ISPRAT
Interdisziplinäre Studien zu Politik, Recht, Administration und Technologie e.V.

Fraunhofer FOKUS

Bürgerfreundliches Identitätsmanagement

Rahmenarchitektur und technischer Lösungsvorschlag zur Umsetzung eines bürgerfreundlichen Identitätsmanagements in Verwaltung und Wirtschaft

Studie

Rahmenarchitektur und technischer Lösungsvorschlag zur Umsetzung eines bürgerfreundlichen Identitätsmanagements in Verwaltung und Wirtschaft

Autoren:

Jens Fromm

Petra Hoepner

Dr. Angelika Steinacker

Wolfgang Zwerch

25.08.2009

Inhaltsverzeichnis

ABBILDUNGSVERZEICHNIS 6

TABELLENVERZEICHNIS 7

ZUSAMMENFASSUNG DER ERGEBNISSE 8

1. VISION EINES BÜRGERFREUNDLICHEN IDENTITÄTSMANAGEMENTS 10

2. STRUKTUR DER STUDIE 11

3. ANFORDERUNGEN AN EIN IDENTITÄTSMANAGEMENT AM BEISPIEL DER EU-DIENSTLEISTUNGSRICHTLINIE 12

3.1 Beschreibung der EU-DLR Akteure und Aktivitäten 12

3.2 Anforderungen aus Sicht der Akteure 16

3.2.1 Dienstleistungserbringer (DL) 16
3.2.2 Zuständige Behörde (ZB) 17
3.2.3 Einheitlicher Ansprechpartner (EA) 19

3.3 Fazit 21

4. PROZESS- UND INFORMATIONSMODELL 22

4.1 Prozessmodell 22

4.1.1 Dienstanbieter vertraut dem Anwender 22
4.1.2 Attribut-Zertifizierer vertraut dem Anwender und Dienstanbieter vertraut dem Attribut-Zertifizierer 22
4.1.3 Attribut-Zertifizierer1 vertraut dem Anwender und Dienstanbieter vertraut dem Attribut-Zertifizierer2 23
4.1.4 Initiales Vertrauensverhältnis 24
4.1.5 Informationsmodell 25

4.2 Fazit 29

5. RAHMENARCHITEKTUR 30

5.1 Identity Attribute Data Repository 31

5.1.1 Event Service 32
5.1.2 Attribute Certification Service 33
5.1.3 Authentication Service 35
5.1.4 Workflow Service 36
5.1.5 Provisioning Service 36

5.2 Reporting Data Repository 37

5.2.1 Reporting Service 38
5.2.2 Logging Service 38
5.2.3 Monitoring Service 39

5.3 Authorization Data Repository 40

5.3.1 AACS Management Service 40

5.3.2 Policy Management Service 41
5.4 Fazit 42

6. IDENTITÄTSMANAGEMENT - UNTERNEHMENSZENTRIERT VERSUS ANWENDERZENTRIERT 44

6.1 Administration 45
6.1.1 Registrierung neuer Digitaler Identitäten 45
6.1.2 Veränderung von Attributen einer Digitalen Identität 47
6.1.3 Deaktivierung bestehender Identitäten 49

6.2 Autorisierung 50
6.2.1 Verwalten der anwendungsbezogenen Berechtigungsstrukturen 50
6.2.2 Verwalten der unternehmensweiten Rollen und Regeln 51

6.3 Authentifikation 52
6.3.1 Erzeugen der Nachweise 52
6.3.2 Zurücksetzen der Nachweise 53
6.3.3 Synchronisieren der Nachweise 54
6.3.4 Entziehen der Nachweise 55

6.4 Audit 56
6.4.1 Überprüfen der Identitäten und Berechtigungen 56
6.4.2 Überprüfen der unternehmensweiten Rollen und Regeln 57
6.4.3 Überprüfen der anwendungsbezogenen Berechtigungsstrukturen 58
6.4.4 Überprüfen der Metriken 58

6.5 Fazit 59

7. DAS MODELL AM BEISPIEL DER EU-DIENSTLEISTUNGSRICHTLINIE (EU-DLR) 61

7.1 Elektronische Identitätsdokumente 61
7.1.1 Personenkennzeichen/ -kennziffern 61
7.1.2 eIDs in Deutschland 62
7.1.3 eIDs in Europa 64
7.1.4 European Citizen Card 64
7.1.5 Authentifizierung im grenzüberschreitenden europäischen Kontext 64
7.1.6 eIDs und Authentifizierung in Bezug zur Rahmenarchitektur 68

7.2 Komponenten und Dienste 69
7.2.1 Elektronischer Safe (eSafe) 69
7.2.2 Datennotar 72
7.2.3 Elektronische Originaldokumente 73
7.2.4 Elektronische Beglaubigung 74
7.2.5 Elektronische Vollmachten 75
7.2.6 Langzeitarchivierung 76
7.2.7 Fallmanagement 77
7.2.8 Fallakte 79
7.2.9 Rechtsverbindliche Kommunikation 80

7.3 Vertrauens- und Sicherheitsdienste 80

7.4 Fazit 83

8. INITIATIVEN UND ENTWICKLUNGEN 84

8.1 Beschreibung von Initiativen 84

8.1.1 Liberty Alliance 84
8.1.2 Information Card Foundation 84
8.1.3 OSIS 85
8.2 Beschreibung von Standards, Entwicklungen und Produkten 85
8.2.1 Elektronischer Personalausweis 85
8.2.2 eCard-API 86
8.2.3 Bürgerportal 87
8.2.4 S.A.F.E. 88
8.2.5 SAML 89
8.2.6 Nutzerzentrierte Entwicklungen 90
8.2.7 Produkte für Identitätsmanagement 91
8.3 Fazit 91

9. AUSBLICK 92
9.1 Federation 92
9.2 Service-Oriented Architecture 93
9.3 Identity Management und »The Cloud« 94

10. LITERATURVERZEICHNIS 96

11. ANHANG 98
11.1 Abkürzungsverzeichnis 98
11.2 Glossar 99

Abbildungsverzeichnis

Abbildung 1: EU-DLR-spezifische Akteure und ihre Aktivitäten (Quelle: (von Lucke, J., Eckert, K.-P., Breitenstrom, C., 2008)) 15

Abbildung 2: Prozess »Zugriff auf einen Dienst erlangen« (1) 22

Abbildung 3: Prozess »Zugriff auf einen Dienst erlangen« (2) 23

Abbildung 4: Prozess »Zugriff auf einen Dienst erlangen« (3) 24

Abbildung 5: Definition von Vertrauen (nach (Lahno, 2008)) 25

Abbildung 6: Informationsmodell 26

Abbildung 7: Rahmenarchitektur 30

Abbildung 8: Funktionen des Identitätsmanagements 44

Abbildung 9: Prozesslandkarte (Quelle: CSC) 45

Abbildung 10: STORK Mapping der Qualitätslevel (Quelle: (STORK project D2.3, 2009)) 67

Abbildung 11: Beschreibung eines elektronische Safes (Quelle: (Breitenstrom, et al., 2008)) 70

Abbildung 12: Technische Komponenten eines elektronischen Safes (Quelle: (Breitenstrom, et al., 2008)) 71

Abbildung 13: Definition Security Governance und Compliance (Quelle: (BITKOM Arbeitskreis SOA Security)) 81

Abbildung 14: Funktionen des elektronischen Personalausweises (Quelle: Bundesministerium des Inneren) 86

Abbildung 15: SAML Konzepte (Quelle: SAML 2.0 Technical Overview) 89

Abbildung 16: Definition von Cloud Computing nach (Armbrust, 2009) 94

Tabellenverzeichnis

Tabelle 1: Übersicht der Akteure im Szenario Dienstleistungsrichtlinie 15
Tabelle 2: Anforderungen des Dienstleistungserbringers..... 17
Tabelle 3: Anforderungen der Zuständigen Behörde 18
Tabelle 4: Anforderungsprofil für Typen des Einheitlichen Ansprechpartners..... 20
Tabelle 5: Anforderungen des Einheitlichen Ansprechpartners 21
Tabelle 6: STORK QAA Level 66
Tabelle 7: Analogie SOA und Lego-Steine (nach (Mezler-Andelberg, 2008))..... 94

Zusammenfassung der Ergebnisse

Ob Bürger, Kunde, Reisender – immer mehr Identitätsdaten werden in elektronischen Prozessen benötigt. Als Online-Bankkunde, bei der Nutzung von Online-Bürgerdiensten, beim Einkauf im Internet – bislang werden diese Prozesse und die zu übergebenden personenbezogenen Information vom Anbieter der angebotenen Dienste gesteuert und vorgegeben. In der realen Welt und im täglichen Umgang mit Anderen besitzen wir verschiedene Eigenschaften (Attribute), die wir selektiv preisgeben. Die Kernaufgabe des Identitätsmanagements ist es, die Attribute der „Digitalen Identität“ vertrauenswürdig zu erzeugen und während ihrer Lebensdauer auch vertrauenswürdig zu verwalten.

Die Studie führt die Vision eines bürgerfreundlichen Identitätsmanagements in der Zukunft ein. Diese Vision spezifiziert die Anforderungen an das Identitätsmanagements auf abstraktem Niveau. Anhand der EU-Dienstleistungsrichtlinie (Richtlinie 2006/123/EG) (EU-DLR) wird die Vision im konkreten Beispiel analysiert, um die Anforderungen zu präzisieren. Die EU-DLR wurde ausgewählt, da sowohl die elektronischen Identitäten verschiedener Akteure im grenzüberschreitenden Kontext als auch die übermittelten elektronischen Dokumente verifiziert werden müssen und daher das in der vorliegenden Studie entwickelte Modell sehr gut validiert werden kann.

Basierend auf den Anforderungen aus der Vision wird ein generisches Prozess- und Informationsmodell für Identitätsmanagement entworfen, in dem die Prozesse beschrieben werden, in denen die Digitale Identität eines Anwenders und deren Attribute Verwendung finden. Der wesentliche Prozess dabei ist »Zugriff auf einen Dienst erlangen«. Im Informationsmodell wird dargestellt, welche Elemente, genannt Entitäten, in einem bürgerfreundlichen Identitätsmanagement interagieren bzw. in den Prozessen verwendet werden. Dabei werden drei Akteure für ein bürgerfreundliches Identitätsmanagement identifiziert: (1) der Bürger / Anwender, (2) der Dienstanbieter und (3) der Attribut-Zertifizierer. Der Attribut-Zertifizierer ist dabei eine Entität, die die Attribute anderer Entitäten vertrauenswürdig bereitstellen und/oder verifizieren kann.

In der Rahmenarchitektur werden die logischen Komponenten und Dienste für Identitätsmanagement für jeden der Akteure dargestellt. Es wird aufgezeigt, welche Komponenten grundsätzlich erforderlich sind und welchen Funktionsumfang diese besitzen müssen, um ein bürgerfreundliches Identitätsmanagement vollständig umzusetzen. Dabei kann eine technische Implementierung alle Komponenten oder nur ein Teil der aufgezeigten Funktionen und Leistungen bereitstellen. Die Prozesslandkarte stellt die erforderlichen Prozesse für ein Identitätsmanagement aus der Sicht eines Unternehmens und aus der Sicht eines Bürgers dar und umfasst die vier Funktionen: Administration, Authentifikation, Autorisierung und Audit. Jede der vier Funktionen wird analysiert, um die unterschiedlichen Anforderungen und Prioritäten eines Unternehmens und eines Anwenders / Bürgers an ein Identitätsmanagement zu verdeutlichen. Anhand der EU-DLR wird die Rahmenarchitektur auf ein konkretes Beispiel angewendet.

Basierend auf der Rahmenarchitektur und dem Prozessmodell wird eine Auswahl relevanter Initiativen und Entwicklungen, wie z.B. der elektronische Personalausweis, das eCard-API und Information Cards untersucht und dargestellt.

Abschließend werden zukünftige Entwicklungen und Potentiale aufgezeigt, die sowohl personenbezogene als auch objektspezifische Identitäten einbinden, wie z.B. SOA-Security und Cloud-Entwicklungen.

In dieser Studie konnten die wesentlichen Elemente eines bürgerfreundlichen Identitätsmanagements hergeleitet werden. Zu diesen gehört als Entität vor allem der Attribut-Zertifizierer, der zwischen sich nicht vertrauenden Entitäten Vertrauen schaffen soll. Des Weiteren konnten als wesentliche Dienste damit einhergehend der Attribute Certification Service und der Authentication Service identifiziert werden. Weitere Module wurden entwickelt, um den Anforderungen der Bürger gerecht zu werden.

Es wurde gezeigt, dass existierende Initiativen und Entwicklungen immer nur Teilbereiche notwendiger Dienste anbieten, sodass hier durchaus Potential für weitere Entwicklungen zu sehen ist.

1. Vision eines bürgerfreundlichen Identitätsmanagements

Im Folgenden wird die Vision, also die Vorstellung eines bürgerfreundlichen Identitätsmanagements in der Zukunft, beschrieben. In wieweit sich diese Vision realisieren lässt, wird in den nachfolgenden Kapiteln untersucht.

In der Vision eines bürgerfreundlichen Identitätsmanagements hat jeder Bürger eine Digitale Identität mit verschiedenen Attributen, die er nutzen kann, um Interaktionen in der digitalen Welt durchzuführen, z.B. Dienste eines Dienstanbieters in Anspruch zu nehmen.

Der Bürger ist Eigentümer seiner Digitalen Identität und Besitzer der dazu gehörenden Attribute. Er kann frei entscheiden, wem er welche Attribute aus seiner Digitalen Identität für wie lange überlässt und hat das Vertrauen, dass der Empfänger dieser Informationen, z.B. der Dienstanbieter, authentisch und vertrauenswürdig ist.

Der Bürger kann den weiteren Fluss der eigenen Informationen – auch über mehrere Instanzen hinweg – steuern. Es ist dem Bürger möglich, die weitergegebenen Informationen verlässlich und nachweisbar wieder zurückzuholen. Ihm wird jederzeit genaue Auskunft darüber erteilt, welche Aktivitäten der Empfänger mit den Informationen durchgeführt hat.

Jeder Dienstanbieter fordert einen Satz an Attributen, damit ein Anwender seinen Dienst nutzen darf. Der Bürger kann entscheiden, ob er Attribute seiner Digitalen Identität bei Transaktionen in der Digitalen Welt den jeweiligen Partnern präsentiert. Die Partner haben Vertrauen in die präsentierten Attribute und können deren Integrität und Authentizität leicht überprüfen.

Ist es für die Transaktion nicht notwendig, einen Bezug zur realen Person – dem Besitzer der Digitalen Identität – herzustellen, so kann der Bürger die Attribute in einer Form präsentieren, dass diese keinen Rückschluss auf seine reale Identität erlauben, aber dennoch die Integrität und Authentizität der Attribute von den Partnern verifizierbar sind.

Die Nutzung seiner Digitalen Identität und die Auswahl der passenden Attribute für die jeweilige Transaktion und den entsprechenden Partner sind für den Bürger einfach möglich und erfordern keine tiefgreifenden technischen Kenntnisse.

Für die Nutzung der Digitalen Identität entstehen keine wesentlichen zusätzlichen Kosten, die über diejenigen einer Standardausstattung an Hard- und Software hinausgehen. Die Nutzung der Digitalen Identität ist an verschiedenen Orten und zu allen Zeiten, auch über Ländergrenzen hinweg, möglich.

2. Struktur der Studie

Kapitel 1 führt die Vision eine bürgerfreundlichen Identitätsmanagements in der Zukunft ein. Diese Vision spezifiziert die Anforderungen an das Identitätsmanagements auf abstraktem Niveau.

Kapitel 2 (dieses Kapitel) erläutert den Aufbau der Studie und den Inhalt der Kapitel.

Kapitel 3 erläutert die Vision eines bürgerfreundlichen Identitätsmanagement anhand eines konkreten Beispiels. Das Beispiel ist die Europäische Dienstleistungsrichtlinie. Als grenzüberschreitender Dienst, der sowohl Digitale Identitäten als auch elektronische Dokumente einbindet, konkretisiert dieses Kapitel die allgemeinen Anforderungen aus Kapitel 1.

Kapitel 4 definiert das Prozess- und Informationsmodell für ein bürgerfreundliches Identitätsmanagement. Basierend auf den Anforderungen aus der Vision wird ein generisches Prozess- und Informationsmodell für Identitätsmanagement entworfen. Es werden die Prozesse beschrieben, in denen die Digitale Identität eines Anwenders und deren Attribute Verwendung finden.

Kapitel 5 stellt die Rahmenarchitektur für das Identitätsmanagement vor. Die Rahmenarchitektur umfasst die logischen Komponenten und Dienste für Identitätsmanagement für Bürger, Dienstanbieter und Attribut-Zertifizierer. Es wird aufgezeigt, welche Komponenten grundsätzlich erforderlich sind und welchen Funktionsumfang diese besitzen müssen, um ein bürgerfreundliches Identitätsmanagement vollständig umzusetzen.

Kapitel 6 stellt die erforderlichen Prozesse für ein Identitätsmanagement aus der Sicht eines Unternehmens und aus der Sicht eines Bürgers dar und umfasst die vier Funktionen: Administration, Authentifikation, Autorisierung und Audit.

Kapitel 7 erläutert die Rahmenarchitektur und das Prozessmodell anhand der Europäischen Dienstleistungsrichtlinie. Um die Anforderungen aus Kapitel 3 zu erfüllen, werden Komponenten und Dienste eingeführt, die als „Bausteine“ für ein umfassendes Identitäts- und Sicherheitsmanagement für verschiedene bürgerfreundliche Anwendungen in Wirtschaft und Verwaltung dienen können.

Kapitel 8 ordnet eine Auswahl relevanter Initiativen und Entwicklungen in die Rahmenarchitektur und das Prozessmodell ein.

Kapitel 9 gibt einen Ausblick auf zukünftige Entwicklungen und weitere Aspekte des Identitätsmanagements.

Im Anhang werden relevante Begriffe aus dem Identitätsmanagement im Glossar kurz erläutert.

3. Anforderungen an ein Identitätsmanagement am Beispiel der EU-Dienstleistungsrichtlinie

Die im Dezember 2006 verabschiedete EU-Dienstleistungsrichtlinie (Richtlinie 2006/123/EG) (EU-DLR, 2006) soll den Zugang zum Dienstleistungsmarkt in allen Mitgliedstaaten der Europäischen Union vereinfachen, bestehende bürokratische Hindernisse für Dienstleistungserbringer[1] abbauen und so die grenzüberschreitende Erbringung von Dienstleistungen in Europa fördern (Europäische Kommission, 2007). Bis Dezember 2009 muss die Richtlinie in allen EU-Staaten in nationales Recht überführt werden. Behörden aller Verwaltungsebenen müssen zudem dafür sorgen, dass die von der EU-Dienstleistungsrichtlinie betroffenen Verwaltungsverfahren elektronisch abgewickelt werden können.

Mit der Einrichtung „Einheitlicher Ansprechpartner (EA)“ (point of single contact), sollen die Mitgliedstaaten bis Ende 2009 sicherstellen, dass Dienstleistungserbringer alle Verfahren und Formalitäten rund um die Aufnahme und die Ausübung von Dienstleistungstätigkeiten über eine einzige Anlaufstelle abwickeln können. EAs sollen Grundinformationen verständlich aufbereiten, Koordinationsaufgaben für Entgegennahme und Weiterleitung der Verfahrenskorrespondenz übernehmen und Änderungsmitteilungen und genehmigungsrelevante Pflichtmeldungen entgegen nehmen (Bund-Länder-Ausschuss Dienstleistungswirtschaft, 2007).

Wenig Beachtung wurde bisher den sicherheits- und datenschutzrelevanten Prozessen geschenkt, die für eine elektronische Abwicklung von Verwaltungsprozessen, der Übergabe und Überprüfung von Personalien und Dokumenten sowie der revisionssicheren Aufbewahrung und Nachverfolgung von Vorgängen unabdingbar sind. Sind diese Prozesse schon im nationalen Kontext nicht vollständig spezifiziert, so sind bezüglich des grenzüberscheitenden Aspekts der EU-DLR zusätzliche Anforderungen zu erwarten.

3.1 Beschreibung der EU-DLR Akteure und Aktivitäten

Eine wesentliche Voraussetzung für den operationalen Betrieb der EU-DLR in der IT-Infrastruktur eines Landes ist die Etablierung von Vertrauensverhältnissen zwischen den beteiligten Akteuren. Dies erfolgt nicht nur durch die technische Realisierung, sondern auch durch nicht-technische Vereinbarungen.

Die beteiligten Akteure für die Umsetzung der EU-DLR werden in Tabelle 1 vorgestellt, dabei werden die EU-DLR-spezifischen Akteure auf die allgemeinen Akteure im Identitätsmanagement (siehe Kapitel 4) abgebildet.

Abkürzung	EU-DLR Akteur	Allgemeiner Akteur
DL	**Dienstleistungserbringer** Dienstleistungserbringer sind die Benutzer einer DLR-Infrastruktur, also Bürger (Freiberufler) und	Nutzer (Bürger und Unternehmen)

[1] Dienstleistungserbringer sind die Bürger (Freiberufler) und Unternehmen, die Dienstleistungen in einem Mitgliedstaat der Europäischen Union erbringen wollen. In Kontext der Studie sind Dienstleistungserbringer die *Nutzer* von angebotenen Diensten der Dienstanbieter.

