

Bildungsportal-Verbund

BPVP Bildungsportal-Verbund Protokoll Kurzspezifikation

Für weitere technische Details nehmen kontaktieren Sie bitte:

Robert.kristoefl@bmbwk.gv.at

Thomas.menzel@bmbwk.gv.at

Version 0.5, Stand: 10.03.2005

**Im Auftrag des Bundesministeriums für
Bildung, Wissenschaft und Kultur (BMBWK)**

MR Dr. Robert Kristöfl, BMBWK

Technische Herausgeber

Franz Schildberger, CSD Management Consulting GmbH

Unter Mitarbeit von

MinR DI Dr. Robert Kristöfl, bm:bwk

Dr. Thomas Menzel, bm:bwk

Robert Hach, CSD Software Entwicklungsges.m.b.H

Peter Pichler, CSD Software Entwicklungsges.m.b.H

Inhaltsverzeichnis

1	Management Summary	3
2	Aufbau des Bildungsportal-Verbundes	4
2.1	Ablauf einer BPVP Anfrage	4
2.2	Teilnehmer und Zuständigkeiten	5
<i>Benutzer</i>		5
<i>Das Stammportal</i>		5
<i>Outbound Gateway</i>		5
<i>Das Bildungsdirectory des Ministeriums</i>		5
<i>Das Anwendungsportal</i>		5
<i>Inbound Gateway</i>		5
3	Bildungsportal-Verbund Protokoll	6
3.1	BPVP Parameter	6
3.2	Globale Rollen (BPVP Parameter GlobalRoles)	6
3.3	Anwendungsbezogene Rollen (ApplicationRoles)	6
3.4	Rollenparameter	6
3.5	Fehlermeldungen	6
3.6	HTTP-Bindung	6
3.7	Zertifikate / Sichere Verbindungen	6
4	Datenstrukturen	8
4.1	Rollen, Rollenstrukturen, Anwendungsportale und Applikationen	8
4.2	Rollenzuordnungen	8
<i>User (Benutzer)</i>		8
4.3	Datenstrukturen im Bildungsdirectory des Ministeriums	8
<i>HomePortal (Stammportal)</i>		8
5	Soap Schnittstelle des Bildungsdirectorys	9
6	Design Rechteverwaltung / Beispiele	9
6.1	Rechteverwaltung in den Stammportalen	9
6.2	Applikationsinterne Rechteverwaltung / redundante Benutzerdatenverwaltung	10
7	Appendix A: Schnittstelle für den Import von Benutzerdaten	11

1 Management Summary

Das System des Bildungsportal-Verbundes basiert auf dem Konzept des Portalverbundes (e-government Bund-Länder-Gemeinden, siehe <http://reference.e-government.gv.at/>) und wurde speziell für die Anforderungen des Bildungsbereichs adaptiert.

Der Portalverbund definiert das Zusammenspiel von Stammportalen und Anwendungsportalen. Stammportale verwalten Benutzerdaten und Rechte und sind für die sichere Authentifizierung von Benutzern zuständig.

