

Portalverbund mit weiteren Benutzerkreisen		Whitepaper	
		PV-ErwBK 4.5.2007	
		interner Entwurf	
Kurzbeschreibung:	Die Kommunikation zwischen Portalen im Portalverbund war bisher auf öffentlich-rechtliche Körperschaften beschränkt. Die vorhandenen und zukünftigen Verbindungen außerhalb der Portalverbundvereinbarung sollen technisch und rechtlich auf einen gemeinsamen Nenner gebracht werden, um eine Vielzahl von bilateralen Regelungen und Protokollen zu vermeiden.		
Autor:	Rainer Hörbe	Projektteam / Arbeitsgruppe:	Q-PV
Beiträge von:	Wilfried Connert Franz Grandits Peter Pfläging		

Stelle:	Vorgelegt am:	Angenommen am:	Abgelehnt am:

Inhalt

1	Zusammenfassung.....	2
2	Einleitung	3
2.1	Bisherige Entwicklung.....	3
2.2	Kosten, Nutzen, Risiken	4
2.3	Ziele der Erweiterung	4
3	Konzept	5
3.1	Anwendungsfälle für die Erweiterung	5
3.1.1	Bildungsportalverbund	5
3.1.2	Unternehmen	5
3.1.3	Provider.....	5
3.1.4	Agrar- und Umweltbereich	6
3.1.5	Gesundheits- und Sozialbereich	6
3.2	Umsetzung des Portalverbunds über mehrere Domänen	7
3.2.1	Voraussetzungen.....	7
3.2.2	Struktur	7
3.2.3	Vertrauensstellung	9
3.3	Zertifikate für Stamm- und Anwendungsportale	10
3.3.1	Status Quo.....	10
3.3.2	Änderungsbedarf.....	10
3.4	Erweiterung des Portalverbundprotokolls	12

1 Zusammenfassung

Für die Kommunikation zwischen Organisationen der Verwaltung wurde der Portalverbund erfolgreich eingeführt. Die Infrastruktur des Portalverbunds wird zum Teil auch für den Zugang von Personen und Organisationen außerhalb der Verwaltung genutzt.

Aus den unten angeführten Anwendungsfällen Bildungsportalverbund, B2G, Agrarbereich und Gesundheitssektor ergibt sich ein erhebliches Potential um anwendungsspezifisches Identity Management auf ein Verbundsystem umzustellen.

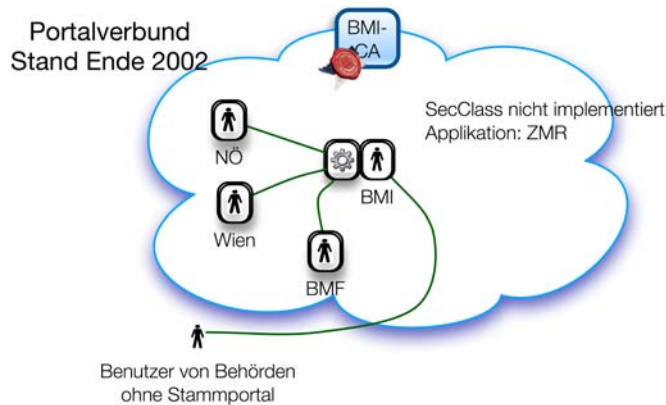
Das Nutzenpotential liegt in folgenden Punkten:

- Eine Vielzahl von bilateralen Nutzungsvereinbarungen, Sicherheitsrichtlinien und Protokollen kann auf multilaterale reduziert werden.
- Die Delegation der Benutzer- und Rechteverwaltung spart redundante Geschäftsprozesse ein.
- In unterschiedlichen Bereichen der öffentlichen Hand kann Infrastruktur gemeinsam genutzt werden und dadurch Entwicklungs- oder Lizenzkosten eingespart werden
- Die technische Offenheit der Portalstruktur ermöglicht die Koexistenz unterschiedlicher Authentifizierungsverfahren wie Bürgerkarte, Softwarezertifikate und UserID/Passwort. Dadurch können Anwendungen rasch ausgerollt werden und die Umstellung auf die aufwändigere Smartcardtechnologie kann entsprechend der Benutzerakzeptanz erfolgen.
- Identity-Management im Verbund ist eine Basiskomponente für eine Service Orientierte Architektur, die wiederum zu besserer und einfacherer Integration von Anwendungen führt.