<table>
<tr><th>Abkürzung</th><th>EU-DLR Akteur</th><th>Allgemeiner Akteur</th></tr>
<tr><td></td><td>Unternehmen, die Dienstleistungen in einem Mitgliedstaat der Europäischen Union erbringen wollen.
Der Begriff des Dienstleistungserbringers umfasst, abgesehen von einigen Ausnahmen, jede selbstständige, regelmäßig entgeltliche Tätigkeit, insbesondere gewerbliche, kaufmännische, handwerkliche und freiberufliche Tätigkeiten. Für den DL kann auch ein Bevollmächtigter, z.B. ein Rechtsanwalt, Steuerberater oder Notar, tätig werden, der im Namen des Antragstellers handelt.</td><td></td></tr>
<tr><td>EA</td><td>Einheitlicher Ansprechpartner
Der Einheitliche Ansprechpartner ist eine Anlaufstelle, über die Dienstleistungserbringer alle Verfahren und Formalitäten rund um die Aufnahme und die Ausübung von Dienstleistungstätigkeiten abwickeln können. Das Aufgabenspektrum eines EAs ist über die EU-DLR vorgegeben. EAs sollen Dienstleistungserbringer bei Verfahren und Formalitäten rund um die Aufnahme und die Ausübung von Dienstleistungstätigkeiten in einem anderen Mitgliedstaat unterstützen, indem sie Grundinformationen bereitstellen, Koordinationsaufgaben übernehmen, sowie Verfahrenskorrespondenz, Änderungsmitteilungen und genehmigungsrelevante Pflichtmeldungen entgegen nehmen und weiterleiten. Die EU-DLR legt zwar die Grundfunktionen eines EAs fest, bei der Umsetzung steht es den EU-Mitgliedstaaten aber frei, den einheitlichen Ansprechpartnern weitere Aufgaben zu übertragen. Im ISPRAT-Projekt EU-Dienstleistungsrichtlinie (von Lucke, J., Eckert, K.-P., Breitenstrom, C., 2008) wurde daher eine Typisierung der funktionalen Ausprägung von EAs eingeführt:

<table>
<tr><td>Bote</td><td>Reine Botentätigkeit, kein Einblick in die Inhalte.
Boten nehmen lediglich Nachrichten entgegen und leiten diese ungelesen an die Zuständigen Behörden weiter.</td></tr>
<tr><td>Berater</td><td>Funktionalität eines Boten plus allgemeine (nicht personalisierte) Auskunfts- und Beratungsdienste.</td></tr>
<tr><td>Lotse</td><td>Funktionalität eines Beraters plus personalisierte Auskunfts- und</td></tr>
</table>
</td><td>Dienstanbieter</td></tr>
</table>

Abkürzung	EU-DLR Akteur		Allgemeiner Akteur
		Beratungsdienste, jedoch ohne Vollmacht. Als Lotse erhält der EA Einblick in das Anliegen und die damit einzureichenden Unterlagen. Da ein Lotse keine „Vollmacht“ des Dienstleistungserbringers besitzt, kann er nicht in dessen Auftrag handeln.	
	Mittler	Funktionalität eines Lotsen plus Vollmacht für einfache Entscheidungen. Als Mittler kann ein EA direkt mit den zuständigen Behörden kommunizieren und vermitteln. Dabei verfügt er auch über eine Vollmacht für Routinefälle, so dass er bei einfachen Entscheidungen im Sinne des Dienstleistungserbringers selbständig tätig werden kann. Vor allem soll er aber koordinieren, Fristen überwachen, auf eine ordnungsgemäße und zügige Bearbeitung hinwirken, Statusauskünfte geben und eine Akteneinsicht ermöglichen. Um ein solches Portfolio zu gewährleisten, muss auch ein Fallmanagement durchgeführt werden, d.h. die verschiedenen Verwaltungsvorgänge müssen koordiniert, überwacht und administriert werden.	
	Verfahrensmanager	Funktionalität eines Mittlers plus umfassende Vollmacht. Als Verfahrensmanager ist ein EA mit einer umfassenden Vollmacht für den Dienstleistungserbringer tätig. Er übernimmt dann nicht nur die Boten- und Beratungsdienste, sondern verwaltet das Gesamtvorhaben, kümmert sich um die Kommunikation mit den zuständigen Behörden und trifft gegebenenfalls Entscheidungen im Sinne seines Auftraggebers.	

Abkürzung	EU-DLR Akteur		Allgemeiner Akteur
	Super-behörde	Bündelung aller Zuständigkeiten in neuer Behörde. Für eine Superbehörde müssten alle Aufgaben und Zuständigkeiten rund um die Erbringung von Dienstleistungen in einer Behörde gebündelt werden.	
ZB	**Zuständige Behörden** Zuständige Behörden (ZB) sind die sachlich und örtlich zuständigen Behörden oder Stellen bezüglich des zu bearbeitenden Antrags oder Falles. Die ZBs beraten, nehmen Anträge entgegen, bearbeiten die Anträge und erbringen Verwaltungsleistungen. Gemäß EU-DLR dürfen die DLs sich mit ihrem Anliegen auch weiterhin an die ZB direkt wenden, ohne dass ein EA einbezogen werden muss.		Dienstanbieter

Tabelle 1: Übersicht der Akteure im Szenario Dienstleistungsrichtlinie

Die allgemeinen Aktivitäten, die von den beteiligten Akteuren ausgeführt werden, sind in Abbildung 1 dargestellt.

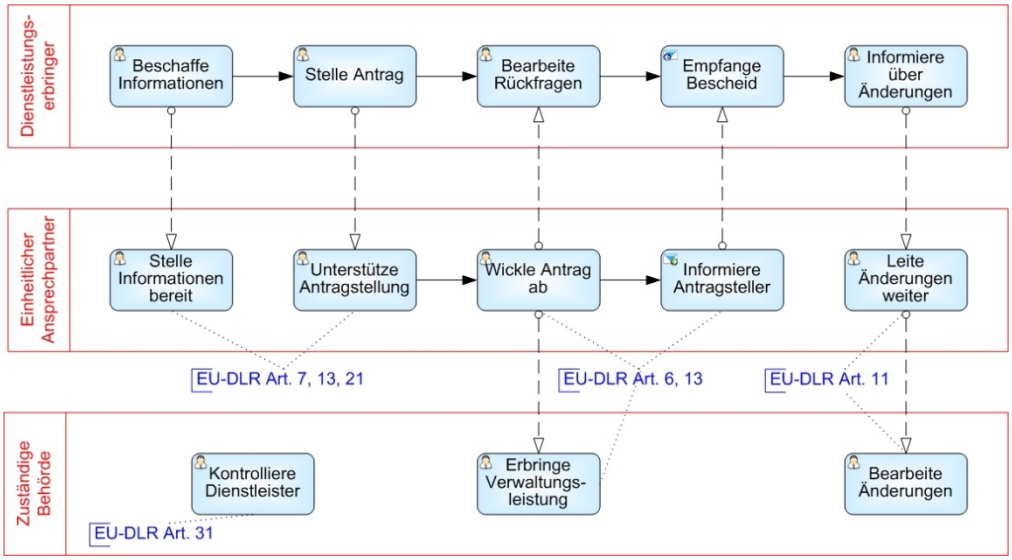


Abbildung 1: EU-DLR-spezifische Akteure und ihre Aktivitäten (Quelle: (von Lucke, J., Eckert, K.-P., Breitenstrom, C., 2008))

3.2 Anforderungen aus Sicht der Akteure

Im DLR-Kontext kommunizieren die beteiligten Akteure in einem grenzüberschreitenden Verbund. Aus Sicht der Akteure werden in diesem Abschnitt die Anforderungen hinsichtlich des Identitätsmanagements, des Datenschutzes und der Datensicherheit betrachtet, die eine notwendige Voraussetzung darstellen, um das Vertrauensverhältnis zwischen den Akteuren zu etablieren.

3.2.1 Dienstleistungserbringer (DL)

Nr.	Anforderungen
DL-A1	**Verwendung der nationalen elektronischen Identitätsnachweise** Identitätsattribute und –nachweise von natürlichen und juristischen Personen können sich national unterscheiden. Will ein DL in einem Mitgliedstaat eine Dienstleistung erbringen und diese per EU-DLR Infrastruktur beantragen, so sollte der DL seine nationalen elektronischen Identitätsnachweise verwenden können. Es sollte nicht erforderlich sein, sich in jedem Mitgliedstaat gesondert für die Nutzung der EU-DLR-Infrastruktur zu registrieren. Generell ist davon auszugehen, dass nationale eIDs in den verschiedenen Mitgliedstaaten bereits vorhanden sind oder zukünftig eingeführt werden. Diese werden in verschiedenen Kontexten für die Nutzung von elektronischen Diensten verwendet und sollten daher auch für DLR eingesetzt werden können.
DL-A2	**Keine mehrfache Authentifizierung** Für die grenzüberschreitende Authentifizierung existieren zwei Möglichkeiten: (1) DL authentifiziert sich lokal bei einer nationalen Instanz; diese generiert Authentifizierungsnachweise. Die Authentifizierungs-nachweise werden vom EA oder ZB im Zielland anerkannt. (2) DL authentifiziert sich direkt im Zielland bei EA oder ZB. Die Authentifizierung sollte für einen DLR-Vorgang nicht unnötigerweise mehrfach erfolgen, d.h. Single Sign-On sollte basierend auf der nachgewiesenen Identität erfolgen.
DL-A3	**Gegenseitige Authentifizierung** Kommunizieren DL, EA bzw. ZB, so müssen die Kommunikationspartner authentisch sein, d.h. eine gegenseitige Authentifizierung muss erfolgen, damit die Akteure sicher sein können, dass sie mit dem gewünschten Kommunikationspartner kommunizieren. Dies ist insbesondere erforderlich, da auch vertrauliche Daten übermittelt werden.
DL-A4	**Schutz vertraulicher Daten und Datenminimierung** Vertrauliche Daten dürfen nur Behörden zugänglich sein, die diese für die Verfahrensabwicklung benötigen. In einem komplexen DLR-Verfahren werden vertrauliche Daten an verschiedene beteiligte Behörden übermittelt. Diese Daten umfassen die Identitätsdaten von Personen bzw. Firmen, sowie alle weiteren Daten, die für die Aufnahme oder die Ausübung einer Dienstleistung notwendig sind. Da dies auch den Austausch von Informationen über die Zuverlässigkeit von

Nr.	Anforderungen
	Dienstleistungserbringern umfasst, können vertrauliche Informationen über strafrechtliche Sanktionen und Disziplinar- und Verwaltungsmaßnahmen von den zuständigen Behörden angefordert werden. Die vertraulichen Daten sind vor unbefugter Einsicht zu schützen.
DL-A5	**Schutz vor Modifikation der Daten** Die übermittelten Daten und Informationen im DLR-Verbund müssen vor unrechtmäßiger Modifikation geschützt werden.
DL-A6	**Vollmachten müssen erteilt werden können** Um die zügige Abwicklung des DLR-Verfahrens zu unterstützen, kann es erforderlich sein, dass Handlungsvollmachten vom DL an einen externen Bevollmächtigen oder den EA erteilt werden. Umfang und technische Realisierung einer Handlungsvollmacht sind durch EU-DLR nicht festgelegt. Erteilt der DL eine Handlungsvollmacht, dann erhält der Bevollmächtigte bestimmte Rechte (Attribute) vom DL. Die Gültigkeit und Rechtmäßigkeit der Handlungsvollmacht muss nachvollziehbar und überprüfbar sein.
DL-A7	**Rechtssichere Aufbewahrung von elektronischen Dokumenten** In elektronischen Verfahren wie DLR müssen Daten (inkl. Identitätsdaten und –nachweise) und Dokumente sicher empfangen und aufbewahrt werden, sowie einfach in den Fachverfahren verwendet werden können. Der Zugriff auf diese Dokumente darf nur durch den Nutzer selbst ausgeführt bzw. durch ihn veranlasst werden. Da elektronische Bescheide bestimmten Aufbewahrungsfristen unterliegen, kann auch eine Langzeit-aufbewahrung erforderlich sein.
DL-A8	**Gültigkeit von elektronischen Originaldokumenten** Für die Aufnahme oder die Ausübung einer Dienstleistung sind elektronische Originaldokumente dem Verfahrensantrag beizufügen. Diese Dokumente werden unter anderem für die Vergabe von Attributen benötigt, z.B. die berufsrechtliche Zulassung. Aus diesem Grund müssen diese Originaldokumente in anderen Mitgliedstaaten als gültig akzeptiert werden können, ohne dass der DL diese vorab übersetzen oder gesondert anerkennen lassen muss.

Tabelle 2: Anforderungen des Dienstleistungserbringers

3.2.2 Zuständige Behörde (ZB)

Die Zuständige Behörde muss nicht durch eine einzelne Behörde bzw. deren Mitarbeiter repräsentiert werden. Die zuständige Behörde kann durch einen Verbund interagierender Behörden je nach beantragter Dienstleistung vertreten werden. Hier ist zu beachten, dass jede Behörde über eigene Richtlinien, Verfahren und technische Infrastrukturen verfügen kann. Die Zuständige Behörde ist daher ihrerseits ein organisatorischer und technischer Verbund, d.h. ein verteiltes System, mit den entsprechenden Anforderungen an Interoperabilität aus organisatorischer, semantischer und technischer Sicht. Die Zuständige Behörde bearbeitet DLR-Vorgänge, die hier auch als „Fälle“ bezeichnet werden.

Nr.	Anforderungen
ZB-A1	**Registrierung und Authentifizierung der Mitarbeiter** Die Registrierung und Authentifizierung der Mitarbeiter gegenüber den behördeninternen Systemen obliegt der jeweiligen Behörde. Um die Berechtigungen der einzelnen Mitarbeiter zu verwalten, können diesen bestimmte Rollen zugeordnet werden.
ZB-A2	**Gegenseitige Authentifizierung** Die Kommunikationspartner (EA, DL) müssen authentisch sein, d.h. eine gegenseitige Authentifizierung muss erfolgen, damit die ZB sicher sein kann, dass sie mit den gewünschten Kommunikationspartnern kommuniziert. In direktem Kontakt muss die ZB auch die grenzüberschreitende Authentifizierung des DL ermöglichen.
ZB-A3	**Autorisierter Zugriff auf alle erforderlichen Verfahrensdaten** Der zuständige Mitarbeiter muss Zugriff auf alle erforderlichen Daten und Dokumente des Falles/Verfahrens haben. Liegen die Daten nicht lokal vor, so muss auch ein entfernter Zugriff möglich sein.
ZB-A4	**Überprüfung von Daten und Dokumenten des DLs auf Echtheit und Gültigkeit** Die vom DL übermittelten elektronischen Dokumente müssen hinsichtlich ihrer Echtheit und Gültigkeit überprüft werden können. Dies kann eine grenzüberschreitende Kommunikation mit den Behörden des Ursprungslands erfordern, z.B. mittels IMI (Internal Market Information System, Binnenmarkt-Informationssystem) oder in direktem Kontakt.
ZB-A5	**Sichere Verwaltung und Bearbeitung von Fällen** Die ZB muss die DLR-Vorgänge fristgerecht bearbeiten. Alle DLR-Vorgänge müssen sicher verwaltet werden, weitere Kommunikationsvorgänge mit dem EA, DL und ggfs. externen Akteuren müssen ausgelöst, Ein- und Ausgangsdokumente und Bescheide sicher übermittelt und aufbewahrt (Langzeitarchivierung), Terminmanagement durchgeführt und die Identitätsdaten und weitere vertrauliche Daten geschützt werden. Da die ZB nicht notwendigerweise eine zentrale Instanz ist, müssen eine Vielzahl verschiedener Behörden/Mitarbeiter interagieren, um den DLR-Vorgang zu bearbeiten. Dies erfordert nicht nur eine sichere behördenübergreifende Kommunikation, sondern auch den authentifizierten und autorisierten Zugriff auf die zu bearbeitenden Falldaten und –dokumente. Dabei ist der Zugriff nur für die Daten und Dokumente zu gestatten, die für die Bearbeitung notwendig sind. Identitätsmanagement ist daher eine notwendige Voraussetzung aus Sicht eines Dienstanbieters.
ZB-A6	**Zustellung von Bescheiden** Die ZB muss die termingerechte und rechtssichere Zustellung von Bescheiden ausführen.

Tabelle 3: Anforderungen der Zuständigen Behörde

3.2.3 Einheitlicher Ansprechpartner (EA)

Basierend auf der Typisierung von EAs (siehe Tabelle 1) sind unterschiedliche Ausprägungen hinsichtlich des angebotenen Funktionsumfangs möglich. Diese unterschiedlichen Funktionen bedeuten, dass je nach EA-Typ auch unterschiedliche Anforderungen hinsichtlich des Identitätsmanagements, des Datenschutzes und der Datensicherheit, z.B. für Authentifizierung, Dokumenteneinsicht, Fall- bzw. Vorgangsmanagement, Vollmachten, existieren.

Generell bearbeitet ein EA DLR-Vorgänge, die hier auch als „Fälle“ bezeichnet werden. Grundsätzlich kann man folgende Anforderungsprofile feststellen:

EA-Typ	IDM und sicherheitsbezogene Aktivitäten	Anforderungsprofil
Bote	Keine Verarbeitung von personenbezogenen Informationen; keinerlei Einblick in die Inhalte der Schriftsätze; Nachrichten werden ungelesen an die ZB gesendet	Bote muss authentisch sein; Nachweise der Übermittlung an die ZB müssen erbracht werden
Berater	Keine Verarbeitung von personenbezogenen Informationen; keinerlei Einblick in die Inhalte der Schriftsätze; Nachrichten werden ungelesen ZB gesendet	Berater muss authentisch sein; Nachweise der Übermittlung an die ZB müssen erbracht werden
Lotse	Einblick in das Anliegen, da gezielte Beratungs- oder Botendienste angeboten werden; jedoch kann dies auch ggfs. ohne Angabe personenbezogener Daten erfolgen da die Nachrichten nur weitergeleitet werden.	Lotse muss authentisch sein; Nachweise der Übermittlung an die ZB müssen erbracht werden
Mittler	Identitätsbezogener Zugang; einfache Vollmacht des DLs für Routinekommunikation mit ZB; Verwaltung der Fälle/Vorgänge; sichere Kommunikation mit ZB und DL	Mittler muss authentisch sein; DL Authentifizierung; Sichere Kommunikation mit DL/ZB einschließlich der Nachweise der Übermittlung; Einfache Vertretungsbefugnis; Fallmanagement
Verfahrens-manager	Identitätsbezogener Zugang; umfassende Vollmacht des DLs für Verfahrensvorgänge (verfahrensleitend) mit ZB; komplexe Verwaltung der Fälle/ Vorgänge; sichere Kommunikation mit ZB und DL	Verfahrensmanager muss authentisch sein; DL Authentifizierung; Sichere Kommunikation mit DL/ZB einschließlich der Nachweise der Übermittlung; Umfassende Vertretungsbefugnis; des DL Fallmanagement

EA-Typ	IDM und sicherheitsbezogene Aktivitäten	Anforderungsprofil
Superbe-hörde	In Deutschland nicht relevant, da keine Superbehörde eingerichtet wird, die bundesweit alle EU-DLR Anträge empfangen und bearbeiten kann.	Wird nicht betrachtet

Tabelle 4: Anforderungsprofil für Typen des Einheitlichen Ansprechpartners

Die Ergebnisse in Tabelle 4 zeigen, dass IDM und Sicherheitsanforderungen für alle EA-Typen existieren. Von allen EA-Typen hat der Verfahrensmanager die umfassendsten IDM und Sicherheitsanforderungen. In dieser Studie wird daher der Typ Verfahrensmanager hinsichtlich der Anforderungen näher betrachtet.

Nr.	Anforderungen für EA-Typ Verfahrensmanager
EA-A1	**Registrierung und Authentifizierung der Mitarbeiter** Die Registrierung und Authentifizierung der Mitarbeiter gegenüber den internen Systemen obliegt dem jeweiligen EA. Um die Berechtigungen der einzelnen Mitarbeiter zu verwalten, können diesen bestimmte Rollen zugeordnet werden.
EA-A2	**Gegenseitige Authentifizierung** Die Kommunikationspartner (DL, ZB) müssen authentisch sein, d.h. eine gegenseitige Authentifizierung muss erfolgen, damit der EA sicher sein kann, dass er mit den gewünschten Kommunikationspartnern kommuniziert. In direktem Kontakt muss der EA auch die grenzüberschreitende Authentifizierung des DL ermöglichen.
EA-A3	**Autorisierter Zugriff auf alle erforderlichen Verfahrensdaten** Der zuständige Mitarbeiter muss Zugriff auf alle erforderlichen Daten und Dokumente des Falles/Verfahrens haben. Liegen die Daten nicht lokal vor, so muss auch ein entfernter Zugriff möglich sein.
EA-A4	**Überprüfung von Daten und Dokumenten des DL auf Echtheit und Gültigkeit** Die vom DL übermittelten elektronischen Dokumente müssen hinsichtlich ihrer Echtheit und Gültigkeit überprüft werden können.
EA-A5	**Sichere Überwachung und Verwaltung von Fällen** Der EA muss alle DLR-Vorgänge sicher verwalten, weitere Kommunikationsvorgänge mit der ZB, DL und ggfs. externen Instanzen auslösen, Ein- und Ausgangsdokumente und Bescheide sicher übermitteln, ggfs. eine Mailbox bzw. persönlichen Bereich für den DL bereitstellen, Terminmanagement durchführen und die Identitätsdaten und weitere vertrauliche Daten schützen.

Nr.	Anforderungen für EA-Typ Verfahrensmanager
EA-A6	**Zustellung von Bescheiden** Der EA muss die termingerechte und rechtssichere Zustellung von Bescheiden ausführen.

Tabelle 5: Anforderungen des Einheitlichen Ansprechpartners

3.3 Fazit

In diesem Kapitel wurde die Vision eines bürgerfreundlichen Identitätsmanagement anhand eines konkreten Beispiels erläutert. Das Beispiel ist die Europäische Dienstleistungsrichtlinie. Die im Dezember 2006 verabschiedete EU-Dienstleistungsrichtlinie (EU-DLR, 2006) soll den Zugang zum Dienstleistungsmarkt in allen Mitgliedstaaten der Europäischen Union vereinfachen.

Die Umsetzung der EU-DLR involviert drei Akteure: Dienstleistungserbringer, d.h. Bürger oder Unternehmen, den Einheitlichen Ansprechpartner und die Zuständige Behörde als Dienstanbieter.

Für eine elektronische Abwicklung von Verwaltungsprozessen wie EU-DLR, sind die Übergabe und Überprüfung von Personalien und Dokumenten sowie die revisionssichere Aufbewahrung und Nachverfolgung von Vorgängen erforderlich. Zusätzlich erfordert die Umsetzung der EU-DLR eine grenzüberschreitende Authentifizierung der beteiligten Akteure. Nachgewiesen werden die jeweiligen Digitalen Identitäten der Akteure durch Attribute. Dabei besitzen nicht nur Personen eine Digitale Identität, sondern auch Dinge wie elektronische Dokumente oder ein Vorgang in der Verwaltung müssen eindeutig identifizierbar sein.

Für die Durchführung von EU-DLR gilt, dass zwischen den beteiligten Akteuren grenzüberschreitend ein Vertrauensverhältnis etabliert werden muss. Wie Vertrauensverhältnisse etabliert werden können, wird im folgenden Kapitel generisch untersucht. Dabei wird deutlich, dass »vertrauenswürdigen Dritte« unter bestimmten Bedingungen eingeschaltet werden müssen, um zwischen den Kommunikationspartnern Vertrauen zu schaffen.