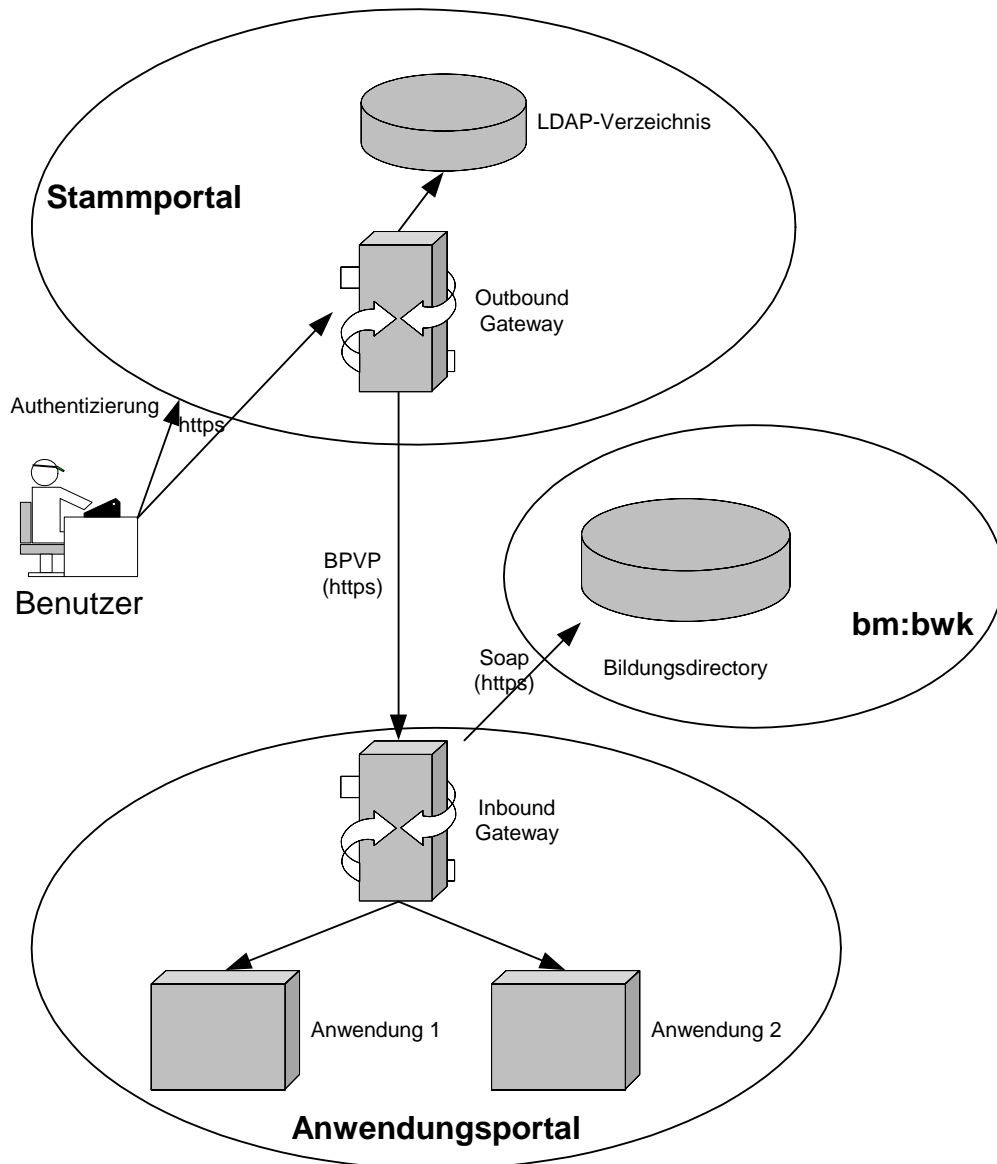
Anwendungsportale stellen Inhalte zur Verfügung. Anwendungsportale sind von der Verwaltung von Benutzerdaten und Rechteinformationen entlastet.

Zusätzlich zu den Konzepten des Portalverbundes gibt es im Bildungsportal-Verbund ein zentrales Verzeichnis aller Stamm- und Anwendungsportale – das Bildungsdirectory. Im Bildungsdirectory werden die Rechte von Stammportalen definiert. Zudem stellt das Bildungsdirectory ein zentrales Verzeichnis verfügbarer BPVP Applikationen und derer Rechtestruktur dar.

Weiters kennt der BPV globale Rollen, mithilfe derer grundsätzliche Rollen-zugehörigkeiten definiert und kommuniziert werden können (z.B. Schüler, Lehrer,...)

Das System des BPVP reduziert den Aufwand für die Verwaltung von Benutzerdaten und ermöglicht Single-Sign-On für alle Anwendungen des Verbundes. Es werden Einsparungen bei der Datenpflege im Bereich der Schulverwaltungen erwartet.

2 Aufbau des Bildungsportal-Verbundes



2.1 Ablauf einer BPVP Anfrage

Ein Benutzer meldet sich mit einem Internet-Browser an dem Stammportal an, bei dem er registriert ist. Seine Benutzerdaten sind im Bereich seines Stammportals gespeichert. Für den Zugriff auf Inhalte, die von fremden Anwendungsportalen bezogen werden, stellt das Stammportal Links zur Verfügung. Diese verweisen auf das Outbound Gateway des Stammportals. Das Gateway prüft, ob der Benutzer für die Applikation prinzipiell berechtigt ist, und es erweitert die Anfrage des Benutzers um die in diesem Protokoll definierten Parameter, welche die Rechte des Benutzers für die gewählte Anwendung beschreiben.