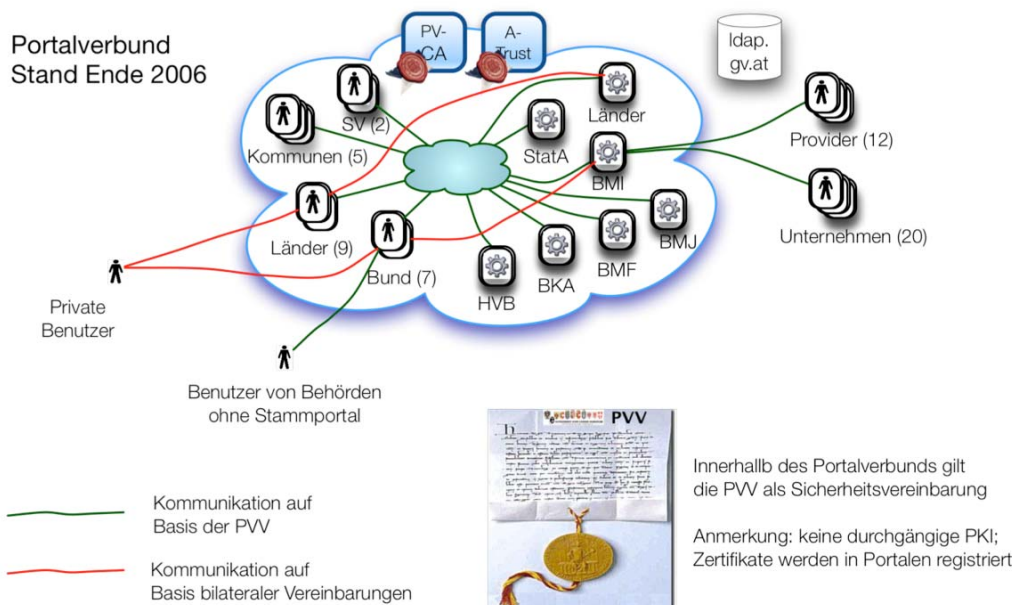
2 Einleitung

2.1 Bisherige Entwicklung

Der Vergleich der beiden Skizzen von 2002 und 2006 zeigt, dass der Portalverbund von einer überschaubaren Vernetzung mit der Möglichkeit Probleme ad hoc zu lösen, zu einem komplexeren Verbund mit der Notwendigkeit einer stärkeren Regulierung gewachsen ist:



In den nächsten Jahren wurden weitere Benutzerkreise, auch außerhalb der Portalverbundvereinbarung, angebunden:



2.2 Kosten, Nutzen, Risiken

Die **Kosten** für die Einbindung weiterer Benutzerkreise in den Portalverbund sind von mehreren Faktoren abhängig. Wird bereits ein PV-kompatibles Portal betrieben, wird die technische Anpassung geringfügig sein. Ist eine neue Infrastruktur einzurichten, sind neben den Lizenzkosten (0 .. mehrere 10,000€) die Kosten für Anpassung, Integration der Benutzer- und Rechteverwaltung, Betriebsumgebung, Inbetriebnahme, Wartung und Betrieb zu berechnen. Alternativ kann die Funktionalität auch als Service bei einem Provider eingekauft werden.

Der direkt quantifizierbare **Nutzen** liegt einerseits bei den Einsparungen für die redundante Benutzerführung, andererseits bei der Konsolidierung von Sicherheitsfunktionen in der Portalinfrastruktur, was für Anbieter mehrerer Anwendungen operative Einsparungen bringt.

Wo die Administrierbarkeit von redundanten Benutzerrechten in unterschiedlichen Systemen an ihre Grenzen stößt, entsteht der indirekte Nutzen durch die Einführung neuer Anwendungen.

Die Verpflichtung zur Kontrolle von Berechtigungen ist eine rechtliche Vorgabe, die in stark zersplitterten Systemen in der Praxis unerfüllt bleibt. Die Struktur des Portalverbunds ermöglicht wesentlich bessere Kontrollen.