4. Prozess- und Informationsmodell

4.1 Prozessmodell

In den folgenden Abschnitten werden die Prozesse beschrieben, in denen die Digitale Identität eines Anwenders und deren Attribute entsprechend der Vision Verwendung finden. Der wesentliche Prozess dabei ist **»Zugriff auf einen Dienst erlangen«**.

Um die Prozesse darzustellen, wird eine vereinfachte Form des Standards Business Process Modeling Notation – BPMN benutzt (OMG, 2008). Dabei hat jeder Akteur seine eigene Bahn (»swim lane«), in der seine Aktivitäten liegen.

Über mehrere Stufen hinweg wird entwickelt, unter welchen Voraussetzungen und Annahmen welche Entitäten, z.B. Attribut-Zertifizierer, notwendig und sinnvoll sind. Dabei zeigt die Darstellung des Prozesses nicht alle möglichen Wege und Kreuzungen auf, sondern nur diejenigen, die für die Ableitung der Voraussetzungen und Annahmen erforderlich sind.

4.1.1 Dienstanbieter vertraut dem Anwender

Der **Dienstanbieter** benötigt für die Freigabe seines Dienstes eine Auswahl der Attribute der Digitalen Identität des **Anwenders**. Sofern er dem Anwender vertraut, wird er auch den vom Anwender präsentierten Attributen vertrauen.

Damit sind in diesem Szenario nur zwei Akteure, der Anwender und der Dienstanbieter, notwendig. Folgendes Diagramm stellt diesen Sachverhalt dar.

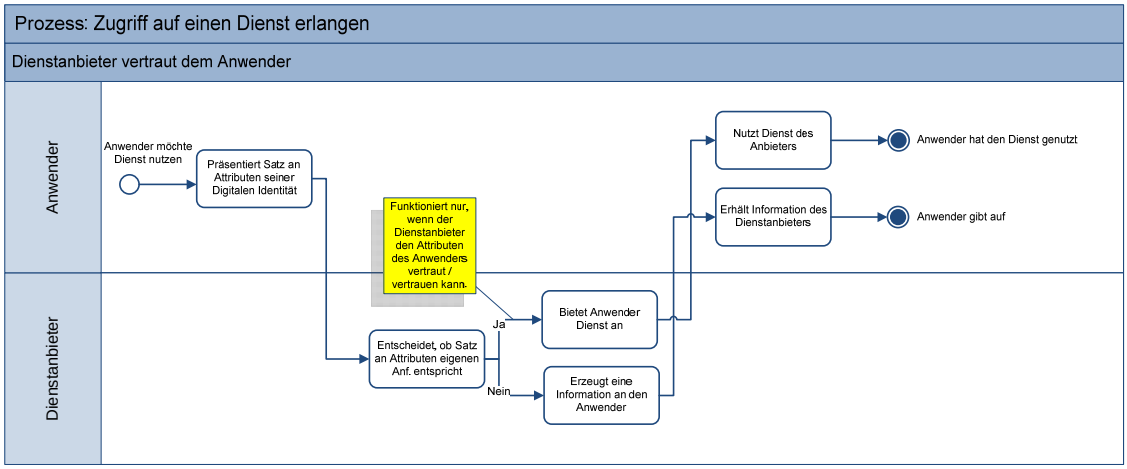


Abbildung 2: Prozess »Zugriff auf einen Dienst erlangen« (1)

Ein grundsätzliches Vertrauen zwischen dem Dienstanbieter und dem Anwender kann aber nicht vorausgesetzt werden. Damit befasst sich der nächste Abschnitt.

4.1.2 Attribut-Zertifizierer vertraut dem Anwender und Dienstanbieter vertraut dem Attribut-Zertifizierer

Gibt es dieses Vertrauen zwischen Anwender und Dienstanbieter nicht, so ist eine der Möglichkeiten, diese Situation zu lösen, einen »vertrauenswürdigen Dritten« einzuschalten, der eine Vertrauensbeziehung zwischen den Attributen des Anwenders und dem Dienstanbieter schafft. Der Attribut-Zertifizierer bestätigt dabei dem Satz an

Attributen des Anwenders mittels eines **Zertifikats** seine Gültigkeit; dabei soll hier ein Zertifikat als eine Bescheinigung verstanden werden (Wahrig, 2002).[2]

Damit wird der Prozess um den Akteur **Attribut-Zertifizierer**[3] erweitert, was in folgender Abbildung dargestellt ist.[4]

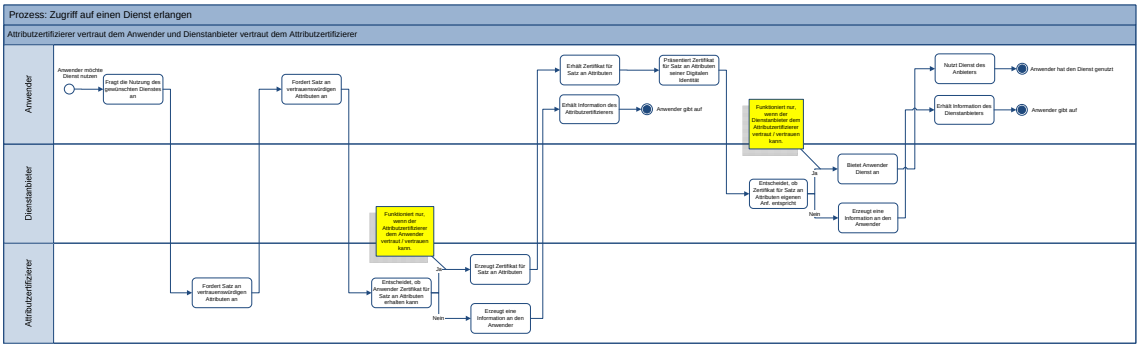


Abbildung 3: Prozess »Zugriff auf einen Dienst erlangen« (2)

Daher ergibt sich als erste These:

These 1:
Ein Attribut-Zertifizierer ist nur notwendig, um Vertrauen zwischen einem Anwender und einem Dienstanbieter zu schaffen.

Unter Umständen ist mehr als ein Attribut-Zertifizierer notwendig, um das benötigte Vertrauen zu schaffen; damit beschäftigt sich der nächste Abschnitt.

4.1.3 Attribut-Zertifizierer1 vertraut dem Anwender und Dienstanbieter vertraut dem Attribut-Zertifizierer2

Gibt es keinen gemeinsamen vertrauenswürdigen Dritten, auf den sich Anwender und Dienstanbieter einigen können, so ergibt sich aus dieser Situation keine neue Entität im Prozess. Es wird nur eine weitere Instanz des Akteurs **Attribut-Zertifizierer** benötigt.

Dies wird in der folgenden Abbildung dargestellt, der Attribut-Zertifizierer2 erhält dabei seine eigene Bahn neben dem Attribut-Zertifizierer1. Zudem vertraut der Attribut-Zertifizierer1 dem Anwender und der Dienstanbieter dem Attribut-Zertifizierer2.

---

[2] An dieser Stelle wird noch nichts über eine technische Umsetzung des Zertifikats ausgesagt, insbesondere sind hier nicht zwingend Digitale Zertifikate gemäß X.509 gemeint.

[3] In einem Teil der Literatur wird der Attribut-Zertifizierer auch Identitätsanbieter (Identity Provider) genannt. Wir halten diese Bezeichnung für irreführend, da zum einen keine komplette Digitale Identität zur Verfügung gestellt wird, sondern immer nur Ausschnitte davon, und zum anderen die Aufgabe dieser Instanz das Bestätigen des Satzes von Attributen und nicht nur die Bereitstellung der Attribute ist.

[4] In diesem Prozess könnte der Attribut-Zertifizierer sein Zertifikat zum Satz an Attributen der Digitalen Identität des Anwenders auch direkt an den Dienstanbieter übermitteln. Hier wurde eine andere Möglichkeit gewählt, um entsprechend der Vision die Verfügungsgewalt des Anwenders über die Attribute seiner Digitalen Identität zu zeigen.

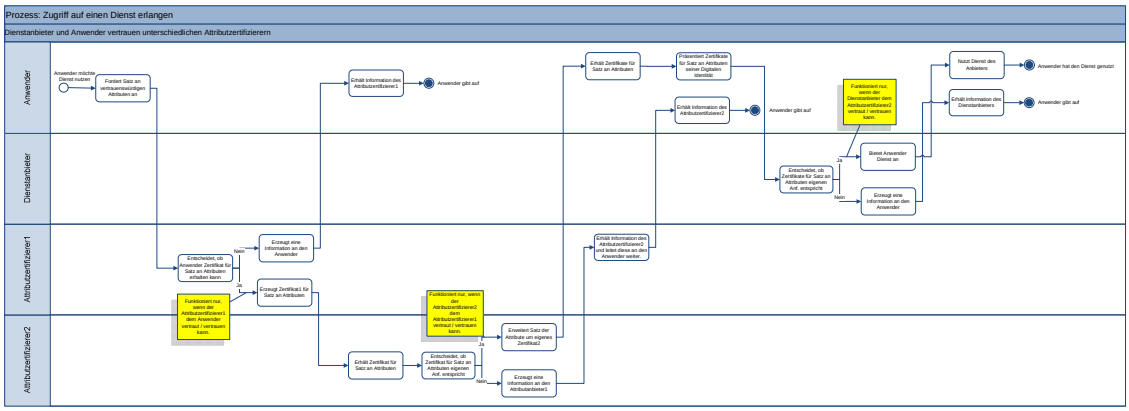


Abbildung 4: Prozess »Zugriff auf einen Dienst erlangen« (3)

Hierdurch gelangen wir zu unserer nächsten These:

These 2:
Wird vom Anwender und vom Dienstanbieter unterschiedlichen Attribut-Zertifizierern vertraut, so muss es ein Vertrauensverhältnis zwischen den verschiedenen Attribut-Zertifizierern (»Vertrauenskette«) geben, um dem Anwender den Zugriff auf den gewünschten Dienst zu ermöglichen.

Ein Vertrauensverhältnis ist bisher noch nicht vollständig beschrieben worden, das zwischen dem Anwender und dem Attribut-Zertifizierer; damit beschäftigt sich der nächste Abschnitt.

4.1.4 Initiales Vertrauensverhältnis

Zwischen dem Anwender und dem Attribut-Zertifizierer ist ein initiales Vertrauen zu schaffen, damit dem Anwender die entsprechenden Attribute durch den Attribut-Zertifizierer bescheinigt werden und der Anwender sich dessen sicher sein kann, das die erhaltenen Bescheinigungen auch einen Wert haben.

Wie ist dieses Vertrauen zu erlangen? Lassen wir dazu Bernd Lahno, Professor für Philosophie an der Frankfurt School of Finance & Management, zu Wort kommen (Lahno, 2008):

Vertrauen ist ein merkwürdiges Phänomen. Wir denken vor allem dann darüber nach, wenn es prekär geworden ist. Wenn es nicht da ist, beschäftigt es uns. Ist es da, umgibt es uns oft, ohne wirklich bemerkt zu werden. …

So wie es manchmal schwerfällt, regelmäßig zu atmen, wenn man sich einmal der Notwendigkeit der Atmung bewusst wird, so wird Vertrauen oft in dem Augenblick problematisch, in dem man versucht, seine Gründe zu finden. Wer fragt „Warum vertraue ich?“, der hat damit die Selbstverständlichkeit, die Vertrauen in aller Regel umgibt, schon zerstört und Vertrauen „in Frage“ gestellt. Das ist auch einer der Gründe, warum Vertrauen, wenn es einmal verloren gegangen ist, nur so schwer wiederhergestellt werden kann. Nachdenken allein hilft da nur selten. In einem gewissen Sinne ist es sogar kontraproduktiv – weil es den Blick auf Risiken richtet, die Vertrauen gerade ausblenden. …

Damit sind zwei wesentliche Aspekte des Vertrauens genannt. Vertrauen ist einerseits durch die Bereitschaft gekennzeichnet, sich für die Handlungsentscheidungen anderer verletzlich zu machen, und andererseits durch Vertrauenserwartungen, die diese Bereitschaft stützen und motivieren – Erwartungen, dass die Verletzlichkeit nicht

ausgenutzt wird. Vertrauenserwartungen werden in vielen Fällen nicht auf einer bewussten Überlegung oder Abwägung der Fakten beruhen. Oft werden ja gerade solche Überlegungen nicht angestellt. Eine Erwartung zu haben bedeutet aber nicht notwendig, bewusst einen bestimmten Gedanken zu haben. Manchmal wird einem erst hinterher klar, dass man eine bestimmte Erwartung hatte, zum Beispiel wenn diese Erwartung schmerzlich enttäuscht wird. Ob also mehr oder weniger bewusst, … Vertrauen ist grundsätzlich durch die Erwartung gekennzeichnet, derjenige, dem man vertraut, werde unsere vertrauensvollen Handlungen nicht zu unserem Schaden nutzen. …

Abbildung 5: Definition von Vertrauen (nach (Lahno, 2008))

In diesem Sinne ist das initiale Vertrauen durch eine Vertrauenserwartung zu schaffen. Das geht oft am leichtesten, wenn die entsprechende Instanz schon in vorangegangenen Erfahrungen, möglicherweise auch in einem ganz anderen Kontext, als vertrauenswürdig erlebt wurde.

Beispiele hierzu wären etwa die „Sterne“, die ein Verkäufer bei Amazon sammeln kann und die anderen Käufern als Erfahrungssammlung dienen, um ein initiales Vertrauen in diesen Verkäufer zu schaffen.

4.1.5 Informationsmodell

Im vorangegangenen Abschnitt wurden die Prozesse beschrieben, in denen die Digitale Identität Anwendung findet. Im nachfolgenden Informationsmodell wird detailliert beschrieben, welche Elemente, genannt Entitäten, in einem bürgerfreundlichen Identitätsmanagement interagieren bzw. in den Prozessen verwendet werden.

Eine **Entität** ist die kleinste, wiederverwendbare Einheit, die in der Darstellung der Prozesse in einem bürgerfreundlichen Identitätsmanagement verwendet wird. Entitäten besitzen Eigenschaften und Beziehungen zueinander.

Eine Beziehung zwischen zwei Entitäten ist immer bidirektional, d.h. ein Anwender besitzt eine Digitale Identität und in der Gegenrichtung gehört die Digitale Identität einem Anwender.

In der Beschreibung wird Wert darauf gelegt, das Wesentliche, den Kern einer Entität zu beschreiben und nicht mögliche Realisierungen darzustellen. Dies erlaubt es, die wesentlichen Anforderungen an die jeweiligen Entitäten zu ermitteln.

Die nachfolgende Grafik gibt einen Überblick, wie die einzelnen Entitäten zueinander in Beziehung stehen.

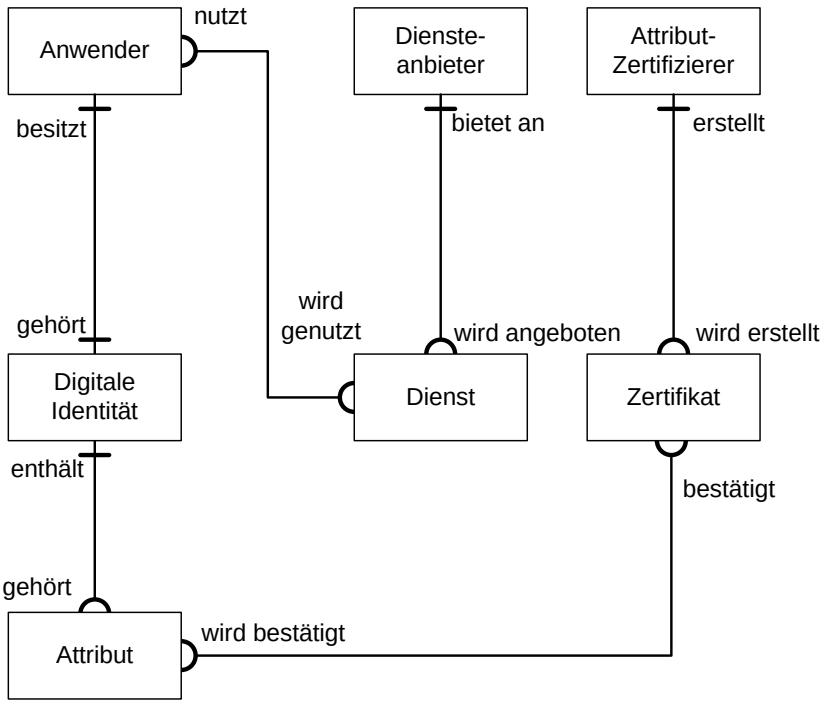
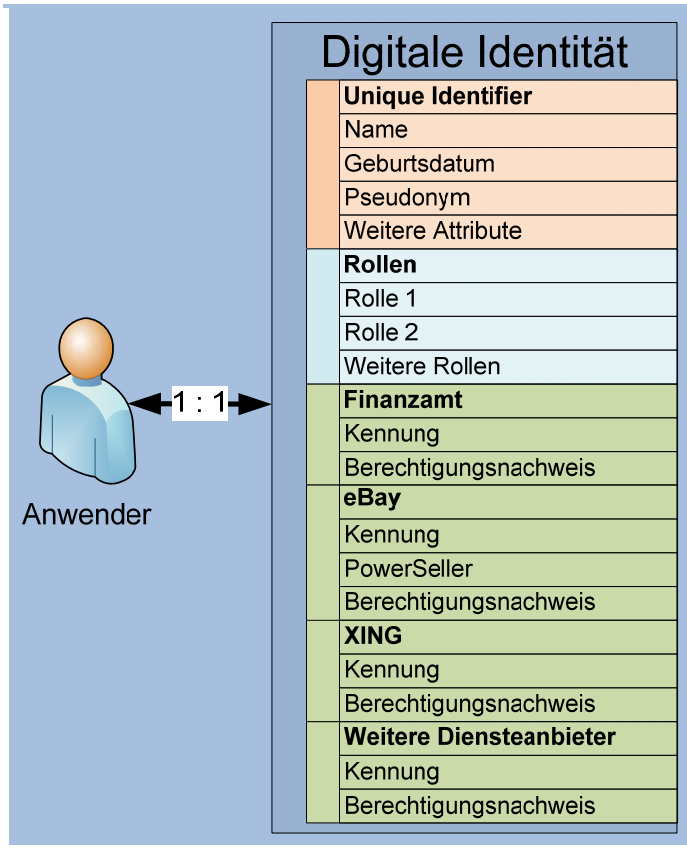


Abbildung 6: Informationsmodell

In den folgenden Tabellen werden die Entitäten kurz beschrieben.

Name der Entität	Anwender
Entität ID	E-001
Beschreibung	Ein Anwender ist eine natürliche oder juristische Person, die in der Digitalen Welt interagiert, interagiert hat oder interagieren will.
Beispiele	Angelika Steinacker FOKUS

Name der Entität	Digitale Identität
Entität ID	E-002
Beschreibung	Die Digitale Identität eines Anwenders ist die Repräsentation des Anwenders in der Digitalen Welt. Sie enthält Informationen, die Attribute, die dem Anwender zugeordnet sind. Jeder Anwender besitzt genau eine Digitale Identität; die Anzahl und Art der Attribute ist nicht festgelegt.

Beispiele	

Name der Entität	**Attribut der Digitalen Identität**
Entität ID	E-003
Beschreibung	Ein Attribut ist eine Information innerhalb der Digitalen Identität eines Anwenders. Zwar besitzt jeder Anwender genau eine Digitale Identität, aber die Anzahl der zugeordneten Attribute und die Art ist nicht festgelegt. Attribute werden der Digitalen Identität eines Anwenders in dem Maße hinzugefügt, in dem er Transaktionen in der Digitalen Welt durchführt. Der Anwender muss nicht Eigentümer eines Attributs sein, er hat aber die Verfügungsgewalt über die seiner Digitalen Identität zugeordneten Attribute. Eine Sonderstellung nimmt das Attribut des „Unique Identifier“ ein. Es differenziert einen Nutzer eineindeutig von einem anderen und ist zunächst einmal nur ein virtuelles Konstrukt. In einer tatsächlichen Realisierung kann es vorkommen, dass ein solches eineindeutiges Merkmal unerwünscht oder sogar ungesetzlich ist, sofern es anderen als dem Eigentümer der Digitalen Identität bekannt wird.

	In diesem Fall wird in einer Realisierung das eineindeutige Merkmal durch verschiedene, dienstspezifische Merkmale ersetzt werden.
Beispiele	Name Geburtsdatum Steuernummer Personalausweisnummer Adresse Kennung und Passwort bei XING Kontonummer Zuverlässiger Verkäufer bei Amazon

Name der Entität	**Dienstanbieter**
Entität ID	E-004
Beschreibung	Ein Dienstanbieter ist eine natürliche oder juristische Person, die einen Dienst in der Digitalen Welt anbietet.
Beispiele	Amazon Finanzamt Gemeindeverwaltung

Name der Entität	**Dienst**
Entität ID	E-005
Beschreibung	Ein Dienst ist eine Leistung, die in der Digitalen Welt von einem Dienstanbieter angeboten wird, und in der Digitalen oder der realen Welt erbracht wird.
Beispiele	Elektronische Steuererklärung Kauf eines Buches Vermittlung eines Partners

Name der Entität	**Attribut-Zertifizierer**
Entität ID	E-006
Beschreibung	Ein Attribut-Zertifizierer ist eine natürliche oder juristische Person, die die Gültigkeit eines oder mehrerer Attribute, die zu der Digitalen Identität eines Anwenders gehören, bestätigt.

Beispiele	Finanzamt Käufer bei Amazon

Name der Entität	**Zertifikat**
Entität ID	E-007
Beschreibung	Die Gültigkeit eines oder mehrerer Attribute, die zu der Digitalen Identität eines Anwenders gehören, werden mit Hilfe eines Zertifikats bestätigt.
Beispiele	Digitale Signatur „Sternchen“ für den Verkäufer bei Amazon oder ebay

4.2 Fazit

In diesem Kapitel wurden die notwendigen Entitäten für ein bürgerfreundliches Identitätsmanagement hergeleitet. Es wurde gezeigt, wie mit Hilfe von Attributen und den dazugehörigen Zertifikaten Vertrauen zwischen den beteiligten Instanzen geschaffen werden kann und wie die Prozesse und Abläufe für die Dienstnutzung aussehen.

Eine wichtige Stellung nimmt dabei der Attribut-Zertifizierer ein, der durch das Erstellen von Zertifikaten genau dieses Vertrauen zwischen zwei Instanzen herstellt.