Die erweiterte Anfrage des Benutzers wird über eine sichere Verbindung an das Inbound Gateway des Anwendungsportals weitergeleitet, wo die mitgesendeten Parameter überprüft werden. Neben Vollständigkeit wird geprüft, ob für den angefragten Inhalt Rechte gemeldet wurden, die den Zugriff auf die Anwendung erlauben. Anhand der Daten aus dem zentralen Bildungsdirectory des Bundesministeriums wird geprüft, ob der Inhalt mit den gemeldeten Rechten für das anfragende Portal zulässig ist. Wurde die Anfrage positiv geprüft, wird sie an die Anwendung weitergeleitet und dort beantwortet.

2.2 Teilnehmer und Zuständigkeiten

Benutzer

Benutzer des BPV greifen mithilfe eines Internetbrowser auf das Stammportal zu, an dem sie registriert sind. Welche Inhalte direkt vom Stammportal zur Verfügung gestellt werden, und welche aus dem Bildungsportal-Verbund bezogen werden, bleibt für den Benutzer transparent. Er benutzt das Portal wie eine Web-Anwendung.

Das Stammportal

Das Stammportal ist die zentrale Anlaufstelle für Benutzeranfragen. Hier sind die Benutzerdaten und die Benutzerrechte gespeichert. Es ist Aufgabe des Stammportals, den Benutzer sicher zu identifizieren.

Outbound Gateway

Das Outbound Gateway ist Teil des Stammportals. Es bildet die Schnittstelle zu Inhalten aus dem BPV. Es prüft, ob eine Anfrage prinzipiell zulässig ist und leitet die Anfrage via SSL an das jeweilige Anwendungsportal weiter. Dabei wird die Anfrage um die BPVP-Parameter erweitert. Die Antwort wird an den Benutzer zurückgegeben. Alle Requests, die über das Outbound Gateway weitergeleitet werden, werden zu Revisionszwecken protokolliert.

Das Bildungsdirectory des Ministeriums

In diesem Verzeichnis wird verwaltet, welches Portal mit welchen Rechten auf welchen Inhalt zugreifen darf. Anwendungsportale greifen auf diese Informationen zu und benutzen diese, um BPVP-Anfragen zu verifizieren.

Das Anwendungsportal

Das Anwendungsportal stellt Inhalte zur Verfügung. Es vertraut den vom Stammportal gemeldeten Benutzerrechten.

Inbound Gateway

Das Inbound Gateway ist die Schnittstelle eines Anwendungsportals zum BPV. Es prüft die gemeldeten Rechte über das Bildungsdirectory des Ministeriums. Zudem werden alle Requests für die Revision protokolliert.

3 Bildungsportal-Verbund Protokoll

3.1 *BPVP Parameter*

Verschiedene Parameter sind im BPVP spezifiziert und werden bei Anfragen eines Stammportals an ein Anwendungsportal mitgeschickt. Sie identifizieren den Benutzer und definieren seine Rechte.

3.2 *Globale Rollen (BPVP Parameter GlobalRoles)*

BPVP definiert zusätzlich zu den Mechanismen des PVP "Globale Rollen". Einem Benutzer zugeordnete globale Rollen werden an alle Anwendungen weitergegeben.

Folgende globale Rollen sollen in allen Stammportalen verwendet und verwaltet werden:

- SCHUELER
- LEHRER
- ERZIEHUNGSBERECHTIGTER
- VERWALTUNGSPERSONAL

Einer Person können auch mehrere globale Rollen zugeordnet sein (z.B. LEHRER; ERZIEHUNGSBERECHTIGTER)

3.3 *Anwendungsbezogene Rollen (ApplicationRoles)*

Das Konzept applikationsspezifischer Rollen entspricht dem Rollenkonzept wie es auch im Portalverbund verwendet wird. ApplicationRoles können als Applikationsrechte verstanden werden, die im Stammportal verwaltet werden.

3.4 *Rollenparameter*

Strukturell sind Rollenparameter sowohl für globale, als auch für anwendungsbezogene Rollen vorgesehen. Derzeit sind für globale Rollen noch keine Parameter vorgesehen.

Rollenparameter können verwendet werden, um ein Rechtesystem differenzierter zu gestalten.