Das technische **Risiko** ist gering, da der Portalverbund auf gut eingeführten Technologien (SSL, HTTP, SOAP) aufgebaut ist und sich in Umgebungen mit hoher Transaktionslast und Verfügbarkeit bewährt hat. Mittelfristig könnte die Anforderung entstehen, dass zur Integration SAML-kompatibler Produkte PVP auch als SAML-Profil implementiert werden muss¹.

2.3 Ziele der Erweiterung

Der Schwerpunkt der Erweiterung des Portalverbundes liegt in der Organisation weiterer Benutzerkreise nach dem Schema des Portalverbunds.

Anwendungsverantwortlichen innerhalb und außerhalb der Verwaltung soll die Möglichkeit eröffnet werden Benutzern verschiedener Benutzerkreise den Zugriff auf ihre Anwendungen einzuräumen. Dabei sollte auf Webanwendungen zurückgegriffen werden, bei denen Benutzer bereits registriert sind. Bei den meisten Anwendungen lässt sich eine Portalintegration im Rahmen der bestehenden Technologie realisieren, wodurch ein günstiges Kosten/Nutzen-Verhältnis erwartet werden kann.

¹ Die aktuelle Architektur unterstützt SAML nur als Authentifizierungsmethode am Stammportal

3 Konzept

3.1 Anwendungsfälle für die Erweiterung

3.1.1 Bildungsportalverbund

Das Unterrichtsministerium hat die Errichtung eines Portalverbundes für Bildungsinhalte beauftragt, wo Lehrer und Schüler (später auch Eltern) auf Inhalte des Bildungssektors zugreifen können werden. Neben der Vereinheitlichung der Infrastruktur ist die Vermeidung von Redundanzen in der Benutzerverwaltung und der Authentifizierung erwünscht, wenn Lehrer auf Inhalte im Verwaltungs- *und* Bildungsbereich zugreifen (z.B. Sokrates, Gehaltsabrechnung). Der umgekehrte Fall ist auch denkbar: Dass e-Learning-Content der Verwaltung angeboten wird.

Die Authentifizierung im Bildungsportalverbund wird für die Kontrolle der Nutzungsrechte der Inhalte benötigt, darüber hinaus sind keine Informationen über die Benutzer an die Anwendung zu übermitteln. Das ist nicht kompatibel mit den Anforderungen der Sicherheitsklasse 1 nach der Portalverbundvereinbarung, entsprechend muss für diesen Fall eine Konvention geschaffen werden.

3.1.2 Unternehmen

Ca. 25 Unternehmen betreiben derzeit ein eigenes PVP-kompatibles Stammportal, um auf das ZMR zuzugreifen, über 2.000 weitere KMUs greifen auf das ZMR über Stammportale von Providern zu. In Zukunft könnten Unternehmen auf Verwaltungsanwendungen anderer Ämter zugreifen, etwa bei Statistik, Finanz und Justiz. Durch eine Einbindung der Kammern könnte die Unternehmer-eigenschaft verlässlich verwaltet werden, eine Delegation der Rechte könnte direkt durch das Unternehmen realisiert werden. Vor allem für große Unternehmen ist eine zentrale Rechteverwaltung im Unternehmen interessant, da so eine Kontrolle der vergebenen Rechte und erfolgten Zugriffe einfach realisierbar ist.

In vielen dieser Bereiche ist eine umfassende Vereinbarung im Sinne der PVV nicht sinnvoll oder ökonomisch, etwa bei der Abgabe von Statistikmeldungen. Für diese Klasse von Anwendungsfällen ist das Konzept zu erweitern.

3.1.3 Provider

Die Konstellation, dass kostenpflichtige Anwendungen der Verwaltung für Bürger und KMU über Provider angeboten werden, ohne dass der Benutzer eine Personenbindung benötigt, kommt neben dem ZMR auch für andere Anwendungen wie Grund- und Firmenbuch vor. PVP kann hier zur Vereinheitlichung der Protokolle verwendet werden.