Im nächsten Kapitel werden die logischen Komponente und Module erarbeitet, die notwendig sind, um die vorgestellten Prozesse sicher und verlässlich umzusetzen.

5. Rahmenarchitektur

Entsprechend dem im Kapitel 4.1.5 vorgestellten Informationsmodell sind drei Akteure für ein bürgerfreundliches Identitätsmanagement erforderlich. Diese sind

- der Bürger / Anwender
- der Dienstanbieter und der
- Attribut-Zertifizierer.

Die erforderlichen logischen Komponenten und Module für jeden Akteur werden in den nachfolgenden Kapiteln dargestellt und erläutert. Dabei wird die logische Zielarchitektur entworfen. Es soll aufgezeigt werden, welche Komponenten grundsätzlich erforderlich sind und welchen Funktionen bzw. Aufgaben diese erfüllen müssen, um ein bürgerfreundliches Identitätsmanagement umzusetzen.

Die folgende Grafik zeigt die Komponenten der drei Akteure. Um hier einen besseren Abgleich mit bereits bestehenden Architekturen zu erreichen, wurden für die Servicenamen englische Begriffe genutzt. Die Bedeutung der verschiedenen Farben ist weiter unten erklärt.

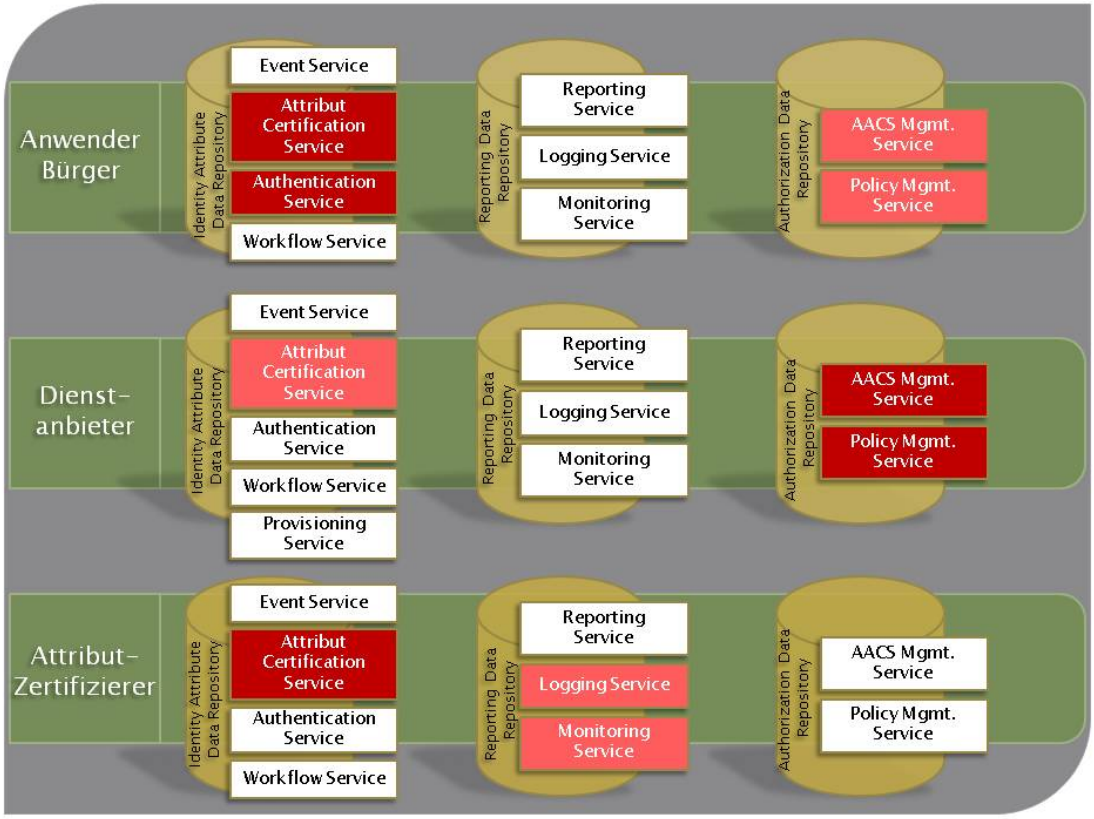


Abbildung 7: Rahmenarchitektur

Die beteiligten Akteure nutzen überwiegend die gleichen Services. Der Provisioning Service ist spezifisch für den Dienstanbieter. Über den Event Service werden Informationen zwischen den Entitäten ausgetauscht.

Innerhalb eines Akteurs wurden Services in der Zeichnung rot eingefärbt. Damit wird die Bedeutung eines Service für den Akteur herausgehoben. Dunkel rot kennzeichnet

einen Service mit sehr hoher Bedeutung, hell rot mit mittlerer Bedeutung. Die weiteren Services sind nicht gefüllt.

Je nach Zielrichtung kann eine nachfolgende technische Implementierung alle Komponenten bzw. nur ein Teil der aufgezeigten Bestandteile und Leistungen bereitstellen. Im Kapitel 8 werden bereits bestehende Lösungen der aufgezeigten Zielarchitektur gegenübergestellt und beschrieben.

In den nachfolgenden Kapiteln werden die Services zunächst allgemein beschrieben. Anschließend werden tabellarisch die unterschiedlichen Ausprägungen hinsichtlich der drei Entitäten ausgearbeitet. Das Farbschema zur Darstellung der Bedeutung des Services wurde auch in der tabellarischen Beschreibung der spezifischen Ausprägungen für die Entitäten verwendet.

5.1 Identity Attribute Data Repository

Die Kernkomponente einer bürgerfreundlichen Identitätsmanagement Lösung ist das Identity Attribute Data Repository. In diesem Ablageort werden Attribute einer der Digitalen Identität eines Anwenders wie z.B.

- Name, Vorname, Adresse,
- Bankverbindung,
- weitere organisatorische Daten,
- bei Dienstanbietern definierten Benutzerkonten und
- Identitätsnachweise

verwaltet.

Änderungen innerhalb des Identity Attribute Data Repository werden, entsprechend der definierten Einstellung, über den Event Service an die entsprechende Entität automatisiert weiter geleitet. Ändert z.B. der Anwender eine Bankverbindung, so wird diese Information – entsprechend der aktiven Einstellung – automatisiert an die betroffenen Dienstanbieter übermittelt. Durch diesen Mechanismus wird die Datenintegrität zwischen Bürger und Dienstanbieter unterstützt.

Entität	Spezifische Ausprägung
Anwender / Bürger	Die zertifizierten Attribute des Anwenders werden im Repository abgelegt und mit Nutzungsberechtigungen versehen.
Dienstanbieter	Im Repository des Dienstanbieters werden die für die Abarbeitung der Geschäftsprozesse des Dienstanbieters erforderlichen Informationen gehalten. Die zertifizierten Attribute des Anwenders bilden eine Teilmenge der verwalteten Informationen.
Attribut-Zertifizierer	Als Grundlage für die Zertifizierung von Attributen nutzt der Attribut-Zertifizierer in der Regel das Repository des Dienstanbieters, da dort die Informationen aktuell durch den Dienstanbieter verwaltet werden. Nur in besonderen Anwendungsfällen ist es erforderlich, dass der Attribut-Zertifizierer ein eigenständiges Repository aufbaut und verwaltet. Änderungen durch den Dienstanbieter an Informationen müssen in diesem Fall zeitnah gemeldet werden.

5.1.1 Event Service

Der Event Service reagiert auf definierte Aktionen wie z.B. den Erhalt von Nachrichten oder das Initiieren eines Monitor Events und stellt die zentrale Kommunikationskomponente einer zukünftigen Lösung dar. Der Event Service arbeitet auf der Basis der Informationen des Identity Attribute Data Repositories.

Die Kommunikation wird bidirektional durchgeführt, d.h. zwischen Anwender und Dienstanbieter, Dienstanbieter und Attribut-Zertifizierer oder Anwender und Attribut-Zertifizierer. Die Nachrichten müssen einen standardisierten Schema entsprechen und die Integrität, Vertraulichkeit, Verfügbarkeit und Verbindlichkeit gewährleisten.

Die nachfolgenden Nachrichten bilden eine Auswahl von Informationen, auf die ein Event Service reagieren muss, z.B. indem er interne Workflowprozesse startet oder Informationen ändert:

- Anforderung, ein Attribut zu übergeben bzw. Erhalt des Attributs
- Information, dass ein Dienst genutzt werden kann
- Information, dass ein Attribut genutzt wurde
- Information, dass ein Attribut verifiziert wurde
- Information, dass ein Attribut weitergeleitet wurde
- Information, dass ein Attribut gelöscht wurde unter Angabe einer Begründung, z.B. Anforderung des Anwenders, Zertifizierung ausgelaufen, Info von Zertifizierungsstelle
- Angeforderte Reports wie z.B. genutzte, gespeicherte oder weitergeleitete Attribute des Anwenders
- Über das Entziehen der Gültigkeit der Zertifizierung eines Attributes vom Attribut-Zertifizierer
- Anfrage des Dienstanbieters eine Authentisierung durchzuführen
- Anfrage an den Dienstanbieter den Nachweis (neu) zu erstellen
- Anforderung ein zertifiziertes Attribut zu erstellen
- Anforderung die Zertifizierung eines Attributs zu prüfen

Die folgenden Nachrichten bilden eine Auswahl der verschiedenen Meldungen, die von einem Event Service versendet werden:

- Anfrage, die Nutzungsmöglichkeit für eine Dienstleistung bereitzustellen
- Information, dass ein Attribut geändert wurde (z.B. Bankverbindung, Adresse)
- Information, dass ein Attribut neu zertifiziert wurde
- Information, dass ein Attribut zurückgezogen wurde
- Anforderung eines durch den Dienstanbieter bereitgestellten Reports
- Angeforderte Attribute inklusive der Nutzungsregeln
- Angeforderte Authentisierungsinformationen
- Anforderung, die Kennung / die Zugriffsmöglichkeit / die Nutzung eines Dienstanbieter zu deaktivieren / löschen
- Anforderung eine Auskunft über die verfügbaren Leistungen des Dienstanbieters hinsichtlich des bürgerfreundlichen Identitätsmanagements zu erhalten.
- zertifiziertes Attribut
- Prüfungsergebnis eines Attributes
- Information über das Entziehen der Gültigkeit eines zertifizierten Attributs

Entität	Spezifische Ausprägung
Anwender / Bürger	Der Anwender sollte die Möglichkeit haben, zu spezifizieren, welche Nachrichten/Events • automatisiert versendet / bearbeitet werden, • welche explizierter Zustimmung bedürfen und • welche nicht gesendet / bearbeitet werden.
Dienstanbieter	Der Versand und die Verarbeitung von Nachrichten sollen automatisiert erfolgen.
Attribut-Zertifizierer	Der Versand und die Verarbeitung von Nachrichten sollen automatisiert erfolgen.

5.1.2 Attribute Certification Service

Der Attribute Certification Service setzt die folgenden Aufgaben um:

- initiiert die Zertifizierung von Attributen,
- führt die Zertifizierung von Attributen aus,
- initiiert die Prüfung der Zertifizierung von Attributen,
- führt die Prüfung der Zertifizierung von Attributen aus.

Durch den Attribute Certification Service kann ein einzelnes Attribut zertifiziert werden z.B.: der Bürger hat einen Ausweis der Stadtbücherei, hat Steuerklasse 3. Ein Set von Attributen kann ebenfalls beglaubigt werden, wie z.B. durch das Finanzamt mit den Attributen Steuernummer, Steuerklasse, Freibetrag.

In der Regel sollte ein Attribut einzeln zertifiziert werden, damit für unterschiedliche Anforderungen die Attribute durch den Anwender unterschiedlich zusammengestellt werden können. Damit wird auch das Grundprinzip der Datensparsamkeit berücksichtigt.

Ein Attribut muss eindeutig und nachweisbar mit einer Identität des Anwenders verbunden werden können. Dazu wird ein Personenkennzeichen (siehe 7.1.1) generiert und verwaltet. Die Identität kann hierbei innerhalb der Domäne eines Dienstanbieters eindeutig sein (dienstanbieterspezifisches Personenkennzeichen) bzw. auch direkt einer Person eindeutig zugeordnet werden (universelles Personenkennzeichen). Durch die Nutzung von dienstanbieterspezifischen Personenkennzeichen kann ein Pseudonym für den Anwender definiert werden.

Die Steuerklasse als Attribut ist für sich alleine keine sinnvoll verwertbare Information. Erst mit der eindeutigen Zuordnung zu einer Steuernummer (dienstanbieterspezifisches Personenkennzeichen) kann zunächst innerhalb der Anwendungen der Finanzbehörden zweifelsfrei auf die betreffende Person geschlossen werden.

Dieses Kennzeichen, mit dem eine eindeutige Zuordnung auf eine Identität möglich ist, muss für jedes Attribut festgelegt werden (siehe Kapitel 4 Prozess- und Informationsmodell). Dazu sind unterschiedliche technische Möglichkeiten zur Realisierung denkbar.

Die Prüfung der Gültigkeit des Attributs wird ebenfalls durch den Service bereitgestellt. Dabei kann der Service nur die selbst ausgestellten Attribute korrekt prüfen. Die Prüfung findet auf dem aktuellen Informationsstand des Attribut-Zertifizierers statt, d.h.

am Beispiel des Finanzamtes wird geprüft, ob die Steuerklasse aktuell noch wie im Zertifikat angegeben eingetragen ist.

Werden Informationen eines Anwenders z.B. im Rahmen der Geschäftsprozesse beim Dienstanbieter geändert, so muss dies eine Rückwirkung auf die zertifizierten Attribute besitzen. Wird z.B. vom Finanzamt die Steuernummer oder der Freibetrag geändert, so muss der Zertifizierungs-Status geprüft werden. Wurde ein Attribut bereits zertifiziert, so muss eine Aktualisierungsmeldung an den Benutzer gesendet werden. Gleichzeitig muss das alte zertifizierte Attribut zurückgezogen werden, d.h. hier muss ein entsprechendes Verzeichnis gepflegt werden.

Die Änderungsmeldung enthält weiterhin einen Kritikalitätsstatus, mit dem angezeigt wird, wie dringend die zeitnahe Verarbeitung der Meldung ist. Wird z.B. die eBay-Bewertung einen Punkt hochgesetzt, hat diese Änderungsmeldung eher informativen Charakter und muss nicht zeitnah verarbeitet werden. Wird jedoch aufgrund eines Verstoßes gegen die Geschäftsvereinbarungen die eBay-Kennung deaktiviert, so muss dies zeitnah gemeldet und von den beteiligten Akteuren verarbeitet werden.

Entität	Spezifische Ausprägung
Anwender / Bürger	Für den Bürger ist dieser Dienst von zentraler Bedeutung, da hier sensible, personenbezogene Informationen des Bürgers verwaltet werden. Für ein Attribut können durch den Anwender unterschiedliche Privacy Policies gesetzt werden wie z.B.: • Darf das Attribut von einem Dienstanbieter weitergeleitet werden (Ja / Nein) • Verwendungszweck des Attributes, z.B.: nur für einen Dienstanbieter, für einen Typ von Dienstanbietern (Behörden, oder mit definierbarer Vertrauensstellung) oder für alle Dienstanbieter, d.h. frei • Die Gültigkeitsdauer des Attributes z.B. vom Anwender definiert bzw. von der Zertifizierungsstelle. Dabei gilt immer die kleinste definierte Zeitdauer. Der Anwender kann selbst Attribute in einer Art Selbstauskunft zertifizieren und verwenden.
Dienstanbieter	Für die innerhalb der Geschäftsprozesse erforderlichen Informationen fordert der Dienstanbieter zertifizierte Attribute beim Anwender / Bürger ein. Die Prüfung durch den Attribut-Zertifizierer wird je nach Vertrauensstellung durch den Dienstanbieter eingeleitet. Werden Attribute des Anwenders geändert z.B. Veränderung der Käuferbewertung bei eBay muss eine entsprechende Benachrichtigung versendet werden.
Attribut-Zertifizierer	Der Service verbindet mit der Zertifizierung vertrauenswürdig ein Attribut mit einem eindeutigen Kennzeichen mittels dessen eindeutig und nachvollziehbar auf eine Identität geschlossen werden kann. Die Informationsbasis auf der der Attribut-Zertifizierer die Zertifizierung durchführt liegt in der Regel beim Dienstanbieter.

5.1.3 Authentication Service

Die Aufgabe der Verwaltung, der sicheren Speicherung der Benutzerkonten und der dazugehörigen Nachweise übernimmt der Authentication Service. Nachweise können im einfachsten Falle Passwörter mit unterschiedlichen Qualitätsstufen sein. Für sicherheitskritische Anwendungen können Zertifikate oder Tokens verwaltet werden.

Der Authentication Service führt die Authentisierung zwischen den Entitäten, z.B. des Bürgers beim Dienstanbieter, automatisiert aus. Informationen werden über den Event Service des Dienstanbieters an den Event Service des Anwenders übermittelt. Sind die erforderlichen Nachweise im Authentication Service (bzw. im Identity Attribute Data Repository) des Anwenders vorhanden, werden sie übermittelt und die Authentisierung durchgeführt.

Entsprechend der Kritikalität wird vorab der Sicherheitslevel vom Dienstanbieter definiert und damit die Art des erforderlichen Nachweises bestimmt. Hier können die Kriterien aus dem STORK Projekt (siehe 7.1.5) genutzt werden.

Weiterhin stößt dieser Service den Start der Generierung eines neuen Nachweises an. Dieser Prozess kann transparent ausgeführt werden, solange keine speziellen Produkte zum Einsatz kommen, die besondere Hardware (z.B. SecureID Token) erfordern.

Das Rücksetzen und das Deaktivieren von Nachweisen werden durch diesen Service ebenfalls automatisiert ausgeführt. Durch die weitgehende Automatisierung können dienstleistungsspezifische, komplexe Passwörter genutzt werden, da in der Regel der Anwender das definierte Passwort nicht selbst manuell verwenden muss. Dies erhöht insgesamt das Sicherheitsniveau.

Entität	Spezifische Ausprägung
Anwender / Bürger	An diesem Dienst hängt stark die Bürgerfreundlichkeit der gesamten Lösung. Die automatisierte Authentisierung muss durch den Anwender transparent gesteuert werden können. Dabei sind unterschiedliche Stufen denkbar, z.B. • vollständig automatisiert; • automatisiert, Benutzer erhält Information; • Start der automatisierten Authentisierung wird durch; Benutzer freigegeben • Manuelle Authentisierung.
Dienstanbieter	Für den Dienstanbieter gibt es unterschiedliche Situationen in denen es sinnvoll ist eine eigenständige Kennung für Benutzer anzulegen und damit eine Authentisierung durchzuführen. Ein Grund ist z.B. dem Anwender Zugriff auf nicht öffentlich zur Verfügung stehende Informationen zu geben. Ein weiter Grund kann die Abwicklung von Bestell-/Bezahlvorgängen sein.
Attribut-Zertifizierer	Bei Anfragen an den Attribut-Zertifizierer findet zunächst eine Authentisierung statt, um die Anfragende Identität zu bestimmen. Damit ist es möglich dem Benutzer Auskunft zu geben, welche Identitäten z.B. eine Prüfung eines Attributes des Benutzers initiierten.

5.1.4 Workflow Service

Der Workflow Service lässt automatisierte Prozesse mit und ohne Benutzerinteraktion ablaufen. Damit werden Schritte wie

- das Anlegen von Accounts mit den entsprechenden Attributen
- das Löschen von Accounts inklusive der gespeicherten Attribute
- die Zertifizierung von Attributen
- das Prüfen der Zertifizierung von Attributen
- das Rücksetzen von Nachweisen zur Anwenderauthentisierung

nachvollziehbar und zeitnah durchgeführt.

Die Ausprägung und der Umfang verwendeter Workflows sind spezifisch für die Entitäten. Durch eine einheitliche Schnittstelle können auch entitätsübergreifende Prozesse eingerichtet und automatisiert werden.

Entität	Spezifische Ausprägung
Anwender / Bürger	Generische, wiederverwendbare Workflows können durch Dritte zur Verfügung gestellt und vom Anwender für seine Zwecke genutzt werden. Damit können unterschiedliche Einsatzzwecke ohne Programmierkenntnisse des Anwenders realisiert werden.
Dienstanbieter	Workflow-Prozesse werden eigenverantwortlich vom Dienstanbieter erstellt und gewartet. Durch eine standardisierte Schnittstelle wird der Informationsaustausch ermöglicht.
Attribut-Zertifizierer	Workflow-Prozesse werden eigenverantwortlich vom Attribut-Zertifizierer erstellt und gewartet. Durch eine standardisierte Schnittstelle wird der Informationsaustausch ermöglicht.

5.1.5 Provisioning Service

Ein Dienstanbieter nutzt in der Regel mehrere Systeme oder Anwendungen, um die angebotene Dienstleistung zu erbringen. Die Darstellung des Angebots wird z.B. über ein Web-Portal gesteuert. Die Abwicklung der Bestellung geschieht im ERP System. Um eine Nachvollziehbarkeit der Aktionen zu gewährleisten werden individualisierte Kennungen in beiden Systemen angelegt und mit Berechtigungen versehen.

Dieser Service dient dazu, Kennungen und Berechtigungen für die Anwender auf den einzelnen Systemen automatisiert zu erzeugen und zu verwalteten. Über den Provisioning Service kann

- die Erzeugung von Benutzerkonten,
- die Erteilung bzw. der Entzug von Berechtigungen und
- die Deaktivierung / Löschung von Benutzerkonten

stringent und automatisiert ausgeführt werden.

Das Aufnehmen eines Auftrags, die Durchführungsschritte und das Ergebnis werden über die Logging Service automatisiert dokumentiert.

Entität	Spezifische Ausprägung
Anwender / Bürger	Keine Anwendung
Dienstanbieter	Siehe Text
Attribut-Zertifizierer	Keine Anwendung

5.2 Reporting Data Repository

Im Logging und Monitoring Repository werden Informationen aus den entsprechenden Services abgelegt. Dabei werden zumindest die folgenden Informationen in jedem Datensatz gespeichert:

- zugehöriges Benutzerkonto
- Datum und Zeit des protokollierten Ereignisses
- Typ des Ereignisses
- Art der Statusänderung
- Weitere prozessrelevante Informationen

Zusätzlich sind im Repository noch definierte Schwellwerte und die zugehörigen Reaktionen abgelegt. Als Schwellwert für den Anwender kann z.B. die Anzahl der Weiterleitungen seiner Adressdaten definiert werden. Der Schwellenwert und die Reaktion wären dann wie folgt definiert: Werden diese Informationen mehr als dreimal durch einen Dienstanbieter weitergeleitet, so wird automatisiert der Anwender informiert.