3.5 *Fehlermeldungen*

Es gelten die Vorgaben der Spezifikation "Portal Verbund Protokoll", wobei im BPVP eine Gruppe von Fehlermeldungen spezifiziert ist.

3.6 *HTTP-Bindung*

Bei der Verwendung des HTTP Protokolls sind die BPVP Parameter bei jedem Request als HTTP-Parameter zu übergeben.

3.7 *Zertifikate / Sichere Verbindungen*

Für BPVP werden die Definitionen aus PVP übernommen. Es gelten sinngemäß die Definitionen für die Security-Klasse 1. Für die Kommunikation zwi-

sehen Servern sind Zertifikate von beim bm:bwk zertifizierten ZDAs zu verwenden. Das Zertifikat identifiziert den Portalbetreiber.

4 Datenstrukturen

4.1 Rollen, Rollenstrukturen, Anwendungsportale und Applikationen

Diese Datenstrukturen beschreiben die Struktur des Rechtesystems im BPV. Sie werden im Stammportal, im Anwendungsportal um im Bildungsdirectory verwendet.

4.2 Rollenzuordnungen

Hier wird eine Datenstruktur beschrieben, die in Stammportalen und im Bildungsdirectory verwendet wird. Im Bildungsdirectory werden Rollenzuordnungen für Stammportale definiert, um die möglichen Rechte abzubilden. In Stammportalen werden Rollenzuordnungen für Benutzer definiert, um die einem Benutzer zugeordneten Rechte festzulegen.

User (Benutzer)

Mit dieser Entität werden Benutzerdaten gehalten.

Als userId muss eine innerhalb des BPVP eindeutige ID verwendet werden. Es kann eine ID nach dem Muster "<Schulkennzahl>+<Schüler-Stammblattnummer>" oder eine bPK (bereichsspezifische Personen Kennung) verwendet werden.

4.3 Datenstrukturen im Bildungsdirectory des Ministeriums

Im zentralen Bildungsdirectory werden alle Stamm- und Anwendungsportale, alle Applikationen und alle möglichen Rollen und Parameter verwaltet. Das Bildungsdirectory ist somit ein Verzeichnis aller Portale und aller verfügbarer Anwendungen inklusive der Rechtestruktur.

Im Bildungsdirectory werden die Rechte von Stammportalen festgelegt. Die Rechtezuordnungen zu BPVP Benutzern ist nicht Teil des Bildungsdirectories. Diese werden ausschließlich in den Stammportalen verwaltet.

HomePortal (Stammportal)

Ein Stammportal kann für alle Anwendungen eines Anwendungsportals berechtigt werden (durch eine Zuordnung "allowed application portal").

Eine Zuordnung von von Applikationen durch "allowed application" erlaubt mit beliebigen Rechten auf Applikation zuzugreifen.

Eine Zuordnung einer RoleStructure zu einem Stammportal erlaubt den Zugriff unter Verwendung der zugeordneten Rechtestruktur. (allowed role structure)

Sind zu einem Stammportal RoleAssignments definiert darf diese konkrete Rollenzuordnung verwendet werden. ("allowed role assignment")

5 Soap Schnittstelle des Bildungsdirectorys

Anwendungsportale müssen Anfragen von Stammportalen gegen das zentrale Bildungsdirectory des Ministeriums überprüfen. Dazu wird das Ministerium das SOAP Service "ValidatePortalRights" zur Verfügung stellen.

