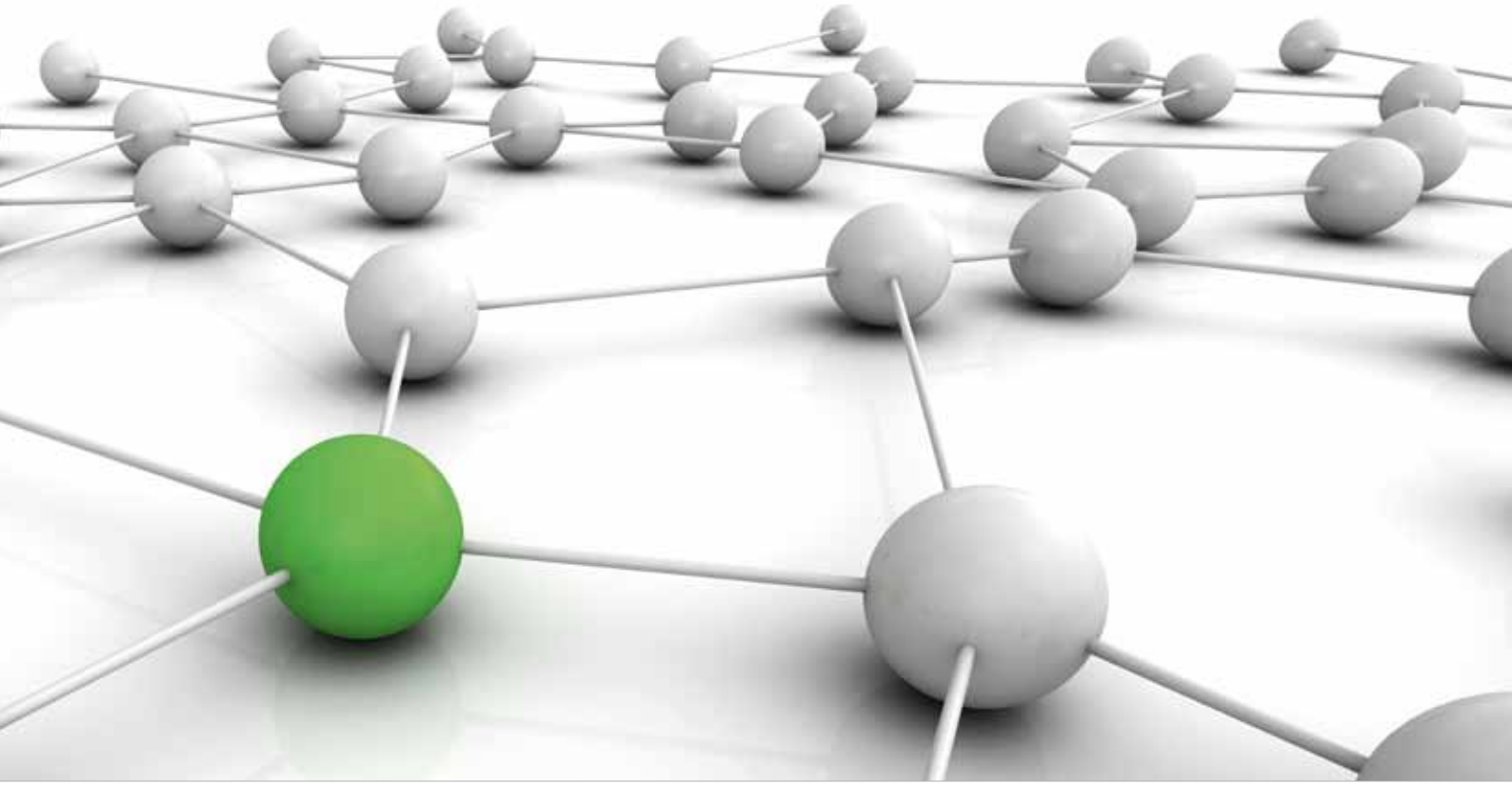
BÜNDNIS FÜR BILDUNG
vernetztes Lernen

REFERENZARCHITEKTUR TEIL 6:

Identitätsmanagement

VERSION 1.0



Bündnis für Bildung e. V.

www.b-f-b.net

Über das Bündnis für Bildung e. V.
Unter dem Dach des Bündnis für Bildung e. V. (BfB) arbeiten Hard- und Software-Hersteller, Entwickler bildungsspezifischer Lösungen, Netzwerk-Spezialisten, Schulbuchverlage sowie Anbieter von Lerninhalten und -medien eng mit Vertretern der Ministerien, Schulträgern sowie Lehrkräften und Eltern zusammen. Das Bündnis für Bildung ist ein gemeinnütziger Verein und finanziert sich ausschließlich über Mitgliedsbeiträge und Spenden.

Weitere Informationen zum BfB finden Sie unter www.b-f-b.net/

REFERENZARCHITEKTUR TEIL 6:

Identitätsmanagement

VERSION 1.0

Einleitung

Bildung ist die wichtigste Investition in die Zukunft unserer Gesellschaft und einer der Schlüsselfaktoren für wirtschaftliches Wachstum. Dabei muss unser föderales Bildungssystem zahlreichen Herausforderungen gerecht werden: Um der vernetzten Informationsgesellschaft Rechnung zu tragen und die nächste Generation optimal auf die beruflichen Herausforderungen der Zukunft vorzubereiten, muss ein nachhaltiges Bildungssystem stets einen Schritt voraus sein.

Das Bündnis für Bildung e. V. (BfB) hat sich zusammengeschlossen, um einen Beitrag für eine zukunftsgewandte Bildung zu leisten und gemeinsam mit allen Stakeholdern im Bildungsbereich offene und produktneutrale Konzepte für eine IT- Bildungsinfrastruktur für das ganzheitliche Lernen von morgen in Deutschland zu erarbeiten – die sogenannte Referenzarchitektur.

Diese besteht derzeit aus den Kapiteln Pädagogik, Infrastrukturmanagement, Zentrale Dienste (Data Services und Schnittstellen), Content Distribution und ID-Management. Das BfB veröffentlicht nun erste Kapitel der Referenzarchitektur, um den Dialog darüber mit den Akteuren und Entscheidern im Bildungsumfeld zu eröffnen und zur weiteren Mitarbeit an diesem Dokument anzuregen. Ziel des BfB ist es, die Referenzarchitektur ständig weiterzuentwickeln und an neue technische Entwicklungen anzupassen.

Das vorliegende Kapitel der Referenzarchitektur „Identitätsmanagement“ liegt nun in der Version 1.0 vor.

Das BfB freut sich auf konstruktive Vorschläge und die Mitarbeit bei der Weiterentwicklung dieses Kapitels.

Inhaltsverzeichnis

Identitätsmanagement

Eine wesentliche Anforderung bei der Kommunikation von Lösungskomponenten der „Referenzarchitektur" ist neben der Prüfung der Zulässigkeit die zweifelsfreie Identifikation und Verifikation der beteiligten Identitäten. Dies gilt insbesondere beim Abgleich und bei der Übermittlung von personenbezogenen Daten zwischen Lösungskomponenten.

1 Zusammenfassung und Überblick

Das Identitätsmanagement (ID-Management) verwaltet mit Hilfe anonymer Identifikatoren (ID) einzelne Individuen (SchülerInnen, Lehrkräfte, Eltern etc.), Institutionen (Bildungseinrichtungen, Schulträger) und Objekte (Anwendungen, Ressourcen) sowie deren Beziehungen untereinander anhand einer festzulegenden Taxonomie des Bildungswesens.

Auf diese Weise wird eine Vermittlungsfunktion zwischen einer zentralen, eindeutigen ID und den korrespondierenden IDs in den jeweiligen Lösungskomponenten etabliert (ID-Mapping). Aus Sicht des ID-Managements existiert eine klare 1:n-Beziehung: Eine eindeutige, zentrale ID bezieht sich auf dieselbe Identität in n Subsystemen.