Entität	Spezifische Ausprägung
Anwender / Bürger	Im Repository des Anwenders / Bürgers werden insbesondere die Informationen zur Nutzung der Attribute verwaltet. Damit kann der Bürger eine Übersicht gewinnen, welche Informationen von welchen Dienstanbietern genutzt werden.
Dienstanbieter	Es werden Informationen verwaltet, die aufzeigen welche Attribute einer Prüfung unterzogen wurden, das Ergebnis der Prüfung und die weitere Verwendung.
Attribut-Zertifizierer	Das Reporting Data Repository des Attribut-Zertifizierers unterliegt besonders hohen Anforderungen hinsichtlich der Integrität und Vertraulichkeit der verwalteten Informationen. Jederzeit muss der eindeutige Nachweis erbracht werden können wann und auf welcher Informationsgrundlage ein Attribut zertifiziert wurde.

5.2.1 Reporting Service

Die Datenquellen für die verfügbaren Berichte bilden das Identity Attribute Repository, das Reporting Repository und das Authorization Data Repository. Der Reporting Service startet in festgelegten Intervallen oder nach Anfrage standardisierte oder individuell definierbare Berichte. Diese werden über den Service abgerufen und visualisiert. Der Service bildet ein wichtiges Element, um Vertrauen aufzubauen und zu erhalten, da damit die Nutzung der Attribute nachvollzogen werden kann.

Die Entitäten stellen dabei unterschiedliche Berichte zur Verfügung, z.B.: der Reporting Service des Anwenders.

- welche Attribute können von welchen Dienstanbietern eingesehen werden
- welche Attribute wurden von den Dienstanbietern verwendet
- welche Berechtigungen sind auf den Attributen vergeben
- welche Regeln und Rollen sind definiert

Die verfügbaren Berichte beim Dienstanbieter und beim Attribut-Zertifizierer können vom Anwender angefordert und eingesehen werden. Es wird dabei gewährleistet, dass der Benutzer nur seine Informationen über den Bericht einsehen kann.

Entität	Spezifische Ausprägung
Anwender / Bürger	Mittels des Reporting Service können auch individuelle Berichte auf der Basis der Daten in den Repositories erstellt werden. Die Reports können im Repository abgelegt werden.
Dienstanbieter	Stellt standardisierte Berichte zur Verfügung wie z.B.: • Report über gespeicherte Attribute für einen Anwender • Report über die Nutzung der Attribute eines Anwenders Die Vertraulichkeit, Integrität der Informationen wird sichergestellt.
Attribut-Zertifizierer	Stellt standardisierte Berichte zur Verfügung wie z.B.: • Report über für den Benutzer zertifizierte Attribute • Report über die Identitäten, die eine Prüfung eines Attributs des Benutzers anstießen. Die Vertraulichkeit, Integrität der Informationen wird sichergestellt.

5.2.2 Logging Service

Über den Logging Service werden definierte Ereignisse zum Zeitpunkt ihres Eintretens protokolliert. Solche Ereignisse sind z.B.

- die Durchführung einer Status- und Konfigurationsänderungen,
- der Empfang bzw. das Versenden von Events,
- die Anforderung, die Übermittlung und Nutzung eines Attributs,
- der Start von Workflows und Aktionen
- die Nutzung des Dienstes
- Fehlermeldungen z.B. bei der Authentisierung, beim Zugriff auf ein Attribut
- Aktionen des Nutzers oder eines Dienstanbieters innerhalb eines Workflows

Über den Reporting Service kann der Anwender einen Überblick über die durchgeführten Aktionen erhalten.

Entität	Spezifische Ausprägung
Anwender / Bürger	Die zu protokollierenden Aktionen können vom Anwender selbst frei definiert werden. Das Logging wird automatisiert, nachvollziehbar und sicher durchgeführt.
Dienstanbieter	Ein Grundmenge an zu protokollierten Aktionen (die Anforderung, Verwendung, ggf. Weiterleitung, Aktualisierung und Löschung von Benutzer-Attributen) werden dem Dienstanbieter vorgegeben. Weitere Aktionen können frei definiert werden. Das Logging wird automatisiert, nachvollziehbar und sicher durchgeführt.
Attribut-Zertifizierer	An den Logging Service werden sehr hohe Anforderungen hinsichtlich der Integrität gestellt. Insbesondere die Durchführung einer Zertifizierung eines Benutzer-Attributes und die Prüfung und deren Ergebnis müssen revisionssicher protokolliert werden.

5.2.3 Monitoring Service

Der Monitoring Service dient der Überwachung vorab definierter Schwellwerte. Ist ein Schwellwert erreicht, so wird ein Event angestoßen und z.B. der Anwender informiert oder ein lokaler oder übergreifender Workflow initiiert.

Entität	Spezifische Ausprägung
Anwender / Bürger	Die überwachte Schwellwerte können z.B. sein: • die Anzahl der Weiterleitungen eines Attributes an andere Dienstanbieter • die Anzahl der Zugriffe/ Nutzung eines Attributs • der Gültigkeitszeitraum eines Attributs • die Änderung eines Attributs
Dienstanbieter	Die überwachte Schwellwerte können z.B. sein: • die Anzahl fehlerhafter Zertifizierungsversuche • die Anzahl fehlerhafter / ausgelaufener Anfragen für Attribute • die Anzahl fehlerhafter Login Versuche
Attribut-Zertifizierer	Der Monitoring Service dient der Überwachung vorab definierter Schwellwerte, wie z.B. • die Anzahl der Anfragen ein Attribut zu zertifizieren • die Anzahl der Prüfungen eines Attributs

5.3 Authorization Data Repository

Das User Authorization Repository dient als Datenspeicher für die definierten Berechtigungen und Zugriffsregeln einer Entität.

Weiterführende Informationen über die anwendungsspezifischen Berechtigungsstrukturen (Application Access Control Structure, AACS) aus den genutzten Systemen / Anwendungen des Dienstanbieters bzw. des Attribut-Zertifizierers werden im Authorization Data Repository gespeichert, z.B. Informationen über SAP-Rollen oder Gruppen im MS Active Directory.

Zusätzlich werden beschreibende Informationen wie, welche Zugriffsmöglichkeiten mit einer Berechtigung bzw. Policy ausgeübt werden können dokumentiert. Diese Informationen sind wichtig für den Anwender bzw. allgemein für Personen, die Zugriffsberechtigungen anschließend vergeben, um Transparenz zu schaffen.

Entität	Spezifische Ausprägung
Anwender / Bürger	Im Repository werden die Berechtigungen auf einzelne Attribute und die definierten Zugriffsregeln verwaltet.
Dienstanbieter	Informationen über AACS und die definierten Zugriffsregeln werden system- bzw. anwendungsübergreifend verwaltet.
Attribut-Zertifizierer	Informationen über AACS und die definierten Zugriffsregeln werden system- bzw. anwendungsübergreifend verwaltet.

5.3.1 AACS Management Service

Unter Application Access Control Structure (AACS) versteht man eine anwendungsspezifische Struktur mit Hilfe der man Berechtigungen auf verwaltete Informationen vergeben kann. Üblich sind Strukturen wie Rollen (SAP Rolle) oder Gruppen (MS Active Directory).

In diesem Service werden die Berechtigungsstrukturen einer Anwendung definiert, gepflegt und gelöscht. Zusätzlich verwaltete Informationen werden genutzt, um den Einsatzzweck einer Berechtigungsstruktur näher zu beschreiben. Die Berechtigungen werden durch die jeweilige Entität selbstständig definiert, entwickelt und verantwortet.

Systeme und Anwendungen insbesondere beim Dienstanbieter können komplexe Berechtigungsstrukturen besitzen. Der AACS Management Service kann für jede eingesetzte Applikation oder jedes System spezifisch ausgeprägt sein.

Entität	Spezifische Ausprägung
Anwender / Bürger	Der Service verwaltet und prüft die vom Anwender definierten Zugriffs- bzw. Nutzungsberechtigungen auf Attribute. Alle abgelegten Attribute können mit Zugriffsberechtigungen versehen werden z.B. • Leseberechtigung für Dienstanbieter o frei, o bei Zugriff immer fragen oder o kein Zugriff

Entität	Spezifische Ausprägung

	• Weitergabe der Informationen
	  o erlaubt
	  o nicht erlaubt
	• Zeitraum der Gültigkeit des Attributes
	• Nutzungszeitraum
	  o für einen Dienstanbieter
	  o generell für alle
	Stellt ein Dienstanbieter die Anfrage ein Attribut übermittelt zu bekommen, so prüft der AACS Management Service, ob diese auf der Basis der definierten Berechtigungen zulässig ist. Ist das Resultat der Prüfung positiv wird die Information übergeben. Im anderen Fall erfolgt eine entsprechende Statusmeldung.

Dienstanbieter	Die Ausprägung des AACS Management Service hängt direkt von den eingesetzten Systemen bzw. Anwendungen ab. Grundsätzlich werden über diesen Service die Zugriffsberechtigungen der Anwender auf Informationen und Dienstleistungen gesteuert.
Attribut-Zertifizierer	Der Zugriff auf Informationen des Attribut-Zertifizierers wird über den AACS Management Service gesteuert. Die Granularität der erforderlichen AACS Strukturen ist von den zu zertifizierenden Attributen abhängig.

5.3.2 Policy Management Service

Eine Policy (Regel) dient zum einem dazu mehrere AACS Strukturen zu bündeln. Zum Anderen können Regeln dynamisch und damit automatisiert auf die AACS Strukturen angewandt werden, um damit das Management von Zugriffsberechtigungen zu vereinfachen und effektiver zu gestallten.

Am Beispiel eines Dienstanbieters kann dieses Prinzip erläutert werden. Nutzer eines Dienstanbieters benötigen z.B. unterschiedliche Berechtigungen auf drei Systemen (Portal, ERP System und Datenbank). Diese Berechtigungen werden in einer Policy „Standard Benutzer“ zusammengefasst. Neuen Anwendern muss nur noch diese Policy zugewiesen werden. Die Anlage der Benutzerkonten und die Verteilung der Berechtigungen wird über den Provisioning Service (siehe Kapitel 5.1.5) durchgeführt.

Durch eine Anforderung aus den Geschäftsprozessen sollen mehrere Benutzer auf einer Informationsbasis zusammenarbeiten können. Dazu wird für jede Benutzergruppe ein eigenständiger Buchungskreis eingerichtet. Der relevante Buchungskreis eines Anwenders wird in einem Attribut abgelegt, welches nur vom Dienstanbieter verwaltet wird. Durch eine automatisierte Regel wird nun dem Benutzer die Policy „Standard Benutzer_<Buchungskreis>“ zugewiesen. Damit kann ohne manuelle Interaktion die korrekte Berechtigung, unter Nutzung des Provisioning Service, verteilt werden.

Die Policies werden von Entitäten eigenständig definiert, entwickelt und verantwortet.

Entität	Spezifische Ausprägung
Anwender / Bürger	Für die im Identity Attribute Data Repository abgelegten Attribute kann der Anwender Policies definieren, um die Berechtigungsvergabe zu vereinfachen. Dazu können festgelegte Policies wie z.B. Bank, Internetshop, Behörde oder Vertrauensstufen genutzt werden: • Vertrauensstufe offen: z.B. Name und Adresse • Vertrauensstufe hoch: Kreditkartennummer, Bankdaten • Vertrauensstufe sehr hoch: Behindertenstatus
Dienstanbieter	Die Ausprägung der Policies hängt direkt von den eingesetzten Systemen bzw. Anwendungen und vom Dienstleistungsspektrum ab.
Attribut-Zertifizierer	Die Ausprägung der Policies hängt direkt von den zu zertifizierenden Attributen und den gespeicherten Informationen ab.

5.4 Fazit

In diesem Abschnitt wurde eine Rahmenarchitektur eines bürgerfreundlichen Identitätsmanagements auf der Basis des Prozess- und Informationsmodells definiert und beschrieben. Die erforderlichen Services zur Umsetzung werden für alle drei Entitäten (Anwender/Bürger; Dienstanbieter; Attribut-Zertifizierer) in ähnlicher Weise benötigt. Der spezifische Funktionsumfang der Services unterscheidet sich anschließend zwischen den Entitäten.

In den Repositories (Identity Attribute, Reporting und Authorization Data) werden die erforderlichen Informationen entsprechend den Anforderungen verwaltet und bilden die Grundlage für die Funktion der Services. Insbesondere durch den Authentication Service, der die Identifizierung und Authentisierung der Anwender stark vereinfacht und automatisiert wird die Bürgerfreundlichkeit erreicht.

Über den Attribute Certification Service können beliebige Informationen des Bürgers an den Dienstanbieter automatisiert übergeben werden. Dabei ist besonders für den Bürger ausschlaggebend, dass er weiterhin die Kontrolle über seine Informationen besitzt, d.h. er kann diese Informationen jederzeit zurückziehen. Die Aktualität der Informationen ist gewährleistet, da anwenderspezifische Daten nur an einer Stelle verwaltet werden (im Identity Attribute Data Repository des Anwenders). Änderungen (z.B. Bankverbindung) werden bei Bedarf automatisiert an alle Dienstanbieter, die diese Information nutzen weitergeleitet. Der Reporting Service erlaubt eine einfache Erstellung von Berichten, z.B. die Verwendung der Attribute des Bürgers durch Dienstanbieter.

Durch diese Eigenschaften wird zum einen eine hohe Bürgerfreundlichkeit erreicht zum

anderen auch Vertrauen in die Architektur und damit in die nachfolgende technische Lösung. Ohne das Vertrauen der Bürger wird sich eine solche Lösung nicht am Markt durchsetzten können.

Im nächsten Kapitel werden mittels einer Prozesslandkarte die für ein bürgerfreundliches Identitätsmanagement notwendigen Prozesse dargestellt.

6. Identitätsmanagement - Unternehmenszentriert versus Anwenderzentriert

Digitale Identitäten werden in einem initialen Schritt erzeugt und müssen anschließend sicher und konsistent verwaltet werden, d.h. Änderungen wie ein Wechsel des Nachnamens bei einer Heirat müssen identifiziert und nachvollzogen werden. Wird die Digitale Identität nicht mehr benötigt, so wird sie entsprechend den organisatorischen Anforderungen und den Rahmenbedingungen deaktiviert bzw. gelöscht.

Ein Identitätsmanagement-Dienst besteht aus verschiedenen Komponenten (siehe Kapitel 4 Prozess- und Informationsmodell), um in der digitalen Welt die beteiligten Akteure und Systeme in ihrer sicheren Kommunikation zu unterstützen.

Diese Grundsätze gelten sowohl für die unternehmens- als auch für die anwenderzentrierte Sicht.

- In der **unternehmenszentrierten** Sicht ist es das Ziel, alle verwalteten Attribute in einer Digitalen Identität zentral im Sinne des Unternehmens zu verwalten. Ein Attribut kann unterschiedlichste Inhalte enthalten, z.B. den Vor- / Nachnamen des Anwenders, organisatorische Informationen (Büronummer, Stockwerk, Telefonnummer) aber auch Benutzerkonten und deren Berechtigungen in den unterschiedlichen Anwendungen.
- In der **anwenderzentrierten** Sicht ist es das Ziel, die unterschiedlichen Attribute eines Anwenders grundsätzlich zu trennen, so dass die für eine Anwendung erforderlichen Informationen für andere Dienstanbieter nicht zugreifbar sind und damit der Datenschutz gewährleistet ist.

Um diese Unterscheidung auszuarbeiten, werden im nächsten Kapitel die beiden Sichten miteinander verglichen. Als Basis für den Vergleich dienen die verschiedenen Funktionen, die das Identitätsmanagement betreffen:

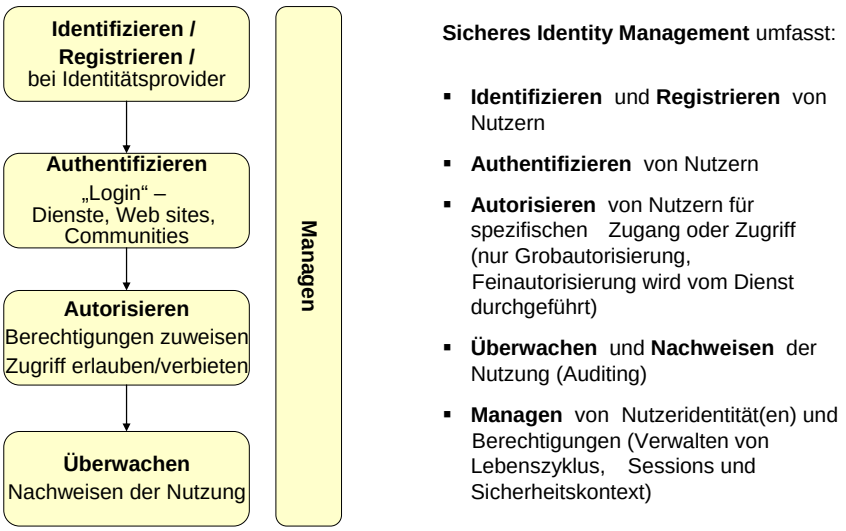


Abbildung 8: Funktionen des Identitätsmanagements

Jede der Funktionen beinhaltet verschiedene Prozesse des Identitätsmanagements. Am Beispiel der Prozesslandkarte von CSC (siehe Abbildung 9) werden diese Funktionen in Prozesse gegliedert.

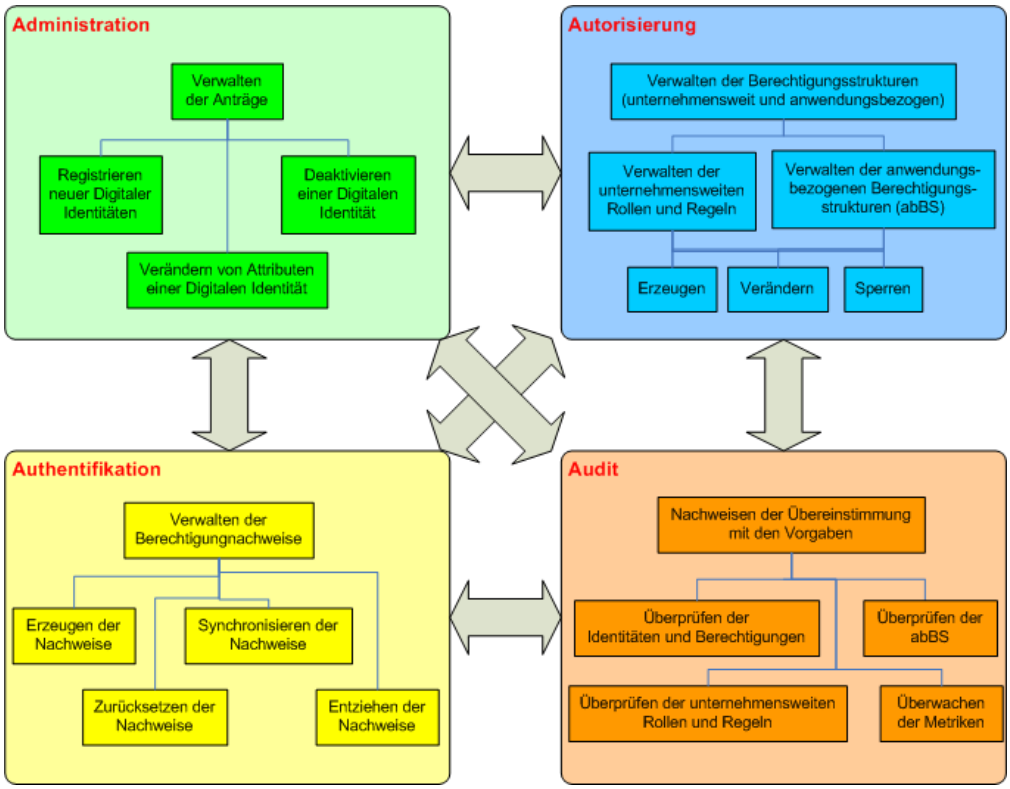


Abbildung 9: Prozesslandkarte (Quelle: CSC)

Die vier Funktionen Administration, Autorisierung, Authentifikation und Audit werden in einer unternehmens- als auch in einer anwenderzentrierten Sicht für eine nachhaltige Verwaltung digitaler Identitäten benötigt. Die Ausprägung der einzelnen Prozesse ist in den beiden Sichten zum Teil unterschiedlich.

Bei der unternehmenszentrieren Sicht wird von einem idealen Unternehmen ausgegangen, in dem ein zentrales Werkzeug zur Verwaltung der Digitalen Identitäten (Identity Management Lösung) zur Verfügung steht und die erforderlichen Prozesse vollständig umgesetzt sind.

In den folgenden Kapiteln werden die beiden Ausprägungen gegenübergestellt. Für die anwenderzentriete Sicht wird der heutige Umsetzungsstand dargestellt und anschließend die Zukünftige Implementierung eines bürgerfreundlichen Identitätsmanagements entworfen.

6.1 Administration

6.1.1 Registrierung neuer Digitaler Identitäten

Unternehmenszentrierte Sicht: Mitarbeiter eines Unternehmens benötigen für ihre Aufgabenerfüllung eine Digitale Identität. In dieser Identität, repräsentiert durch ein eindeutiges Kennzeichen („unique identifier“), werden zahlreiche Attribute wie z.B. Vor- / Nachname, organisatorische Informationen, Benutzerkonten und Berechtigungen in

Anwendungen zentral verwaltet. Das benutzte Schema zur Erzeugung der unternehmensweit eindeutigen Kennung kann variieren. Die grundlegende, von allen Mitarbeitern benötigte Digitale Identität, kann nach der Unterschrift des Arbeitsvertrages durch den neuen Mitarbeiters automatisiert erstellt werden. Anschließend werden die Zugriffe auf Anwendungen auf der Basis der zukünftigen Funktion (Rolle) im Unternehmen ermöglicht. Die hierzu erforderlichen Attribute (d.h. Kennungen und Berechtigungen) werden in der Digitalen Identität des Anwenders verwaltet.