3.1.4 Agrar- und Umweltbereich

Ähnlich wie beim Agrarbereich gibt es einen Bestand von jeweils mehreren 10,000 Benutzern in Anwendungen unterschiedlicher Organisationen, wie Landwirtschaftsministerium, LFRZ, AMA, Statistik und Landwirtschaftskammer, mit potentiell sehr großen Überschneidungen. Mit der Einrichtung eines Agrarportals, in dem diese Benutzerstämme zusammengeführt werden, könnte eine Konsolidierung erreicht werden.

Im kleineren Ausmaß gibt es Benutzergruppen in Forschung und NGOs, denen Zugriffsrechte etwa für CMS-Systeme eingerichtet werden.

3.1.5 Gesundheits- und Sozialbereich

Für die Geschäftsfälle zwischen Krankenanstalten öffentlicher Betreiber und den Bereichen Sozialversicherung, Statistik und Standesamt ist die derzeitige Portalverbundvereinbarung ausreichend. Andere Anwendungsfälle betreffen Benutzer, die nicht in den Geltungsbereich der PVV fallen. So haben Amtsärzte z.B. diverse Bezüge (Aufsicht, Untersuchung) zu Stellen, die nicht als beliehene Unternehmen einzustufen sind, wie niedergelassene Ärzte, Sanitätsdienste, Heime, Apotheken und Schulen.

Wegen der starken Vernetzung zwischen Gesundheits- und Sozialbereich wäre zu überlegen hier einen Benutzerkreis nach einheitlichen Richtlinien zu schaffen.

Die Benutzergruppen aus diesem Bereich sind ohne Anspruch auf Vollständigkeit:

- Private Krankenanstalten
- Kuranstalten und Heilbäder
- Alten- und Pflegeheime
- Apotheken
- Leichenbestatter
- Gesundheitsdienstanbieter (niedergelassene Ärzte, Hebammen, Therapeuten, ..)
- Sachverständige
- Sachwalter
- Hilfswerk
- Sanitätsdienste
- Kindergärten und Horte
- Vereine zur Sozialbetreuung

Der Nutzen der Einbindung in ein Portal ist vor allem dort gegeben, wo Organisationen überregional tätig sind und z.B. mit Bezirkshauptmannschaften unterschiedlicher Länder kommunizieren.

3.2 Umsetzung des Portalverbunds über mehrere Domänen

3.2.1 Voraussetzungen

Es sind unabhängig von der Organisationsform folgende Anforderungen aus der Vertrauensstellung zwischen Stammportal und Anwendungsverantwortlichem abzuleiten:

- Die organisatorischen und sicherheitstechnischen Bedingungen der Anwendungsverantwortlichen müssen durchgesetzt werden können.
- Es muss ein einheitliches Sicherheitsverständnis geben, da sonst das Sicherheitsniveau reduziert werden könnte, oder wieder bilaterale Sicherheitsvereinbarungen mit ihren unerwünschten Nebenwirkungen geschaffen würden.