Die zu einer Identität gehörigen Detail-Daten wie etwa Kundendaten, Schülerstammdaten, Rechnungsdaten etc. verbleiben immer innerhalb der jeweiligen Lösungskomponente, welche die ID bzw. das ID-Mapping angelegt hat. So kann das ID-Management im Ernstfall nicht kompromittiert werden, und geschützte Daten können nicht nach außen gelangen.

Jede Lösungskomponente erhebt daher grundsätzlich die für ihren Zweck notwendigen Daten selbst. Das ID-Management schafft jedoch die Grundlage dafür, dass die Lösungskomponente weitere Daten zu dieser Identität aus einer anderen Lösungskomponente anfordern kann. Das Berechtigungssystem muss in diesen Fällen klären, ob weitere Daten direkt zwischen den Systemen ausgetauscht werden dürfen oder ob hierzu eine manuelle Zustimmung zu erfolgen hat. Hierbei werden zum Zweck des Datenaustausches Vertrauensstellungen zwischen den beteiligten Systemen abgebildet.

IDs werden nach Primär- und Sekundär-IDs unterschieden. Primär-IDs werden durch das jeweils führende System (MDM) generiert. Sekundär-IDs stammen aus den Systemen, zu denen Vertrauensstellungen bestehen.

Auf dieser Basis können zum einen Lösungskomponenten entscheiden, welche Operationen (Daten-Updates) aufgrund definierter Ereignisse durchzuführen sind, und die Zielobjekte in Fremdsystemen über das ID-Management sicher zuordnen.

Zum anderen ist hier ein Berechtigungssystem aufgehängt, welches Zugriffe und Änderungsanfragen von Anwendungen regelt.

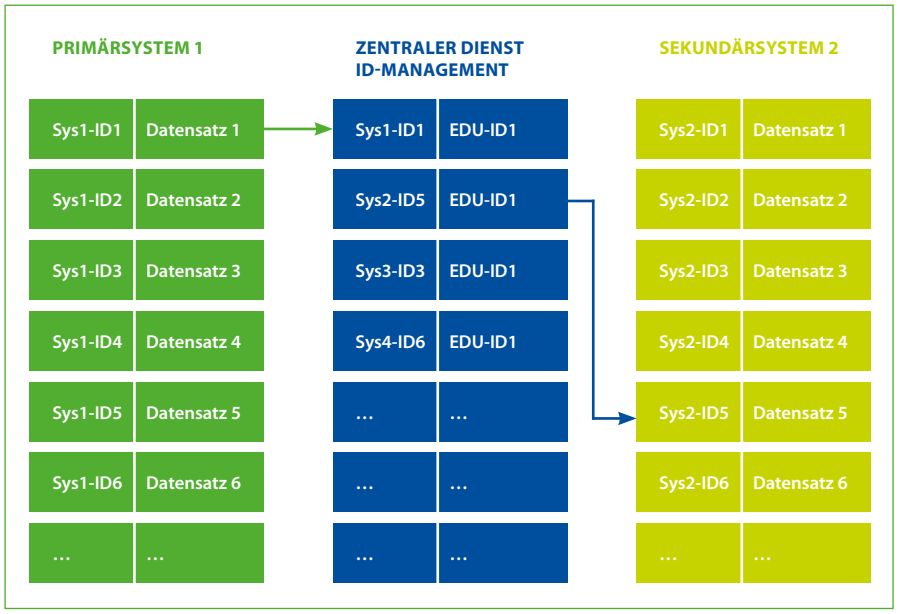


Abb: Vereinfachte Darstellung des ID-Mappings

2 Leistungsbeschreibung

Die Leistungen des ID-Managements sind:

- Verwaltung von IDs für z. B.: Schulaufsicht, Schulträger, Medienzentren, Schulen, Lehrkräfte, SchülerInnen, Eltern, Content-Anbieter, Anwendungen, Dienstanbieter.
- Speicherung von Anschriftsdaten – zu Zwecken der Verifikation und zum Schutz vor Missbrauch – von: Schulaufsicht, Schulträgern, Medienzentren und Schulen. Dabei werden keinerlei personenbezogene Daten von SchülerInnen, Lehrkräften oder anderen Individuen gespeichert! Die Speicherung solcher Informationen obliegt allein den angeschlossenen Systemen, welche die zentralen Dienste in Anspruch nehmen.
- Sicherer Zugriff über Zertifikats-gesicherte Verbindungen für autorisierte Anwendungen (Infrastruktur-Management).
- Zuordnung von Zertifikaten zu Institutionen und Anwendungs-Instanzen für eine gesicherte Kommunikation.
- Mit dem Datenschutz konforme ID-Verwaltung.
- Stellt Taxonomie der verwalteten Objekte (Institutionen, Individuen, Anwendungen, Ressourcen) und ihrer wechselseitigen Beziehungen zur Verfügung.
- Vertrauensstellungen zwischen Lösungskomponenten einer oder verschiedener Institutionen werden durch ID-Mapping erfasst.
- Zur Unterstützung von MDM wird das im Eco-System Schule führende System definiert.Unterstützt auf Basis definierter Vertrauensstellungen SSO zwischen den beteiligten Systemen.
- Standard-Verfahren für SSO wie Federation und Delegation werden transparent unterstützt.
- Standard-ID Systeme und Verfahren wie Live-ID, Office-Online-ID, OpenID, Shibboleth und SAML werden unterstützt.

- Standard-Anmeldeverfahren wie Kerberos, NTLM oder LDAP werden unterstützt.
- Bietet über das ID-Mapping eine zuverlässige Zuordnung zwischen Objekten in einander fremden Teilsystemen und ermöglicht so den sicheren Datenaustausch zwischen Institutionen und Anwendungen über Objekte (Schüler, Lehrer etc.).
- Das ID-Management ist für gesteigerte Sicherheits-Szenarien partitionierbar in Private und Public.
- Enthält Test-Cases für die Entwicklung konformer und zuverlässiger Anwendungen auf Basis des ID-Managements.
- [Bereitstellung eines zentralen, abgesicherten LogonUIs?]
- [Speicherung der Daten nach KDS3 für die Primäre ID von Individuen?]

3 Abhängigkeiten von anderen Diensten

Abhängigkeiten von anderen zentralen Diensten außer den Infrastruktur-Diensten sind zunächst nicht ersichtlich. Eine besondere Herausforderung stellt die Migration bestehender Daten in das ID-Management dar. Hierbei ist eine korrekte Zuordnung von Identitäten aus verschiedenen Quellsystemen sicherzustellen.

4 Anwendungsbeispiele

Das Eco-System einer Schule umfasst neben einem Schulverwaltungsprogramm auch ein AD-basiertes pädagogisches Netzwerk und ein Unterrichts-Portal. Änderungen in der Schulverwaltung als führendes System sollten automatisch im pädagogischen Netz und im Portal nachgeführt werden.

Betrachten wir verschiedene Fälle und deren interne Abwicklung:

Neuaufnahme eines Schülers
Für den Schüler gibt es noch keine Einträge im ID-Management. Die Schulverwaltung legt als führendes System einen neuen Eintrag an. Anschließend werden Netz und Portal über entsprechende Schnittstellen angesteuert, um in diesen Systemen neue Benutzer anzulegen. Übermittelt werden hierbei neben der ID im Ursprungssystem und der ID des Ursprungssystems die benötigten Zusatzinformationen wie Vorname, Nachname, Klasse. Das Format der Daten folgt der Definition in den Data Services. Die Zielsysteme verarbeiten die Anforderung und melden dem ID-Management die angelegten Sekundär-IDs. Hiermit ist eine eindeutige Verknüpfung zwischen dem Schüler in der Schulverwaltung und demselben Individuum im Netz und Portal hergestellt.