	Beschreibung
Auslöser	Neuer Mitarbeiter unterschreibt seinen Anstellungsvertrag Externer benötigt Zugriff auf IT-Anwendungen des Unternehmens

Anwenderzentrierte Sicht:

Heute: Eine Person möchte eine Dienstleistung über ein Internetportal in Anspruch nehmen. Dazu muss sich der Anwender in der Regel vor der Nutzung registrieren, d.h. ein Benutzerkonto beim Dienstanbieter beantragen. Die dazu erforderlichen Informationen werden vom Dienstanbieter vorgegeben. Mindestens muss ein Benutzername und ein entsprechendes Passwort vorgegeben werden. Für andere Dienstleistungen (z.B. eBay, Amazon) sind auch weiterführende Informationen wie z.B. die aktuelle Adresse, Bankverbindungs-/Kreditkartendaten anzugeben. Die übermittelten Daten werden u.U. vom Dienstanbieter validiert. Nach erfolgreicher Registrierung kann die Person das Angebot des Dienstanbieters nutzen. Die übermittelten Informationen werden i.d.R. vom Dienstanbieter gespeichert und genutzt.

Ein Dienstanbieter erstellt für jeden Nutzer ein eigenständiges Benutzerkonto. Ein Anwender kann mehrere, unabhängige Benutzerkonten für sich beim Dienstanbieter anlegen, da nicht immer ein eindeutiges Kennzeichen definiert werden kann. Möchte ein Dienstanbieter die Mehrfachnutzung verhindern, so kann er dies über die Geschäftsbedingungen ausschließen oder über mehrere Attribute (Name, Geburtsort und Geburtsdatum) ein eindeutiges Kennzeichen ableiten.

Zukunft: Mit dem Zugang zum Internet bzw. mit der ersten Transaktion des Anwenders im Internet entsteht seine Digitale Identität. Die Art der im ersten Schritt anzugebenen Attribute hängt direkt von der Art des Internetzugangs ab. Bei anonymen Zugängen wie z.B. in einem Internetcafé wird zumindest die IP-Adresse des genutzten Rechners aufgenommen. Bei einem privaten Zugang gehören zusätzliche Attribute wie Anschlusskennung, Adresse und Bankverbindung zur Digitalen Identität des Anwenders.

Durch weitere Transaktionen wächst die Digitale Identität des Anwenders laufend an. Dies wird über den Prozess „Veränderung der Attribute“ gesteuert.

	Beschreibung
Auslöser	Anwender greift auf das Internet zu, da er eine Dienstleistung nutzen will.
Anforderungen	
P-A1.	Geringer Aufwand bei der Initialisierung und Registrierung
P-A2.	Vertrauenswürdiger Verwaltung aller der Digitalen Identität zugeordneten Attribute.

P-A3.	Problemlose Nutzung mit unterschiedlichen Geräten

6.1.2 Veränderung von Attributen einer Digitalen Identität

Unternehmenszentrierte Sicht: Die Attribute in der Digitalen Identität eines Anwenders unterliegen einer laufenden Veränderung. Wechselt ein Mitarbeiter in einem Unternehmen seinen Arbeitsplatz (z.B. Raumnummer, Telefonnummer), wird eine Umorganisation durchgeführt (z.B. Wechsel der Organisationsbezeichnung) oder ändert sich durch z.B. eine Heirat sein Nachname, müssen diese Informationsänderungen in den Attributen nachvollzogen werden.

In den Attributen werden auch die Rollen und die darin enthaltenen Berechtigungen des Anwenders in Anwendungen verwaltet. Ein Unternehmen nutzt in der Regel eine Vielzahl von unterschiedlichen Systemen / Anwendungen, um Geschäftsprozesse elektronisch zu unterstützten. Diese verwalten den Zugang und die Berechtigungen für Anwender meist eigenständig. Benötigt ein Benutzer Zugriff auf eine Anwendung, so muss er diesen beantragen. Wird dem Antrag zugestimmt, so erhält der Benutzer eine zusätzliche Kennung und die entsprechende(n) Rolle(n).

Änderungen an der Rollenzuordnung (Hinzufügen / Löschen) müssen aufgrund gesetzlicher Rahmenbedingungen nachvollziehbar dokumentiert werden. Die genehmigten Rollen werden in der Digitalen Identität des Anwenders aufgeführt.

	Beschreibung
Auslöser	Änderung des Arbeitsplatzes des Mitarbeiters Änderung an organisatorischen Informationen, z.B. Name des Mitarbeiters Mitarbeiter erhält ein zusätzliches Aufgabengebiet Mitarbeiter erweitert/verringert seinen Aufgabenbereich Änderung der Unternehmensorganisation und damit der Aufgabengebiete Änderung der Unternehmensorganisation Funktionserweiterung innerhalb eines Systems / einer Anwendung

Anwenderzentrierte Sicht:

Heute: Durch einen Umzug des Anwenders oder durch eine Änderung z.B. der E-Mail Adresse sind die Informationen der bei den Dienstanbietern definierten Benutzerkonten nicht mehr korrekt. Eine automatisierte Aktualisierung findet nicht statt. In der Regel wird die Anpassung bei Bedarf durch den Benutzer durchgeführt, d.h. wenn er die Dienstleistung wieder in Anspruch nehmen will und er den Aktualisierungsbedarf erkennt. Dabei muss jedes Benutzerkonto separat vom Anwender aktualisiert werden.

Berechtigungen für Anwender werden in der anwenderzentrierten Sicht vom Dienstanbieter innerhalb einer bzw. mehrerer Applikationen definiert und verwaltet. Diese Informationen werden beim Dienstanbieter lokal in dem Benutzerkonto des Anwenders abgelegt und sind für den Anwender nicht transparent.

Zukunft: Ein Anwender kann selbst die Informationen z.B. Adresse oder Bankverbindung in den Attributen seiner Digitalen Identität bei Bedarf aktualisieren oder neue Attribute hinzufügen/wegnehmen. Nutzt der Anwender eine Dienstleistung im Internet, so kann die Anwendung auf die für sie freigegebenen Attribute zugreifen

und ihre Daten aktualisieren. Damit stehen dem Anwender und dem Dienstanbieter in der Applikation immer die aktuellen Informationen zur Verfügung.

Möchte ein Anwender eine neue Dienstleistung in Anspruch nehmen, so können verschiedene Wege für den Anwender offen stehen. Im ersten Fall kann er den Dienst anonym nutzen. Er benötigt kein Benutzerkonto. Im zweiten Fall gibt der Anwender temporär die erforderlichen Informationen dem Dienstanbieter. Dieser verwendet die Informationen nur für diese Nutzung. Anschließend werden die Informationen vom Dienstanbieter gelöscht.

Im letzen Fall fordert der Dienstanbieter einen personalisierten Zugriff auf den Dienst. Der Anwender leitet zunächst einen Registrierungsprozess ein. Der Dienstanbieter gibt dem Anwender die zur Anmeldung erforderlichen Informationen vor z.B. Adresse, Bankverbindung. Nach einer erfolgreichen Authentisierung des Dienstanbieters durch den Anwender erteilt dieser dem Dienstanbieter die Berechtigung für den Zugriff auf die bereits in seiner Digitalen Identität enthaltenen Informationen. Ist eine Information noch nicht vorhanden, so wird diese in die Digitale Identität des Anwenders neu aufgenommen. Die erforderlichen Daten werden anschließend automatisiert dem Dienstanbieter präsentiert. Nach einer Prüfung beim Dienstanbieter wird der Registrierungsprozess abgeschlossen und die entsprechenden Informationen über den neuen Dienstanbieter in die Digitale Identität aufgenommen.

Über die automatisiert gefüllten Attribute in der Digitalen Identität kann der Anwender erkennen, welche Dienstanbieter er innerhalb einer definierten Zeitspanne genutzt hat bzw. welche Dienstanbieter Informationen angefordert haben. Deaktiviert oder löscht der Anwender einen Eintrag in seiner Digitalen Identität bzw. entzieht er dem Dienstanbieter eine Berechtigung, so wird dieser automatisiert informiert. Der Dienstanbieter kann dann entsprechend reagieren, in dem er z.B. das Benutzerkonto deaktiviert bzw. löscht.

Die einzelnen Berechtigungen des Anwenders innerhalb der Anwendung werden weiterhin vom Dienstanbieter in den Applikationen verwaltet.

	Beschreibung
Auslöser	Änderung des Familiennamens Wechsel des Wohnortes und damit der Adresse Änderung von personen-/behördenabhängigen Identitätskennzeichen (Steuernummer, Kreditkarte, Passnummer, Bankdaten) Neue Funktionen bei Behörden / Unternehmen werden freigeschaltet Nutzung einer weiteren Dienstleistung Neues Interessengebiet des Nutzers Neues Aufgabengebiet des Nutzers, z.B. zusätzliche Zertifizierung wie Steuerberater, Notar
Anforderungen	
P-A4.	Zentrale Verwaltung für mehrfach genutzte Informationen (für Nutzer)
P-A5.	Kein Zugriff auf diese Informationen ohne die explizite Zustimmung durch den Nutzer (Zugriffsberechtigung wird auf einzelne Attribute vergeben)

	Beschreibung
P-A6.	Auf die vollständige Sammlung der Attribute hat niemand – außer dem Anwender selbst – Zugriff.
P-A7.	Automatische Aktualisierung dieser Daten in genutzten Anwendungen
P-A8.	Einheitlicher Weg zur Erweiterung der Berechtigungen
P-A9.	Übersicht über vergebene Berechtigungen auf Informationen in der Digitalen Identität des Anwenders
P-A10.	Weltweiter Zugriff auf die in der Digitalen Identität verwalteten Attribute, 24x7x365
P-A11.	Vergeben von Vollmachten an Dritte (zeitgesteuert, für welche Aktionen, ...)
P-A12.	Single Point of Contact (SPoC) für die Berechtigungen

6.1.3 Deaktivierung bestehender Identitäten

Unternehmenszentrierte Sicht: Verlässt ein Mitarbeiter das Unternehmen, muss seine Digitale Identität im Unternehmen und damit alle seine Zugriffsmöglichkeiten zum Zeitpunkt seines Austritts deaktiviert, ggf. archiviert und gelöscht werden. Unter Umständen müssen bei einzelnen Systemen / Anwendungen Aufräumarbeiten durchgeführt werden, um unternehmensrelevanten Informationen zu identifizieren und geregelt abzulegen oder zu übergeben. Als Beispiele kann das Homelaufwerk oder das E-Mail-Postfach des Mitarbeiters genannt werden.

	Beschreibung
Auslöser	Mitarbeiter verlässt das Unternehmen (Kündigung/Ruhestand) Tod des Mitarbeiters Fristlose Kündigung

Anwenderzentrierte Sicht:

Heute: Benötigt ein Anwender eine Dienstleistung nicht mehr, so deaktiviert er in der Regel das hierfür beim Dienstanbieter angelegte Benutzerkonto nicht. Der Anwender nutzt die Dienstleistung einfach nicht mehr.

Ein Anwender hat nur dann ein Interesse an der (zeitnahen) Deaktivierung eines nicht mehr benötigten Benutzerkontos, falls Kosten für ihn anfallen. Beim Dienstanbieter häufen sich demnach veraltete bzw. nicht mehr genutzte („verwaiste“) Identitäten an.

Zukunft: Die Digitale Identität eines Anwenders kann nicht gelöscht werden und bleibt zumindest in Grundzügen bis über seinen Tod hinaus bestehen. Benötigt ein Anwender auf eine Dienstleistung keinen Zugriff mehr, so setzt er die entsprechenden Berechtigungen für den Dienstanbieter und Attribute inaktiv. Auch der Dienstanbieter kann aktiv Attribute, die in der Digitalen Identität des Anwenders enthalten sind zurückziehen.

Damit werden nur Attribute seiner Digitalen Identität deaktiviert (siehe Prozess „Veränderung der Attribute“).

	Beschreibung
Auslöser	Kein Ereignis kann die Digitale Identität löschen
Anforderungen	keine

6.2 Autorisierung

6.2.1 Verwalten der anwendungsbezogenen Berechtigungsstrukturen

Unternehmenszentrierte Sicht: Innerhalb der Anwendungen werden mit unterschiedlicher Granularität Berechtigungskonzepte definiert und umgesetzt. Dabei müssen vorgegebene Rahmenbedingungen beachtet werden, z.B. wie innerhalb der Anwendung Berechtigungen eingesetzt und geprüft werden können. Über anwendungsbezogene Berechtigungsstrukturen (z.B. SAP Rollen oder LDAP Gruppen) werden Berechtigungen einem Anwender zugewiesen.

Änderungen an bestehenden Berechtigungsstrukturen können große Auswirkungen hinsichtlich der aktiven Berechtigungen für die Anwender bewirken. Aus diesem Grund müssen definierte Prozesse eingehalten werden, um die konsistente Erstellung und Pflege anwendungsbezogener Berechtigungsstrukturen zu gewährleisten.

	Beschreibung
Auslöser	Durchführung von organisatorischen Änderungen Änderungen in den Geschäftsprozessen Einführung neuer Anwendungskomponenten Erweiterung des Aufgabengebiets einzelner Anwender

Anwenderzentrierte Sicht:

Heute: Die Übermittlung von Anwenderinformationen (z.B. Adresse, Bankdaten) an einen Dienstanbieter wird vom Anwender manuell gesteuert, d.h. er gibt bestimmte Informationen in ein Abfrageformular ein oder nicht. Für jeden einzelnen Dienstanbieter kann der Anwender die entsprechende Entscheidung neu treffen.

Zukunft: Informationen wie z.B. Adresse, Bankdaten sind in den Attributen der Digitalen Identität des Anwender abgelegt. Über granulare Berechtigungen z.B.

- Leseberechtigung,
- bei Zugriff fragen,
- kein Zugriff,
- Weitergabe der Informationen erlaubt
- Weitergabe der Informationen nicht erlaubt

kann er den Zugriff eines Dienstanbieters auf diese Daten gezielt steuern.

Den Aktionsumfang, d.h. welche Funktionen der Anwender beim Dienstanbieter nutzen kann, wird auch in Zukunft durch den Dienstanbieter in der jeweiligen Anwendung verwaltet.

	Beschreibung
Auslöser	Anwender möchte mehr / weniger Information dem Dienstanbieter übermitteln Dienstanbieter fordert mehr / weniger Information vom Anwender ein
Anforderungen	
P-A13.	Übergebene Information wird vom Dienstanbieter sicher verwaltet
P-A14.	Zurückgezogene Informationen werden vom Dienstanbieter verbindlich gelöscht
P-A15.	Zugriffsberechtigungen können zeitlich befristet werden

6.2.2 Verwalten der unternehmensweiten Rollen und Regeln

Unternehmenszentrierte Sicht: Ist in einem Unternehmen eine effektives Identitätsmanagement implementiert, so erhält ein Anwender die für sein Aufgabengebiet erforderlichen Berechtigungen über die Zuweisung einer oder mehrerer unternehmensweiter Rolle(n). In dieser Rolle sind Zugriffsberechtigungen auf Systeme und Anwendungen enthalten, die für die Aufgabenerfüllung des Nutzers erforderlich sind.

In diesem Prozess werden die Neuerstellung und die Pflege des gesamten unternehmensweiten Rollensets innerhalb des Unternehmens durchgeführt.

	Beschreibung
Auslöser	Durchführung von organisatorischen Änderungen Verschiebung von Aufgaben innerhalb der Unternehmensorganisation Veränderung der Geschäftsprozesse Integration neuer bzw. Ablösung von Systemen / Anwendungen / Komponenten zur Unterstützung der Geschäftsprozesse

Anwenderzentrierte Sicht:

Heute: eine Entsprechung des Prozesses existiert nicht.

Zukunft: Bestimmte Informationen wie z.B. Bank-/Kreditkartendaten werden von einer großen Zahl von Dienstanbietern zur Kostenverrechnung erhoben. Diese Informationen zusammen mit den Nutzern (d.h. den Dienstanbietern) können gruppiert werden und bilden eine Rolle.

Existiert z.B. eine Rolle „Bankdaten Gehaltskonto“ beim Anwender, erhalten alle darauf berechtigten Dienstanbieter die definierten aktuellen Informationen. Rollen können auch verschachtelt werden.

	Beschreibung
Auslöser	Veränderte Nutzung des Dienstes durch den Anwender Veränderte Vorgaben durch den Dienstanbieter
Anforderungen	
P-A16.	Einfache, transparente Verwaltung durch den Anwender
P-A17.	Protokollierung der Zugriffe auf Daten

6.3 Authentifikation

6.3.1 Erzeugen der Nachweise

Unternehmenszentrierte Sicht: Wird ein neues Benutzerkonto in einer Anwendung erstellt (siehe „Registrierung neuer Identitäten“), so muss ein Identitätsnachweis (z.B. ein Passwort) definiert und dem Mitarbeiter sicher übermittelt werden. Als Identitäts-nachweise können neben Passwörtern auch Softwarezertifikate, Hardwaretoken (RSA Secure ID) oder Smart Cards genutzt werden.

	Beschreibung
Auslöser	Neuanlage eines Benutzerkontos Vermutung, dass der Nachweis (z.B. eines Token) kompromittiert wurde

Anwenderzentrierte Sicht:

Heute: Benötigt ein Anwender Zugriff auf eine Dienstleistung, muss nach einer Registrierung (siehe „Registrierung neuer Identitäten“) ein Identitätsnachweis erstellt werden. Werden hierzu Passwörter genutzt, so kann der Benutzer dieses Passwort meist bei der Registrierung selbst definieren. Im anderen Fall erhält er durch den Dienstanbieter ein Initialpasswort, welches er bei der ersten Anmeldung ändern muss.

Weitere unterschiedliche Arten der Nachweise z.B. HBCI, PIN/TAN Verfahren (siehe Unternehmenszentrierte Sicht) sind möglich. Der Identitätsnachweis muss vom Anwender selbst sicher verwaltet werden.

Zukunft: Der nach einer erfolgreichen Authentisierung und Registrierung übermittelte Identitätsnachweis wird in der Digitalen Identität verwaltet und geschützt. Dabei muss der Anwender keine Informationen liefern. Der Nachweis wird automatisiert zwischen den beiden Parteien (Anwender und Dienstanbieter) ausgehandelt. Nach dem erfolgreichen Durchlaufen des Prozesses wird der Anwender entsprechend informiert.

Nutzt ein Anwender einen Dienst, so wird die Authentisierung entsprechend der Kritikalität der genutzten Anwendung entweder automatisiert (nicht kritisch) oder über die Abfrage einer PIN Nummer zur Freigabe der Informationen (kritisch) zwischen Digitaler Identität und dem Dienst automatisiert durchgeführt.

	Beschreibung
Auslöser	Neuanlage eines Benutzerkontos Vermutung, dass der Nachweis kompromittiert wurde
Anforderungen	
P-A18.	Einfache Nutzung
P-A19.	Einfache Verwaltung unterschiedlicher Nachweise
P-A20.	Keine zusätzlichen Kosten für Software / Hardware
P-A21.	Verwendung schon bekannter, als vertrauenswürdig eingeschätzter Verfahren (SW/HW)
P-A22.	Möglichst keine manuelle Aktion zur Authentisierung erforderlich
P-A23.	Absicherung des Zugangs zu kritischen Anwendungen über die Abfrage einer PIN

6.3.2 Zurücksetzen der Nachweise

Unternehmenszentrierte Sicht: Erinnert sich ein Anwender nicht mehr an seinen Identitätsnachweis für eine Anwendung oder ist das Benutzerkonto durch Fehleingaben gesperrt, so muss es über einen definierten Weg möglich sein, den Nachweis neu zu initialisieren.

Dabei muss sichergestellt sein, dass nur berechtigte Personen diesen Prozess auslösen und nur der Anwender die Information über den neuen Nachweis erhält. Der Nachweis muss dann vom Anwender bei der ersten erneuten Nutzung auf einen neuen Wert gesetzt werden.

	Beschreibung
Auslöser	Sperrung des Benutzerkontos durch mehrere Fehleingaben Anwender kann sich an Passwort nicht mehr erinnern Interne/gesetzliche Anforderung, um einen Nachweis zurückzusetzen Vermutung, dass der Nachweis kompromittiert wurde

Anwenderzentrierte Sicht:

Heute: Auch in der anwenderzentrierten Sicht gibt es Situationen, in denen der Identitätsnachweis auf einen neuen Wert zurückgesetzt werden muss. Im Unterschied zur unternehmenszentrierten Sicht gibt es keine vertrauenswürdige Stelle wie z.B. der direkte Vorgesetzte, der eine zusätzliche Prüfung der Anforderung übernehmen könnte. Über festgelegte Verfahren (wie z.B. vorgegebene Fragen-Antworten) muss sichergestellt werden, dass die Anforderung zur Rücksetzung des Nachweises wirklich vom Anwender stammt und nur dieser die Information über den neuen Nachweis erhält. Auch hier muss der Anwender bei der ersten Anmeldung den Nachweis neu setzen.

Zukunft: Muss ein Nachweis bei einen Dienstanbieter zurückgesetzt werden, so initiiert der Anwender diesen Prozess. Dies ist eine Funktion, die seine Digitale Identität zur Verfügung stellt. Anschließend wird ein neuer Nachweis zwischen beiden Parteien

ausgehandelt und dieser wieder in der Digitalen Identität des Anwenders gespeichert. Der Anwender wird über den Abschluss des Prozesses informiert. Es ist kein manueller Eingriff des Benutzers erforderlich.

	Beschreibung
Auslöser	Sperrung des Benutzerkontos durch Fehleingaben des Nachweises Anwender kann sich an Passwort / PIN nicht mehr erinnern Interne/gesetzliche Anforderung, um einen Nachweis zurückzusetzen
Anforderungen	
P-A24.	Verfügbarkeit 24x7
P-A25.	Einfache Durchführung
P-A26.	Gleicher Prozessrahmen über alle Dienstanbieter (angepasst an Kritikalität)
P-A27.	Keine zusätzlichen Kosten für Software / Hardware
P-A28.	Verwendung schon bekannter als vertrauenswürdig eingestufter Verfahren (SW/HW)

6.3.3 Synchronisieren der Nachweise

Unternehmenszentrierte Sicht: Ein Anwender in einer Organisation muss in der Regel zahlreiche Identitätsnachweise (Passwörter) für die unterschiedlichen Systeme / Anwendungen verwenden und darf diese entsprechend den internen Sicherheitsvorgaben nicht schriftlich dokumentieren.

Eine Hilfestellung für den Anwender ist die automatische Synchronisation eines (Master)Passwortes zwischen den verbundenen Anwendungen. Hierdurch muss ein Anwender deutlich weniger Passwörter, im optimalen Fall nur noch ein Passwort nutzen. Die Synchronisation der Nachweise ist kein Single Sign-On (SSO) Verfahren, da weiterhin bei der Authentisierung in jeder Anwendung ein Benutzernamen und das Passwort vom Anwender manuell eingegeben werden muss. Über den Prozess wird definiert, wann und in welcher Form die Passwörter synchronisiert werden und wie der Anwender über Erfolg bzw. bei Problemen informiert wird.