3.2.2 Struktur

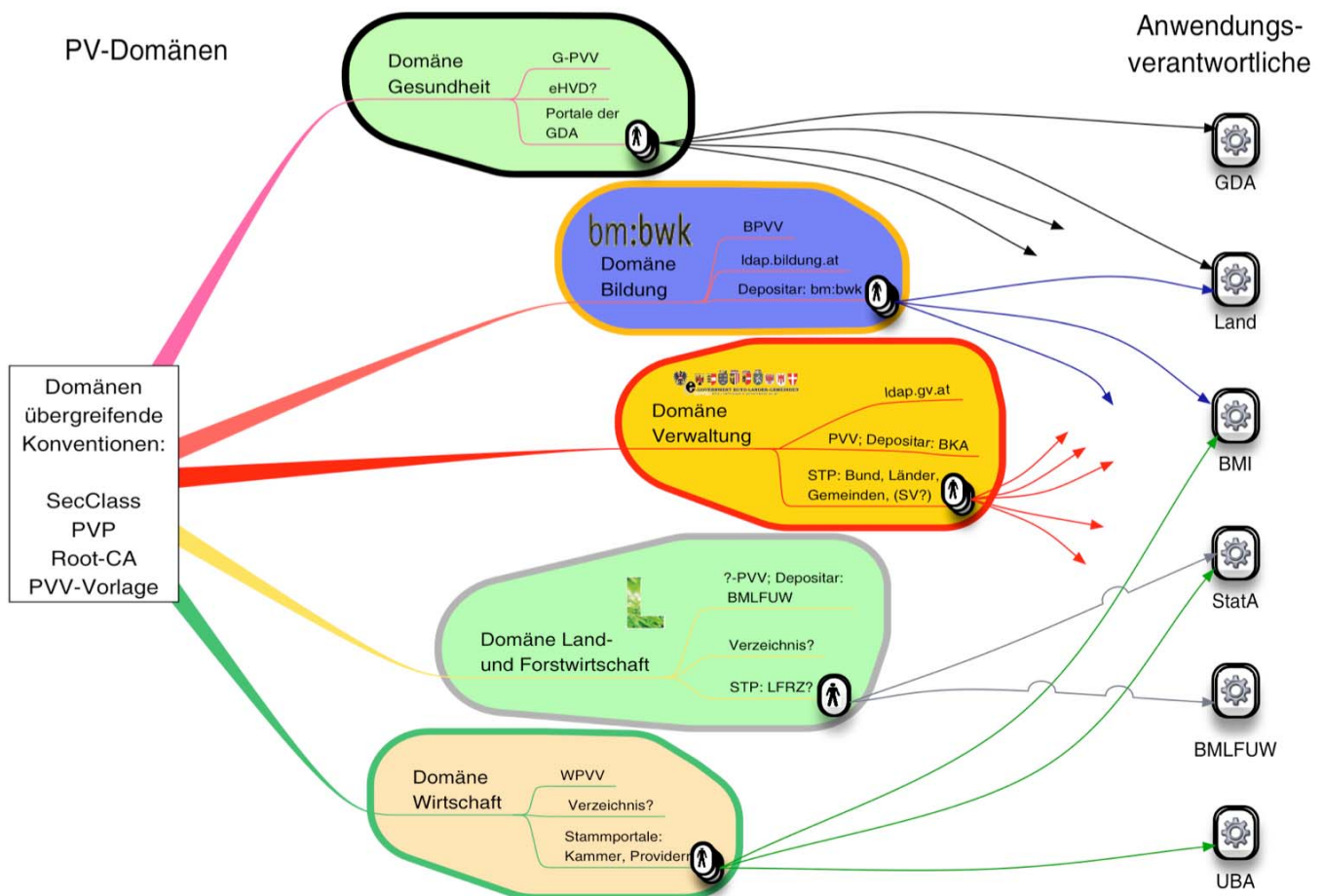
Für die Erweiterung um weitere Benutzerkreise außerhalb der Verwaltung sind zentralisierte Strukturen für Registratur, Sicherheitsverträge, Zertifizierung, Verwaltung und Revision wegen der zu komplexen Abhängigkeiten nicht sinnvoll. Der hier vorgeschlagene Mittelweg zwischen bilateralen Verträgen (wie bereits im Fall **Fehler! Verweisquelle konnte nicht gefunden werden.** gezeigt) und einer einheitlichen Vereinbarung für alle Teilnehmer ist:

- Der erweiterte Portalverbund wird in Portalverbunddomänen (PV-Domänen) eingeteilt, die jeweils eine domänenspezifische Portalverbundvereinbarung (PVV) haben. PV-Domänen werden aus den Klassen der zugriffsberechtigten Stellen gebildet.
- Neben dem Depositär wird ein Organisator ernannt, der die einheitliche Vereinbarung der Domäne erstellt und deren Umsetzung organisiert.
- Pro Domäne werden eigene Verträge nach dem Muster der PVV der Verwaltung geschlossen und Depositäre definiert. Der Depositär richtet den Verzeichnisdienst der Domäne ein.
- Anwendungsverantwortliche entscheiden, welche Vereinbarungen ausreichend sicher sind um darauf aufbauend Benutzerrechte zu delegieren. Für den Anwendungsverantwortlichen ist keine Mitgliedschaft in der jeweiligen Domäne der Benutzer erforderlich. Sie müssen sich aber
- Beim Zugriff prüft die Anwendung², ob die Definition des Anwendungsrechts einen Zugriff aus der Domäne des Stammportals erlaubt.
- Anwendungsverantwortliche gehen eine Publikationspflicht (entsprechend §4 und §5 der PVV) ein. Die Publikation erfolgt in strukturierter Form über den Verzeichnisdienst der Domäne.