SSO
Ein Benutzer hat Sekundär-IDs in verschiedenen Zielsystemen. Er meldet sich an einem dieser Systeme an. In seiner Sitzung wird seine „Edu-ID“ vermerkt. Beim Wechsel zu einem seiner anderen Systeme (Portale, Websites etc.) wird die „Edu-ID“ an dieses gemeldet. Das Zielsystem prüft über das ID-Mapping, ob eine ID im eigenen System vorliegt. Ist dies der Fall, kann der Benutzer ohne erneute Anmeldung die Angebote nutzen, da über das ID-Management eine Vertrauensstellung hergestellt und die Identität im eigenen System zweifelsfrei ermittelt wurde.

5 Priorität / Zeitplanung

Auf dem ID-Mapping und den damit verbundenen Vertrauensstellungen basieren mit Ausnahme der Data Services alle anderen zentralen Dienste. Die Priorität für die Implementierung ist daher sehr hoch!

Impressum

Bündnis für Bildung e. V.
Reinhardtsraße 38, 10117 Berlin

T. +49 30 5 26 87 22 53
F. +49 30 5 26 87 22 60
info@b-f-b.net
www.b-f-b.net

Leiter der Arbeitsgruppe ID-Management:
Victor Baum, RDT Ramcke Datentechnik GmbH

Redaktion:
Anja Janus, Bündnis für Bildung e. V.

Lektorat:
Miriam Buchmann-Alisch, text_transfer

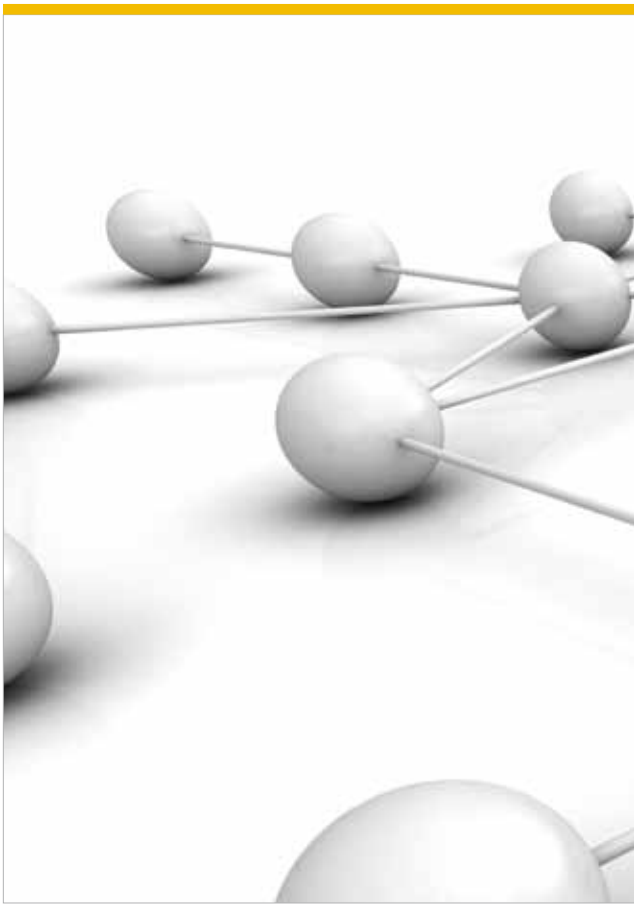
Gestaltung:
Schleuse01 Werbeagentur GmbH, Berlin

Titelfoto:
Fotolia, Parris Cope / fotolia.com

Druck:
LASERLINE Digitales Druckzentrum
Bucec & Co. Berlin KG

Stand:
Februar 2013

BÜNDNIS FÜR BILDUNG
vernetztes Lernen



Bündnis für Bildung e. V.
Reinhardtstraße 38
10117 Berlin

Telefon: +49 30 5 26 87 22 53
E-Mail: info@b-f-b.net

www.b-f-b.net