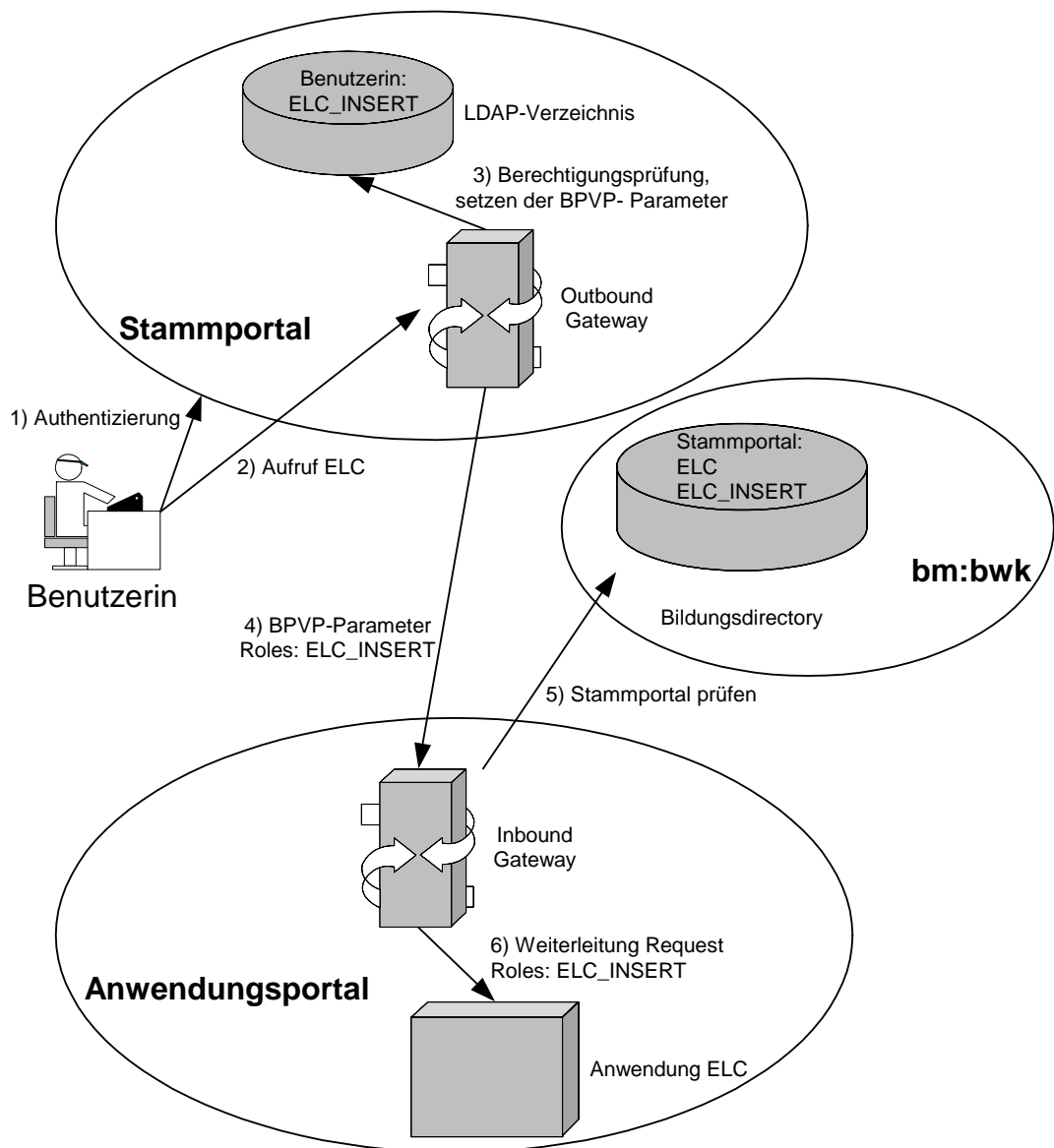
Anwendungsportale sollen die Ergebnisse cachen, wobei sichergestellt werden soll, dass der Cache zumindest alle acht Stunden aktualisiert wird. Es soll möglich sein den, Cache ohne Betriebsunterbrechung zu leeren.