² technisch gesehen das AWP

Beispiel für den Domänen übergreifenden Zugriff:

- Die Benutzer sind in die Domänen Gesundheit, Bildung, Verwaltung, Landwirtschaft und Wirtschaft zusammengefasst.
- PV-Teilnehmer treten dem PV ihrer Domäne bei, was beim Depositar veröffentlicht wird. Zugriffsberechtigte Stellen werden in Sicherheitsvereinbarungen verpflichtet, diese wiederum verpflichten die Endbenutzer.
- Anwendungsverantwortliche räumen den PV-Teilnehmern unterschiedlicher Domänen Zugriffsrechte auf ihre Anwendungen ein.
- Der Zugriff aus unterschiedlichen Domänen erfolgt über eine einheitliche Infrastruktur, die durch PVP und SecClass standardisiert sind.
- Die in den Domänen verwendeten CAs werden über eine gemeinsame Root-CA quersigniert.



Für jede Domäne sind neben der PV-Vereinbarung vom Depositar weitere Daten zu publizieren:

- Definition und Kennzeichnung der Teilnehmer der Portalverbunddomäne (z.B. mit einem Namensraum des OrgKZ)
- Nutzungsbedingungen

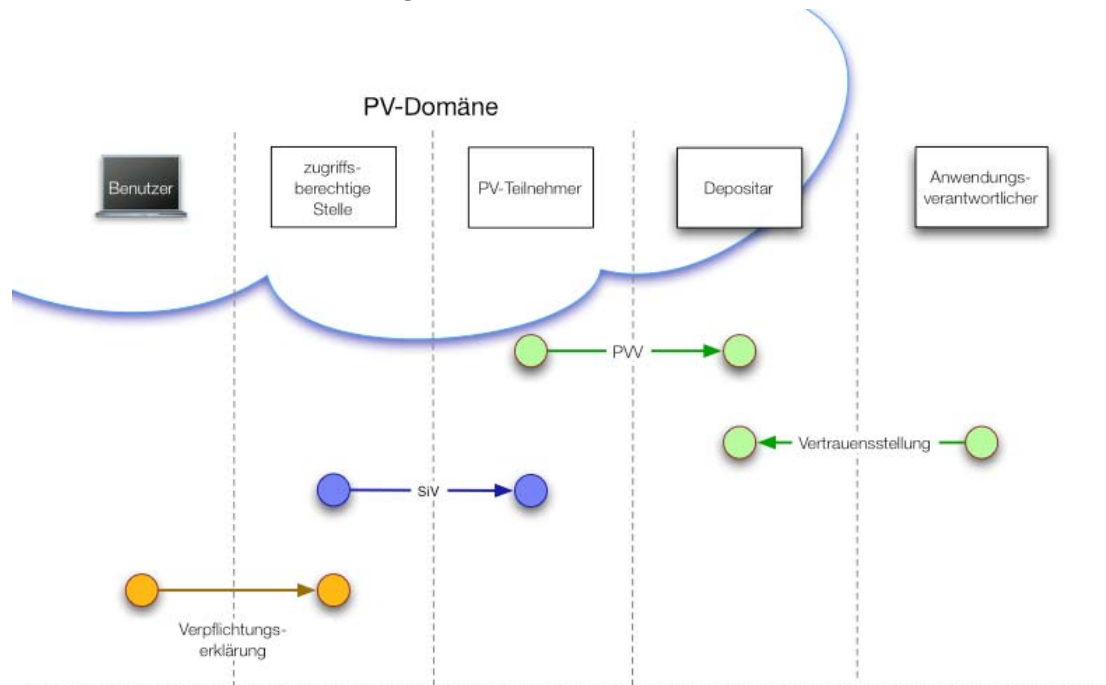
Vom Anwendungsverantwortlichen sind weiters zu publizieren:

- Daten der Anwendung und Anwendungsrechte

Teile der Vereinbarung, die sich gut formalisieren lassen, sollen in geeigneter Form, etwa über einen Verzeichnisdienst mit dem Schema ldap.gv.at, in strukturierter Form kommuniziert werden.