	Beschreibung
Auslöser	Passwort wurde in der führenden Anwendung neu gesetzt

Anwenderzentrierte Sicht:

Heute: Die Dienste, die ein Anwender nutzt, werden von unterschiedlichen Anbietern bereitgestellt. Eine Synchronisation von Nachweisen (i.d.R. Passwörter) ist aufgrund der unterschiedlichen eingesetzten Technologien schwer möglich. Derzeit kann nur eine manuelle Synchronisation der Nachweise durch den Anwender durchgeführt werden.

Zukunft: Die Nachweise für die genutzten Dienstanbieter sind in der Digitalen Identität gespeichert. Eine Synchronisation der Nachweise ist in diesem Fall nicht mehr erforderlich.

	Beschreibung
Auslöser	/
Anforderungen	/

6.3.4 Entziehen der Nachweise

Unternehmenszentrierte Sicht: Benötigt ein Nutzer einen Identitätsnachweis nicht mehr oder besteht die Vermutung, dass der Nachweis kompromittiert wurde, so muss dieser entzogen werden. Dies ist insbesondere relevant für zertifikatbasierende Nachweise. Über einen festgelegten Prozess müssen die Nachweise zurückgezogen werden und bei Bedarf neu definiert werden (siehe 6.3.1 Erzeugen der Nachweise).

	Beschreibung
Auslöser	Anwender benötigt Nachweise nicht mehr Vermutung, dass der Nachweis kompromittiert wurde Interne/gesetzliche Anforderung, um einen Nachweis zurückzusetzen

Anwenderzentrierte Sicht:

Heute: Auch in der anwenderzentrierten Sicht wird ein Nachweis entzogen, wenn der Anwender diesen nicht mehr benötigt und den Dienstanbieter darüber informiert bzw. er den Verdacht hat, dass der Nachweis kompromittiert wurde. Über einen definierten Prozess werden die Nachweise zurückgezogen und bei Bedarf neu erstellt (siehe „Erzeugen der Nachweise“). Die Ausprägung des Prozesses ist abhängig vom Dienstanbieter.

Zukunft: Beendet ein Anwender die Zusammenarbeit mit einem Dienstanbieter, so deaktiviert / löscht er das entsprechende Attribut aus seiner Digitalen Identität. Hierdurch wird ein automatisierter Prozess gestartet, der den Nachweis des Anwenders beim Dienstanbieter entzieht.

Befürchtet ein Anwender, dass sein Nachweis kompromittiert wurde, so startet er den Prozess „Zurücksetzen der Nachweise“. Damit wird ein neuer Nachweis für den Anwender erstellt.

	Beschreibung
Auslöser	Anwender benötigt Nachweise nicht mehr Vermutung, dass der Nachweis kompromittiert wurde Interne/gesetzliche Anforderung, um einen Nachweis zurückzusetzen
Anforderungen	

P-A29.	Einfache Verwaltung
P-A30.	Nutzung an jedem Internet-PC
P-A31.	Keine zusätzlichen Kosten für Hardware / Software
P-A32.	Verwendung schon bekannter als vertrauenswürdig eingestufter Verfahren (SW/HW)

6.4 Audit

6.4.1 Überprüfen der Identitäten und Berechtigungen

Unternehmenszentrierte Sicht: Der Gesetzgeber stellt hohe Anforderungen an die Vergabe von Zugriffsberechtigungen. Nur berechtigte Anwender dürfen Zugriff auf Informationen besitzen, die für die Erfüllung ihrer Aufgaben erforderlich sind. Der Genehmigungsprozess muss nachvollziehbar gestaltet sein. Aus diesem Grund müssen in regelmäßigen Abständen die Attribute / Berechtigungen der Anwender in den einzelnen Systemen / Anwendungen überprüft werden.

Ist eine Identity Management Lösung im Einsatz, so kann ein automatisierter Vergleich zwischen Ist-Zustand (dem Anwender zugewiesenen Berechtigungen in der Anwendung) und dem Soll-Zustand (dem Anwender genehmigte Berechtigungen) durchgeführt werden. Wird keine Identity Management Lösung genutzt, findet der Vergleich manuell über Listen statt. Identifizierte Differenzen werden nach festgelegten Prozessen behandelt.

	Beschreibung
Auslöser	Regelmäßiger Turnus der Berechtigungsprüfung für Anwender Durchführung einer unangemeldeten Prüfung Durchführung einer Prüfung, ausgelöst durch ein Ereignis Prüfung durch Wirtschaftsprüfer / interne Revision / IT-Sicherheit

Anwenderzentrierte Sicht:

Heute: Eine Prüfung der definierten Benutzerkonten und der verbundenen Berechtigungen eines Anwenders über alle/eine Vielzahl von Dienstanbietern darf für alle außer dem Anwender selbst aufgrund des Datenschutzes nicht möglich sein.

Ein Dienstanbieter kann für Anwendungen in seinem Verantwortungsbereich prüfen, welche Benutzerkonten und Berechtigungen ein Anwender besitzt und diese ggf. anpassen (z.B. bei Mehrfachanmeldungen).

Ein Anwender hat in der Regel keine Möglichkeiten seine zugewiesenen Berechtigungen bei einem Dienstanbieter zu prüfen, außer die Zuweisung von Berechtigungen ist mit Kosten verbunden. In diesem Falle ist eine Übersicht meist in der Anwendung implementiert.

Zukunft: Der Anwender setzt Berechtigungen auf Attribute in seiner Digitalen Identität ein, um den Zugriff der Dienstanbieter auf diese Informationen zu steuern. Die vergebenen Berechtigungen sollten regelmäßig bzw. bei Bedarf geprüft werden.

Über eine Aufstellung ist ersichtlich, welcher Dienstanbieter auf welche Informationen zugreifen kann. Dies stellt den Ist-Zustand dar. Der Soll-Zustand ist die Meinung des

Anwenders, welcher Dienstanbieter welche Informationen erhalten soll.

	Beschreibung
Auslöser	Fehlen von Berechtigungen Gefühl des Anwenders, dass der Dienstanbieter Datenmissbrauch betreibt Durchführung einer regelmäßige Prüfung
Anforderungen	
P-A33.	Einfache Verwaltung
P-A34.	Gleiche Prozesse über alle Dienstanbieter
P-A35.	Zeitnahe Realisierung der Modifikation von Berechtigungen

6.4.2 Überprüfen der unternehmensweiten Rollen und Regeln

Unternehmenszentrierte Sicht: Der Inhalt von unternehmensweit definierten Rollen (siehe 6.2.2) muss in definierten Intervallen geprüft werden, d.h. es muss der Ist-Zustand mit dem dokumentierten Soll-Zustand abgeglichen werden. Erkannte Differenzen werden über den festgelegten Prozess abgewickelt. Durch diesen Prozess wird sichergestellt, dass nur die für die Aufgabe definierten Berechtigungen in den unternehmensweiten Rollen enthalten sind.

	Beschreibung
Auslöser	Regelmäßiger Turnus für Prüfungen Durchführung einer Prüfung durch interne Revision / IT-Sicherheit / Geschäftsbereich Durchführung einer Prüfung, ausgelöst durch ein Ereignis

Anwenderzentrierte Sicht:

Heute: eine Entsprechung des Prozesses existiert nicht (siehe auch „Verwaltung von unternehmensweiten Rollen und Regeln“).

Zukunft: Die vom Anwender definierten Rollen z.B. „Bankdaten Gehaltskonto“ müssen in regelmäßigen Intervallen vom Anwender auf Korrektheit geprüft werden. Über eine Übersicht muss ersichtlich sein, über welche Rolle welcher Dienstanbieter Zugriff auf welche Informationen in der Digitalen Identität erhält (siehe Prozess „Verwalten der unternehmensweiten Rollen und Regeln“).

	Beschreibung
Auslöser	Fehlen von Berechtigungen Gefühl des Datenmissbrauchs durch Dienstanbieter Durchführung einer regelmäßige Prüfung
Anforderungen	Siehe 6.4.1

6.4.3 Überprüfen der anwendungsbezogenen Berechtigungsstrukturen

Unternehmenszentrierte Sicht: Die aufgebauten Berechtigungsstrukturen innerhalb der Anwendungen, z.B. die SAP Rollen oder Gruppen im LDAP müssen in regelmäßigen Abständen auf Konformität mit dem dokumentierten Soll-Zustand überprüft werden. Werden bei dem Audit Differenzen entdeckt, werden diese entsprechend des definierten Prozesses abgearbeitet.

	Beschreibung
Auslöser	Regelmäßiger Turnus für Prüfungen Durchführung einer Prüfung durch interne Revision / IT-Sicherheit / Geschäftsbereich Durchführung einer Prüfung, ausgelöst durch ein Ereignis

Anwenderzentrierte Sicht:

Heute: Ein Dienstanbieter muss für Anwendungen in seinem Verantwortungsbereich prüfen, ob die definierten Berechtigungen den Soll-Zustand entsprechen. Der Anwender hat i.d.R. keinen Einfluss auf diesen Prozess.

Berechtigungen auf Attribute in der Digitalen Identität des Anwenders werden in der Gegenwart nicht vergeben.

Zukunft: Der Zugriff auf Attribute in der Digitalen Identität des Anwenders wird über Berechtigungen vorgenommen. Ist das Berechtigungsmodell komplex ausgeführt, so muss dieses durch den Anwender in regelmäßigen Intervallen bzw. bei Bedarf gegen den Soll-Zustand geprüft und angepasst werden.

Ist das Berechtigungsmodell einfach, so kann dieser explizite Prozess entfallen, da die zugewiesenen Berechtigungen auf die Anwender bereits im Prozess „Überprüfen der Identitäten und Berechtigungen“ geprüft werden.

	Beschreibung
Auslöser	Fehlen von Berechtigungen Gefühl des Datenmissbrauchs durch Dienstanbieter Durchführung einer regelmäßige Prüfung
Anforderungen	Siehe 6.4.1

6.4.4 Überprüfen der Metriken

Unternehmenszentrierte Sicht: Zur Prüfung der Qualität der Prozesse müssen Metriken definiert und überwacht werden. Mit Hilfe dieser Kennzahlen kann ermittelt werden, ob ein Prozess effektiv abläuft oder ob Korrekturen erforderlich sind. Eine mögliche Kennzahl ist z.B. die Summe der nicht mehr genutzten Benutzerkonten in einer Anwendung. Wird eine hohe Zahl entdeckt, so ist der Prozess „Deaktivierung einer Identität“ nicht effektiv. Weitere Metriken werden unternehmensspezifisch definiert und ausgewertet.

	Beschreibung
Auslöser	Regelmäßiger Turnus Durchführung einer Prüfung durch interne Revision / IT-Sicherheit / Geschäftsbereich Durchführung einer Prüfung, ausgelöst durch ein Ereignis Prozessschwachstellen wurden erkannt

Anwenderzentrierte Sicht:

Heute: Für die Bestimmung von Metriken sind definierte Statusinformationen erforderlich, z.B. Prozessstart und –ende. Werden die Statusinformationen nicht automatisiert geliefert, können keine aussagekräftigen Metriken ermittelt werden.

In der aktuellen Nutzer-Dienstanbieter-Beziehung werden keine Statusinformationen protokolliert. Somit können keine Metriken ermittelt werden.

Zukunft: Durch die Festlegung von nachvollziehbaren und transparenten Metriken wird die Prozessqualität und die Einhaltung von Regeln überwacht. Damit kann Vertrauen in die eingesetzte Technologie geschaffen werden.

Mögliche Kennzahlen sind z.B.: die Anzahl der zugelassenen bzw. verweigerten Zugriffe auf Informationen, Art der weitergeleiteten Informationen oder die Bestätigung der Löschung bestimmter Informationen beim Dienstanbieter.

	Beschreibung
Auslöser	Regelmäßiger Turnus Durchführung einer Prüfung, ausgelöst durch ein Ereignis Prozessschwachstellen wurden erkannt
Anforderungen	Siehe 6.4.1

6.5 Fazit

In diesem Abschnitt wurden die erheblichen Unterschiede zwischen einem Identitätsmanagement aus Sicht eines Unternehmens und aus der Sicht eines Anwenders / Bürgers ausgearbeitet.

Ein Unternehmen hat aufgrund gesetzlicher Auflagen die Aufgabe, die Berechtigungen der Mitarbeiter auf den erforderlichen Umfang zu beschränken. Zusätzlich muss es jederzeit möglich sein nachzuvollziehen welcher Anwender, mit welchen Berechtigungen und mit welcher Begründung Zugriff auf Informationen hatte. Die notwendigen Informationen kann ein Unternehmen in einem zentralen Identitätsmanagementsystem verwalten und darüber entsprechende Auswertungen erstellen.

Aus Sicht eines Anwenders steht zunächst der Schutz seiner Informationen (Attribute) im Vordergrund, d.h. er möchte die Kontrolle, über an Dienstanbieter übergebene Informationen, behalten. In der aktuellen IT Landschaft ist dies nur sehr beschränkt möglich. In der Zukunft, in einem bürgerfreundlichen Identitätsmanagement soll dies möglich sein. Der Anwender behält die Kontrolle über seine Attribute. Er kann diese über definierte Prozesse Dienstanbietern zur Verfügung stellen, bei Bedarf anpassen, die Veränderungen automatisiert an die betreffenden Dienstanbieter verteilen und auch

Attribute wieder zurückziehen. Zusätzlich kann der Anwender mittels Berichtsprozessen und definierter Metriken die Einhaltung der vorgegebenen Regelungen feststellen.

Die Gegenüberstellung des heutigen Ist-Zustandes aus Sicht des Bürgers mit einem zukünftigen Zustand zeigt, in welche Richtung eine Implementierung der Rahmenarchitektur gehen muss und welche Prozesse umgesetzt werden müssen. Die identifizierten Anforderungen müssen für ein bürgerfreundliches Identitätsmanagement berücksichtigt werden.

Im nächsten Abschnitt wird anhand des konkreten Beispiels der EU-Dienstleistungsrichtlinie die Rahmenarchitektur und das Prozessmodell konkretisiert und erläutert.

7. Das Modell am Beispiel der EU-Dienstleistungsrichtlinie (EU-DLR)

In diesem Kapitel werden am Beispiel von EU-DLR die Rahmenarchitektur und das Prozessmodell erläutert. Die in Kapitel 3 definierten Anforderungen aus Sicht von EU-DLR müssen damit erfüllt werden.

Aus diesem Grund werden verschiedene Komponenten und Dienste eingeführt, die auf der Rahmenarchitektur und dem Prozessmodell basieren und bestimmte Funktionen für verschiedene Akteure bereitstellen. Die vorgestellten Komponenten und Dienste sind jedoch nicht nur für die EU-DLR Umsetzung sinnvoll, sondern dienen als „Bausteine“ für ein umfassendes Identitäts- und Sicherheitsmanagement für verschiedene bürgerfreundliche Anwendungen in Wirtschaft und Verwaltung.

7.1 Elektronische Identitätsdokumente

Im Zuge neuer Strategien und fortschreitender technischer Entwicklungen im E-Government-Bereich, wurden von den politischen Akteuren, mit dem Ziel eine rechtliche Basis zu schaffen, auf EU- und nationaler Ebene ein Reihe von Verordnungen, Richtlinien und Gesetzen angepasst, bzw. neu verabschiedet. Als Grundlage wird häufig die i2010 oder Lissabon-Strategie als Initiative für eine europäische Informationsgesellschaft genannt, die den strategischen Rahmen für eine allgemeine politische Orientierung in diesem Sektor auf EU-Ebene absteckt. Eines der Hauptziele ist hierbei ein europaweit verfügbarer, sicherer Zugang zu öffentlichen Diensten durch gegenseitig anerkannte elektronische Identifizierung und Authentifizierung (eID). (Kommission der Europäischen Gemeinschaften, 2005).

7.1.1 Personenkennzeichen/ -kennziffern

Unter Personenkennzeichen (auch Personenidentifikator genannt) versteht man die als Versicherungs-, Register-, Kunden- und Personalnummern verwendete Kennnummern, die zur **eindeutigen Identifikation** der entsprechenden Person in einer bestimmten Domäne führen, also nicht auf mehrdeutigen Elementen, wie beispielsweise Personennamen oder Geburtsdatum, basieren.

Im Wesentlichen werden Personenkennzeichen bzw. Personenidentifikatoren in dienstanbieterspezifische oder universelle Personenkennzeichen unterschieden.

Die amtlichen Register, wie z.B. Handels-, Straf- und Steuerregister gehören zu Produkten der öffentlichen Verwaltung. In ihnen sind rechtlich bedeutsame Daten über Personen, Sachen und die damit im Zusammenhang stehenden Vorgänge gespeichert. Sie können eine Vielzahl von Personenidentifikatoren enthalten, die zwar innerhalb der Behörde bzw. Domäne die eindeutige Identifikation erlauben, jedoch nicht über Domänengrenzen hinweg genutzt werden können. Diese *dienstanbieterspezifischen* Personenidentifikatoren beziehen sich somit lediglich auf ein konkretes Sachgebiet bzw. Domäne.

Ein anderer Ansatz ist die Verwendung einer personenbezogenen Kennziffer auf nationaler Ebene. Im Gegensatz zu dienstanbieterspezifischen Personenidentifikatoren kann der Personenidentifikator domänenübergreifend eingesetzt werden. Er wird in diesem Fall als „universeller Personenidentifikator“ oder universelles Personenkennzeichen bezeichnet und dient zur Identifizierung derselben Person in

mehreren amtlichen Personenregistern (Hristova, 2005).

Neben den beiden vorgestellten Verfahren existiert ein weiterer Ansatz, der eine Mischung aus dem universellen und dienstanbieterspezifischen Personenidentifikator darstellt. Bei diesem Verfahren wird zwar eine einheitliche Kennzahl, die so genannte Stammzahl, erstellt, aber nicht direkt verwendet. Vielmehr wird die Stammzahl dazu genutzt, mehrere bereichsspezifische Identifikatoren aus einem universellen Identifikator zu generieren. Im Unterschied zum dienstanbieterspezifischen Personenidentifikator, der frei vergeben wird, ist der bereichsspezifische Identifikator aus dem universellen Personenidentifikator abgeleitet. Das dabei verwendete technische Verfahren stellt sicher, dass aus einer bereichsspezifischen Kennzahl *keine* Stammzahl generiert werden kann, die Ableitung also nur in eine Richtung funktioniert. Mit diesem System kann beispielsweise den besonderen Datenschutzbestimmungen in Österreich und Deutschland Rechnung getragen werden, da in Deutschland ein universelles Personenkennzeichen unzulässig ist.

Noch strittig ist in Deutschland die lebenslange und einheitliche Steuernummer, die jeder deutsche Staatsbürger ab Geburt erhält und über den Tod hinaus fortdauert. Als dienstanbieterspezifisches Kennzeichen für die Finanzbehörde konzipiert, kann eine Verknüpfung, z.B. mit den Daten im geplanten zentralen Bundesmelderegister, zu einem universellen Kennzeichen führen.

Generell unterscheidet sich der Einsatz von Personenkennzeichen in den verschiedenen EU Mitgliedsstaaten: Deutschland, Ungarn, die Schweiz, Großbritannien und Portugal nutzen dienstanbieterspezifische, domäneninterne Personenkennzeichen, während sich in Irland, Spanien, Slowenien, Italien, Tschechien, Dänemark, Estland, Finnland, Polen, Frankreich, Dänemark, Litauen und Belgien die Anwendung universeller Personenkennzeichen durchsetzten konnte.

Bezug zur Rahmenarchitektur:

In Kapitel 5.1.2 Attribute Certification Service wird ein Kennzeichen eingeführt, mittels dessen eine eindeutige Zuordnung eines Attributs zu einer Identität möglich ist. Universelle Personenkennzeichen wären hier die technisch einfachste Lösung, da eine eindeutige, domänenübergreifende und lebenslange Bindung zwischen Attribut und Person möglich wäre. Wie bereits ausgeführt, verstößt diese Lösung gegen das deutsche Grundgesetz[5] und kann daher national nicht umgesetzt werden.

Die eindeutige Zuordnung muss daher domänen- bzw. dienstanbieterspezifisch umgesetzt werden. So kann auch die Unverkettbarkeit von Attributen, eine wesentliche Anforderung aus Datenschutzgesichtspunkten, gewährleistet werden.

7.1.2 eIDs in Deutschland

Das Bundeskabinett hatte am 9. März 2005 die Eckpunkte für die eCard-Strategie der Bundesregierung zur Unterstützung der flächendeckenden Einführung von elektronischen Karten beschlossen. Das Eckpunktepapier der Bundesregierung sah vor, dass die Funktionalitäten Signatur, Authentisierung und Verschlüsselung aller Chipkarten interoperabel sein müssen und die optionale Aktivierung von qualifizierten Zertifikaten zur Erzeugung von qualifizierten elektronischen Signaturen möglich sein

[5] Das Bundesverfassungsgericht hat im Volkszählungsurteil von 15.12.1983 klargestellt, dass die Festlegung eines einheitlichen Personenkennzeichens unzulässig ist. Denn dies wäre „(…) gerade ein entscheidender Schritt, den einzelnen Bürger in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren.“ http://www.lfd.m-v.de/dschutz/ges_ver/guv/guv_a_20.html

soll. Der aktuelle Stand der Chipkartenprojekte wurde durch den BITKOM dokumentiert (BITKOM, 2008).