6 Design Rechteverwaltung / Beispiele

6.1 Rechteverwaltung in den Stammportalen

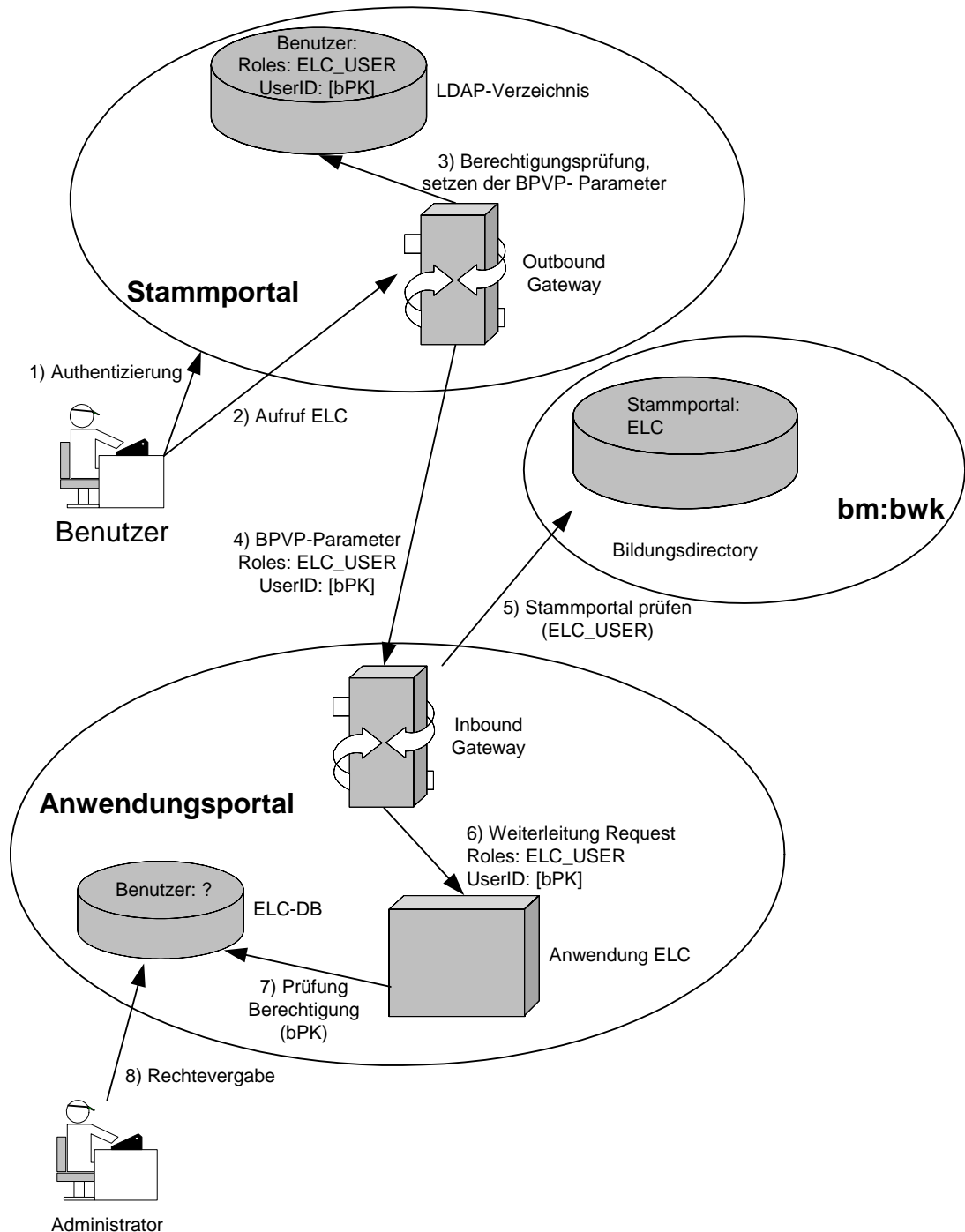
Diese Variante nutzt alle Features des BPV. Benutzerauthentifizierung und Rechteverwaltung werden von den Stammportalen übernommen. Die Anwendung wertet die durch BPVP Parameter übermittelten Benutzer- und Rechteinformationen aus.

Beispielanwendung Brokerage System zum Austausch selbstentwickelter Lehrmaterialien für E-Learning Cluster (ELC-Brokerage System)



6.2 Applikationsinterne Rechteverwaltung / redundante Benutzerdatenverwaltung

Es sind auch Anwendungen denkbar, die nur die BPV Funktion der Benutzerauthentifizierung nutzen und die Rechteverwaltung applikationsspezifisch lösen.



7 Schnittstelle für den Import von Benutzerdaten

Stammportale sollen eine Datenschnittstelle unterstützen, um Benutzerdaten aus den Daten von Schulverwaltungen zu übernehmen.

Es sollen zwei Formate – ein CSV-Format, und ein XML-Format unterstützt werden.

Wenn in einem Stammportal eine bPK als Schlüssel für Benutzer verwendet wird, wird diese ermittelt, bevor ein Report erstellt wird. Wurde die bPK ermittelt werden, scheint diese im Report auf. Traten bei der Bestimmung der bPK Fehler auf, so werden auch diese im Report angezeigt.