Aus diesen Überlegungen ergibt sich folgende Vertrauensstellung:

3.2.3 Vertrauensstellung



3.3 Zertifikate für Stamm- und Anwendungsportale

Serverzertifikate für Anwendungsportale bieten Stammportalen die Möglichkeit zu verifizieren ob das Anwendungsportal zur Domäne im Hostnamen gehört. Bei der Konfiguration soll der Stammportal-Administrator überprüfen, ob die Domäne gültig ist und für wen das Zertifikat ausgestellt wurde.

Bei Stammportalen im Portalverbund ist die Anforderung an die Authentizität höher: Der Anwendungsverantwortliche delegiert die Benutzer- und Rechteverwaltung an den Stammportalbetreiber. Somit muss für jedes Stammportal gewährleistet sein, dass

- o der Betreiber die PV-Vereinbarung der Domäne unterzeichnet hat,
- o der Betreiber nur zugriffsberechtigte Stellen am Stammportal führt, die wiederum die notwendigen Pflichten für die Teilnahme am Portalverbund übernommen haben, und
- o das Stammportals (durch ein Zertifikat) sicher authentifiziert wird.

Eine Verifikation des Hostnamens im Zertifikat durch einen Reverse DNS-Lookup des Anwendungsportals ist aus netzwerktechnischen Gründen nicht praktikabel und soll daher keine zwingende Voraussetzung für die Kommunikation sein.

3.3.1 Status Quo

Stammportale verwenden Serverzertifikate kommerzieller Anbieter (z.B. A-Trust, Trustcenter.de und Thawte) oder der PortalV-CA des BMI. Behörden sollten Serverzertifikate mit Verwaltungseigenschaft verwenden, wofür es derzeit nur Zertifikate von A-Trust und dem BMI gibt.

Anwendungsportale verwenden Zertifikate kommerzieller Anbieter.

Die Zertifikate der Stammportale werden in den jeweiligen Portalen registriert, wobei auch die rechtlichen Voraussetzungen des Stammportals geprüft werden.

Für die nahe Zukunft³ ist die zentrale Registratur von Stammportalen durch das BKA und die Publikation unter ldap.gv.at geplant. Damit wird die mehrfache Registratur an den Anwendungsportalen eliminiert. Da mit dem Stammportal auch gleich das dazu gehörende Zertifikat registriert wird, sind CA und Verwaltungseigenschaft sekundär.

3.3.2 Änderungsbedarf

3.3.2.1 Eliminierung der Verwaltungseigenschaft

Die Auflage, dass Serverzertifikate von Verwaltungsorganisationen eine Verwaltungseigenschaft⁴ haben müssen, sollte aus folgenden Gründen wieder fallen gelassen werden:

³ Im Anschluss an die Erstbefüllung dieser Daten durch das BMI

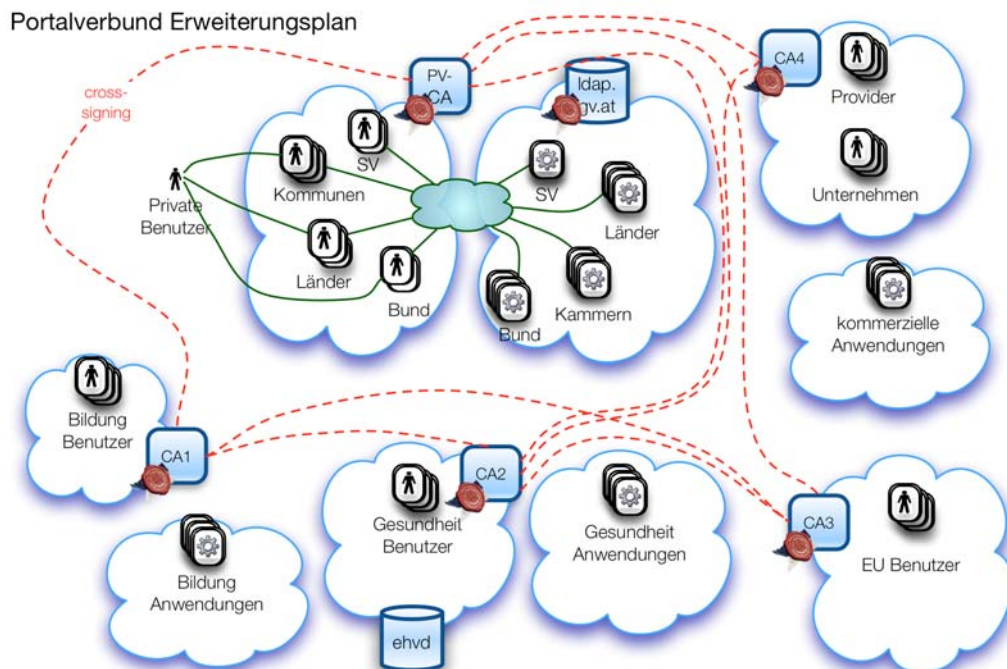
⁴ http://www.cio.gv.at/securenetworks/si-stu/sicherheitsstufen_v13_20030724.pdf

