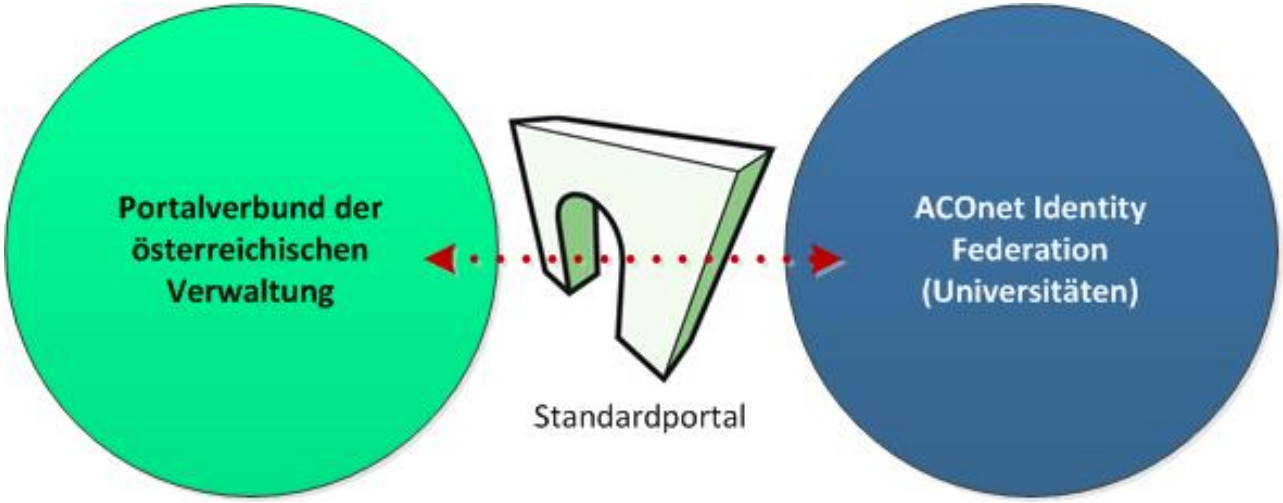


Standardportal 2.0

- Java basierender SP
- Aus dänischem E-Gov
- IdP Discovery
- Mozilla Public License V1.1

- SAML IdP
- IdP Discovery
- Pure Java
- Apache License 2.0

Standardportal als Federation-Bridge



PVP2 WebServices

- Basis ist Web Services Security SAML Token Profile (V1.1)
- Für SAML 1.1 und SAML 2.0
- Implementierung / Vorschlag für PVP2 Spezifikation
- Abstimmung im Projektverlauf mit AG-IZ

Sicherheit / Zertifizierung

- Security-Consulting durch Firma SEC Consult
- Erstellung eines Bedrohungsmodells
- Initiale Überprüfung und Audits für alle Releases
- Security Audit finale Version
- Abschluss mit Zertifizierung nach ÖNORM A7700

Projekt Standardportal 2.0

- Start: 01.03.2012
- Gemeinsame Abwicklung mit BM.I
- Adaptierung der PVP2 Spezifikationen bei Mängeln (AG-IZ)
- Early-Adopter-Versionen für Kunden ab Herbst 2012
- Finale Release Ende 1. Quartal 2013
- Aufwand ca. 550 PT (inkl. Analyse als Vorprojekt)
- Finanzierung aufgeteilt auf 18 Lizenznehmer

Zusammenfassung

- Standardportal ist eine Referenzimplementierung für PVP
- Authentifizierung und Autorisierung für behörden-übergreifende Nutzung von Anwendungen
- SAML Features durch Integration von Shibboleth – Standardframework für SAML 2.0
- Protocol-Brigde (PVP 1/2) für schrittweise Migration
- Erhöhte Sicherheit durch A7700 Zertifizierung

Ansprechpartner

Gerold Pesendorfer
LFRZ GmbH
Tel. +43 1 33176 – 232
gerold.pesendorfer@lfrz.at

Thomas Mader
BM.I – IV/2/d - ZMR
Tel. +43 1 90600 – 39178
thomas.mader@bmi.gv.at

Herzlichen Dank für Ihre Aufmerksamkeit!