1. Die Verwaltungseigenschaft ist etwas vage spezifiziert: Trifft sie nur für Behörden zu, oder für Ämter in wirtschaftlichen Tätigkeiten? Auch bei Privaten, die als Organwalter staatlicher Auftraggeber tätige werden, ergeben sich Abgrenzungsprobleme. Z.B.: Warum haben BRZG und LFRZ die Verwaltungseigenschaft, nicht aber ASFINAG und Kommunalnet? Würden sie Notare in behördlicher Funktion bekommen?
2. Die Beziehung zum Portalverbund (PVV oder PV-DASI) ist spezifischer als die Verwaltungseigenschaft und macht diese somit überflüssig.
3. Die korrekte Verwaltung von Zertifikaten stellt an manche Organisationen bereits hohe Anforderungen, eine Prüfung von Zertifikatsattributen würde möglicherweise nicht vollständig umgesetzt werden, weil die technische Umsetzung von der Entwicklungswerkzeugen nicht gut unterstützt wird.

3.3.2.2 Zertifikatsmanagement

Die Verwaltung der Zertifikate passiert auf mehreren Stellen:

- o Die in den Domänen des erweiterten PV genutzten CAs werden von einer gemeinsamen Root-CA quersigniert.
- o Die Zertifikatsattribute (Seriennummer, Issuer) der Stammportale einer Domäne werden vom jeweiligen Depositar in einem vertrauenswürdigen Verzeichnis konform zu ldap.gv.at veröffentlicht.
- o Der Anwendungsportalbetreiber kann die Zertifikate pro Domäne akzeptieren oder einzeln registrieren.



3.4 Erweiterung des Portalverbundprotokolls

Der PVP-Token soll so erweiterbar gemacht werden, dass domänenspezifische Attribute übermittelt werden können, ohne dass Portale, die diese Erweiterungen nicht kennen, dadurch beeinträchtigt werden. Erweiterungspunkte sollen unter anderem in den Kategorien Authentifizierung, Autorisierung und Accounting gemacht werden.

Der folgende Erweiterungsvorschlag ist für den Fall gedacht, dass zwischen den Sicherheitsklassen 0 und 1 eine weitere Abstufung einzuführen wäre. Das Datenmodell des PVP-Tokens wäre für diesen Zweck zu ergänzen:

- Für Benutzer der Sicherheitsklasse 0 ist der Grad der Identifikation und der Authentifizierung anzugeben:

Identifikationsstufe des Benutzers:

- Anonym: Benutzer ist nicht authentifiziert
- Nicht identifiziert: Benutzer ist authentifiziert, aber keiner Person zugeordnet
- Identifiziert: Benutzer ist einer Person zugeordnet
- Gesicherte Identität: Benutzer ist amtlich identifiziert

Authentifizierungsstufe

- nicht authentifiziert
- Authentifizierung durch Wissen
- Authentifizierung durch Wissen und Besitz (kopierbar⁵)
- Authentifizierung durch Wissen und Besitz (nicht kopierbar⁶)

⁵ TAN-Liste, Zertifikat auf Speicherkarte oder Festplatte

⁶ Zertifikat auf Smartcard