Verschiedene eCards/eIDs für verschiedene Zwecke werden bereits eingesetzt oder sind geplant:

- **Elektronischer Reisepass**: Im November 2005 wurde in Deutschland der elektronische Reisepass (ePass) eingeführt. Er enthält das digitale Passfoto als erstes biometrisches Merkmal im Chip. Seit November 2007 wird der ePass der zweiten Generation ausgegeben, bei dem zusätzlich zwei Fingerabdrücke im Chip gespeichert sind.
- **Elektronischer Personalausweis**: Der elektronische Personalausweis im Scheckkartenformat wird ab November 2010 den bisherigen Personalausweis ablösen. Die Daten, die heute optisch vom Dokument ablesbar sind, sollen zukünftig in einem Ausweis-Chip gespeichert werden. Grundsätzlich kann man aus sicherheitstechnischer Sicht zwei Anwendungsgebiete identifizieren, nämlich Anwendungen, die eine sichere Authentifizierung benötigen, und Anwendungen die eine qualifizierte Signatur, d.h. eine der handschriftlichen Unterschrift gleichzusetzende Signatur, erfordern. Beide Anwendungsfelder können als optionale Funktionen durch den elektronischen Personalausweis abgedeckt werden. Das Hauptanwendungsfeld für den elektronischen Personalausweis wird im Bereich der sicheren Authentifizierung gesehen, um den Bürgern eine einfachen und sicheren Zugang zu Dienstleistungen aller Art zu ermöglichen und den Dienstanbietern authentische Personendaten zu übermitteln (siehe auch Kapitel 8.2.1).
- **Gesundheitskarte**: Die elektronische Gesundheitskarte wird die bisherige Krankenversichertenkarte ersetzen (geplant für Herbst 2009). Die elektronische Gesundheitskarte wird verpflichtend für alle Versicherten ihre Versichertenangaben enthalten und alle Daten, die zur Ausgabe eines elektronischen Rezepts erforderlich sind, sowie die Berechtigung, im europäischen Ausland behandelt zu werden. Zusätzlich, auf freiwilliger Basis, gibt es einen medizinischen Teil mit Gesundheitsdaten. Jeder, der dies möchte, kann die Daten erfassen lassen, die für die eigene Gesundheit wichtig sind. Die Gesundheitskarte kann nachträglich mit einer Signaturfunktion ausgestattet werden, die vor allem bei künftigen elektronischen Patientenakten benötigt wird.
- **Heilberufeausweis**: Der elektronische Heilberufeausweis wird als Berufsausweis für Ärzte und Apotheker benutzt und ist eine Signaturkarte für elektronische medizinische Kommunikation (qualifizierte Signatur). Er ist Teil der Telematik-Infrastruktur für das deutsche Gesundheitswesen.
- **ELENA**: Der elektronische Entgeldnachweis (ELENA), früher auch Jobcard genannt, soll ab 1.1.2012 die Online-Abfrage der auf einem Zentralrechner der Rentenversicherung gespeicherten Entgeldnachweise ermöglichen. Der elektronische Entgeldnachweis wird für die Datenabfrage eine qualifizierte Signatur benötigen. Grundsätzlich ist es nicht notwendig, dass für ELENA eine eigene Karte erstellt wird. Es könnte z.B. der elektronische Personalausweis oder die Gesundheitskarte mit Zertifikaten für die qualifizierte elektronische Signatur ausgestattet werden, die dann bei ELENA benutzt werden.
- **eAT**: Auf europäischer Ebene ist geplant, einen europäische Aufenthaltstitel (eAT) für alle Nicht-EU-Bürger, die sich in der EU aufhalten, einzuführen. Ein eAT ist ein sicheres elektronisches Dokument im Chipkartenformat mit einem kontaktlosen Chip, auf dem u. a. die biometrischen Merkmale gespeichert sind. Im Rahmen der Standardisierung eines eAT wurden verschiedene Profile in den relevanten CEN Standards eingebracht. Ein Profil der europäischen

Aufenthaltskarte entspricht im Wesentlichen dem elektronischen Personalausweis in Deutschland.

7.1.3 eIDs in Europa

In Europa sind auf nationaler Ebene verschiedene eID Varianten und Authentifikationsmethoden geplant oder im Einsatz. Eine länderspezifische Klassifikation bezüglich der Qualität der eIDs und Authentifikationsmethoden ist in Kapitel 6.2 in (IDABC eID Interoperability for PEGS, 2007) zu finden. Anzumerken ist, dass einige Länder eigenständige eID Karten vorsehen bzw. ausgeben (z.B. Deutschland, Belgien), andere eine eID Funktion auf bereits vorhandene Karten aufbringen (z.B. Bürgerkartenfunktion in Österreich auf Krankenkassenkarte, Bankkarte).

7.1.4 European Citizen Card

Basis der Europäischen Bürgerkarte (European Citizen Card, ECC) ist der Wunsch, dass jedermann in ganz Europa eine Chipkarte besitzt, die grenzübergreifend die sichere Nutzung von Diensten ermöglicht, für die Bürger ihre Identität nachweisen müssen. Die entsprechenden CEN-Standards existieren, jedoch fehlt eine Direktive der EU, die eIDs vorschreibt. Ausweisähnliche Identitätskarten werden bisher nicht in allen Ländern Europas genutzt, z.B. nicht in Großbritannien, und können daher derzeit nicht zwangsweise vorgeschrieben werden.

7.1.5 Authentifizierung im grenzüberschreitenden europäischen Kontext

Im Artikel 8 der EU-Dienstleistungsrichtlinie (EU-DLR, 2006) wird die „Elektronische Verfahrensabwicklung“ festgelegt: *„Die Mitgliedstaaten stellen sicher, dass alle Verfahren und Formalitäten, die die Aufnahme oder die Ausübung einer Dienstleistungstätigkeit betreffen, problemlos aus der Ferne und elektronisch über den betreffenden einheitlichen Ansprechpartner oder bei der betreffenden zuständigen Behörde abgewickelt werden können.“*

Dies impliziert unter anderem, dass auch eine grenzüberschreitende Identifizierung und Authentifizierung von Dienstleistungserbringern möglich sein muss; gemäß Kapitel 6 ist dies durch die Funktionen „Administration“ und „Authentifikation“ durchzuführen. Ebenfalls müssen die übermittelten Dokumente authentisch sein.

Grenzüberschreitende Authentifizierung wird in (IDABC, 2007) wie folgt definiert:

- Der Nutzer stammt aus einem Land, dass eine Identitätsinfrastruktur und bestimmte Identifikationssysteme bereitstellt (eID Card, Username/Passwort, Mobile Authentication, …)
- Interoperabilität bedeutet, dass der Nutzer sein nationales Authentifizierungssystem direkt nutzen kann, ohne sich separat in anderen Ländern z.B. für lokale Token oder Credentials registrieren zu müssen.

Um ein grenzüberschreitende Authentifizierung zu ermöglichen, müssen die **nationalen** Systeme gemäß (IDABC, 2007) bestimmte Anforderungen erfüllen:

- Die nationalen Identitätsdaten müssen zuverlässig und korrekt sein, d.h. gegen Manipulation und Veränderung geschützt sein.
- Die Authentifizierung muss nachvollziehbar sein, d.h. sowohl der Authentifizierungsvorgang als auch die genutzten Anwendungen müssen unter Berücksichtigung von Datenschutzanforderungen dokumentiert werden

(Funktion Audit).

- Die unterschiedlichen Sicherheitsanforderungen verschiedener Anwendungen müssen berücksichtigt werden und sollten durch so genannte Authentifizierungslevel charakterisiert werden.
- Die Authentifizierungslevel zwischen verschiedenen Ländern sollten vergleichbar sein.
- Die Authentifizierung durch ausländische Nutzer sollte erlaubt und ermöglicht werden.

Grenzüberschreitende Authentifizierung stellt folgende Anforderungen:

- Semantische Kompatibilität der Identitätsattribute zwischen verschiedenen Ländern ist erforderlich. Um dies zu erreichen, müssen Identitätsattribute bestimmte Voraussetzungen erfüllen: minimale Anzahl erforderlicher Attribute, universell gültig und verfügbar in den verschiedenen Ländern, technologieneutral, nutzerkontrolliert und gesetzeskonform.
- Vertrauen in die Identitätsattribute und Authentifizierungsmethoden der anderen Länder muss erzeugt werden, um den jeweiligen Authentifizierungslevel anzuerkennen, zu verifizieren und gegenüber Anwendungen und Diensten zu bestätigen.

In den verschiedenen Mitgliedstaaten haben sich unterschiedliche Authentifizierungsmethoden (Username/Passwort, eID, Token etc.) etabliert. Es sind jedoch nicht nur diese unterschiedlichen Methoden, sondern auch die Qualität/Stärke der Identifizierung und Registrierung entscheidend für das Sicherheitsniveau, das ein Nutzer für die Authentifizierung und Dienstnutzung erlangen kann, d.h. auch die Administrationsprozesse müssen qualitativ der Authentifizierungsmethode entsprechen.

Um eine Vergleichbarkeit hinsichtlich der Qualität/Stärke der Identifizierung, Registrierung und Authentifizierung auch dann zu erreichen, wenn die diese Vorgänge nicht durch eigene bzw. nationale Instanzen durchgeführt werden, ist eine Metrik erforderlich, die die qualitative und quantitative Einordnung von administrativen Prozessen und Authentifikationsmethoden erlaubt. Dies wurde in einem ersten Ansatz in IDABC PEGS[6] (IDABC eID Interoperability for PEGS, 2007) vorgeschlagen, wobei vier so genannte „Assurance Level“ eingeführt und beschrieben worden sind.

Um Interoperabilität und grenzüberschreitende Authentifizierung auch praktisch zu erreichen und zu erproben, wurde das STORK[7] Projekt – ein „large scale pilot“ im Rahmen des EU-CIP (Competitiveness and Innovation Programme) – von der EU im Mai 2008 gestartet. Das Projekt zielt auf die Umsetzung eines EU-weiten, interoperablen Systems für die Anerkennung von eIDs und Authentifizierung, die es Unternehmen, Bürgern und Verwaltungsmitarbeitern erlaubt, nationale elektronische Identitäten in den verschiedenen Mitgliedstaaten zu nutzen. Verschiedene grenzüberschreitende Dienste, die eIDs nutzen sollen, werden pilotiert. Die Interoperabilität der nationalen eID-Systeme ist der Hauptschwerpunkt.

---

[6] IDABC PEGS: European Community Programme for the interoperable delivery of pan-European e-government services to public administrations, businesses and citizens

[7] STORK (Secure idenTity acrOss boRders linKed) http://www.eid-stork.eu/

Im STORK Projekt (STORK project D2.3, 2009) wurde das STORK Quality Authentication Assurance Framework (QAA) entwickelt, das basierend auf IDABC vier Level der „Authentication Assurance“ definiert, die jeweiligen nationalen Authentifikationsmethoden einordnet und die eID Lösungen aufeinander abbildet.

STORK Quality Authentication Assurance Framework (QAA) Level	Beschreibung
1	Keine oder minimale Sicherheit (no or minimal assurance)
2	Geringe Sicherheit (low assurance)
3	Substanzielle Sicherheit (substantial assurance)
4	Hohe Sicherheit (high assurance)

Tabelle 6: STORK QAA Level

Für die Festlegung der Qualitätskriterien werden in STORK organisatorische und technische Faktoren unterschieden und ihrer jeweiligen Durchführung bei den entsprechenden zuständigen Instanzen auf nationaler Ebene bewertet. Aus den verschiedenen Faktoren ergibt sich dann der insgesamt erreichte QAA Level.

Organisatorische Faktoren bzgl. der Registrierungsdurchführung sind:

- Qualität des Registrierungsprozesses, z.B. Anwesenheitsstatus, vorgelegte Identitäts- und Attributnachweise, Identitätsdokumente
- Qualität des Prozesses für die Ausgabe von Geheimnissen/Nachweisen wie Passwort, PIN etc., z.B. Versand per email, per Einschreibebrief, Aktivierung durch persönliche Anwesenheit
- Qualität der Entität, die die Registrierung durchführt und die Nachweise ausgibt, z.B. private Entität, national akkreditierte Entität, qualifizierte Entität gemäß Signature Directive

Technische Faktoren bzgl. der Authentifikation sind:

- Typ und Robustheit des Nachweises, z.B. Passwort, One-time Passwort, Software-Zertifikat, qualifiziertes Zertifikat auf Smartcard
- Sicherheitseigenschaften bzw. potentielle Risiken des Authentisierungsalgorithmus‘ bzgl. der Authentisierungsdurchführung, z.B. EAL Evaluierung gemäß Common Criteria.

Im STORK Deliverable D2.1 (STORK project D2.1, 2008) sind für Deutschland folgende nationale Qualitätsstufen benannt worden[8]:

- Level 0 (low): keine Sicherheit bzgl. der Information, niedriger Authentifizierungslevel
- Level 1 (normal): zuverlässiger Identitätsnachweis bei der Registrierung, Authentifizierung mit Benutzername/Passwort
- Level 2 (high): zuverlässiger Identitätsnachweis bei der Registrierung,

[8] Diese Qualitätsstufen sind in STORK von den deutschen Partnern im Projekt eingebracht worden (BSI).

Authentisierung mit Hardware Token und PIN

- Level 3 (very high): wie Level 2 aber mit Nutzung von zertifiziertem Hardware Token und Kartenleser

Die Abbildung der deutschen Levels 0-3 entspricht den STORK QAA Levels 1-4.

Bietet ein Dienstanbieter (in STORK: Service Provider) einen Dienst an, dann legt er die Sicherheitseinstufung fest, die erforderlich ist, um seinen Dienst zu nutzen. Die Sicherheitseinstufung entspricht dabei dem erforderlichen nationalen Qualitätslevel für den Authentisierungsnachweis. Im grenzüberschreitenden Fall müssen die nationalen Qualitätslevel in die STORK QAA Level abgebildet werden. Die entsprechende Mapping-Tabelle wurde durch STORK entworfen (STORK project D2.3, 2009).

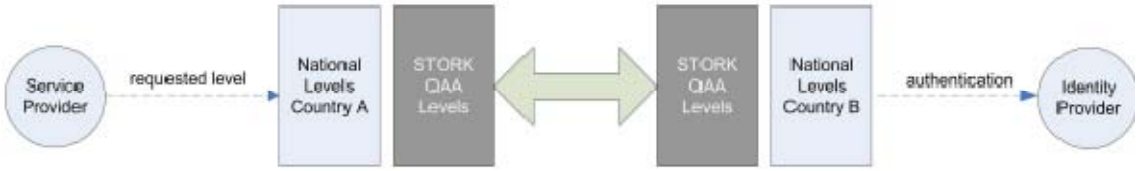


Abbildung 10: STORK Mapping der Qualitätslevel (Quelle: (STORK project D2.3, 2009))

Für die Übermittlung der Identitätsnachweise werden in STORK zwei Lösungen diskutiert, die sich bzgl. der Lokation der Mapping-Funktion unterscheiden:

- **Proxy Ansatz:** Ein Dienstanbieter kontaktiert den nationalen (lokalen) PEPS (Pan-European Proxy Service) zwecks Anforderung der Identitätsnachweise und des QAA Levels. Der lokale PEPS kontaktiert dann den entfernten PEPS des Ursprungsmitgliedstaates. Der entfernte PEPS lässt von seinem zuständigen Attribut-Zertifizierer (Identity Provider in STORK) die Authentifizierung ausführen und die Identitätsnachweise (Credentials in STORK) ausstellen. Diese leitet er dann an den anfordernden lokalen PEPS einschließlich der Information über den QAA Level zurück. Der lokale PEPS übergibt die Nachweise an den Dienstanbieter. Diese Lösung wird als Standardlösung betrachtet, die von allen Mitgliedstaaten implementiert werden soll. Die Mapping-Funktion wird im grenzüberschreitenden Kontext zentral in den PEPS ausgeführt. Im nationalen Kontext können auch die nationalen Qualitätslevels benutzt werden.
- **Middleware-Ansatz:** Der Middleware-Ansatz ist im Wesentlichen für Smartcard- und PKI-basierte Identitätsfeststellung konzipiert. Dabei wird davon ausgegangen, dass die Smartcard die Identitätsnachweise enthält und somit der QAA Level nicht „zentral“ durch den PEPs ermittelt werden muss, sondern durch den auslesenden Attribut-Zertifizierer bzw. der Middleware festgelegt werden kann.[9] Sind für die Dienstnutzung zusätzliche Identitätsattribute notwendig, die nicht durch die eID Karte, sondern durch andere Attributprovider bereitgestellt werden, dann ist für diese Attribute der Proxy-Ansatz durchzuführen.

Die STORK Infrastruktur erfordert diverse Vertrauensverhältnisse zwischen den beteiligten Entitäten, da die Authentisierungsinfrastruktur auf qualitativ akzeptablen Attribut-Nachweisen aus anderen Ländern beruht. Daher wird ebenfalls die

[9] Anmerkung der Autoren: Diese Variante wird von Deutschland bevorzugt, um eCard API und Zugriffszertifikate für die Identitätsnachweise zu verwenden.

organisatorische Überwachung des QAA Frameworks durch eine geeignete Instanz mit festgelegten Regeln gefordert, die noch nicht etabliert ist. Die Umsetzungsmöglichkeiten werden in STORK noch diskutiert.

7.1.6 eIDs und Authentifizierung in Bezug zur Rahmenarchitektur

Elektronische Identitätsdokumente dienen der sicheren Authentifizierung einer Person basierend auf der sicheren Identifikation der Person bei der ausstellenden Institution oder Behörde. Die Attribute, die durch die eID bescheinigt werden, besitzen somit eine bestimmte Qualität, je nachdem wie diese durch die ausstellende Institution überprüft worden sind.

Auch hier können Attribute mit unterschiedlicher Qualität auf einer eID vorhanden sein: beispielhaft sei der elektronische Personalausweis genannt, bei dem Name und Geburtsdatum durch die Geburtsurkunde qualitativ verifizierbar bescheinigt werden, nicht jedoch die Adresse, da die Meldedaten bundeslandspezifisch unterschiedlichen Überprüfungsmechanismen unterliegen, z.B. Bestätigung des Vermieters, Bestätigung des Hauptmieters oder Eigenangaben.

eIDs und grenzüberschreitende Authentifizierung sind eine spezifische Umsetzung für ist für den in der Rahmenarchitektur in Kapitel 5.1.3 beschriebenen Authentication Service.

Folgende Anforderungen werden erfüllt:

Komponente	Akteur	Anforderung	Erläuterung
eID	Dienstleistungs-erbringer	DL-A1	Verwendung der nationalen elektronischen Identitätsnachweise
	Zuständige Behörde	ZB-A1	Registrierung und Authentifizierung der Mitarbeiter mittels eID
	Einheitlicher Ansprechpartner	EA-A1	Registrierung und Authentifizierung der Mitarbeiter mittels eID
	Anwender / Bürger	P-A1	Verwendung der nationalen elektronischen Identitätsnachweise

Komponente	Akteur	Anforderung	Erläuterung
Grenzüber-schreitende Authentifizierung	Dienstleistungs-erbringer	DL-A1	Verwendung der nationalen elektronischen Identitätsnachweise
	Dienstleistungs-erbringer	DL-A2	Keine mehrfache Authentifizierung wenn technisch als Single Sign-On umgesetzt; gemäß Möglichkeit (1)

	Einheitlicher Ansprechpartner	EA-A2	Unterstützung der grenzüberschreitenden Authentifizierung des DL; Weitergabe der Authentifizierungsnachweise an die ZB wenn erforderlich

Die Anforderungen DL-A3, ZB-A2, EA-A2 hinsichtlich der gegenseitigen Authentifizierung der Akteure werden durch die Komponenten eID und grenzüberschreitende Authentifizierung nicht automatisch abgedeckt. Eine Realisierung kann z.B. mittels geeigneter Protokolle in der Infrastruktur erfolgen, die den Client und den Server geeignet gegenseitig authentifizieren. Ein Beispiel hierfür ist der Datenschutzdialog vor Übermittlung der Daten und Berechtigungszertifikate von Behörden und Dienstanbietern für den Zugriff auf die Attribute des elektronischen Personalausweises.

7.2 Komponenten und Dienste

In diesem Abschnitt werden verschiedene Komponenten und Dienste vorgestellt, die zur Abdeckung der Anforderungen von EU-DLR eingesetzt werden können.

Die vorgestellten Komponenten basieren auf den in der Rahmenarchitektur (Kapitel 5) beschriebenen Diensten, Komponenten und Modulen für Identitätsmanagement und stellen Funktionalitäten zur Verfügung, die auch für andere komplexe elektronische Fachanwendungen in Verwaltung und Wirtschaft sinnvoll erscheinen.

7.2.1 Elektronischer Safe (eSafe)

Mit der elektronischen Kommunikation fallen immer mehr elektronische Dokumente an. Gerade für Verwaltungsvorgänge wie in der DLR beschrieben, sind diese Dokumente teilweise langfristig sicher und beweiswerterhaltend aufzubewahren und zu verwalten. Meist verfügen Bürgerinnen und Bürger, kleinere Unternehmen und andere Organisationen nicht über eine geeignete technische Infrastruktur.

Um Bürgern den elektronischen Zugang zur Verwaltung zu erleichtern, ist die Einrichtung eines Systems zur sicheren Ablage und die Einbindung digitaler Daten und Dokumente in die Verwaltungsprozesse der Bürger notwendig. Ein solches System stattet die Bürger mit geeigneten Werkzeugen aus, um den Gebrauch persönlicher Daten zu steuern und nachzuvollziehen.

(Breitenstrom, et al., 2008) beschreiben im „FOKUS White Paper eSafe“ die Verwaltung von elektronischen Dokumenten mittels eines elektronischen Safes. Die Einführung in elektronische Safes wird im Folgenden auszugsweise vorgestellt.

Elektronische Safes:

Elektronische Safes sind auf modernen Informations- und Kommunikations-technologien basierende und über elektronische Medien erreichbare virtuelle Schließfächer zur Ablage, Verwaltung und Freigabe elektronischer Dokumente. Als elektronisches Pendant zum herkömmlichen Bankschließfach gewährleistet der elektronische Safe die unbedingte Vertraulichkeit der enthaltenen Daten und Dokumente. Der Eigentümer des elektronischen Safes ist alleiniger Verwalter des Safeinhaltes. Der elektronische Safe bietet dem Eigentümer neben den Funktionen zur Verwahrung von Daten und Dokumenten auch Funktionen zur feingranularen Freigabe seiner Inhalte. Hiermit wird es dem Eigentümer möglich, Dritten jeweils nur die für sie notwendigen Daten zur Verfügung zu stellen.

Im Sinne einer kundenorientierten modernen Verwaltung ist es notwendig, den Datenaustausch zwischen Kunden und Verwaltung möglichst einfach zu gestalten. Insbesondere die Datenerhebung zu Beginn von Verwaltungsprozessen wird durch den Gebrauch von elektronischen Safes stark vereinfacht. Daten, die bereits vom Kunden in seinem Safe gepflegt sind, und Dokumente, die bereits vorhanden sind, müssen nicht erneut erfasst beziehungsweise beschafft werden.

Der Safe steht unter ausschließlicher Verfügungsgewalt des Bürgers oder des Unternehmers, vollkommen unabhängig vom Anbieter des Schließfaches, aber auch unabhängig von staatlichen Stellen oder sonstigen Dritten. Die Basisfunktionalität des elektronischen Dokumentensafes stellt sicher, dass der Nutzer des Safes beliebige elektronische Objekte öffnen, speichern, versenden, weiterleiten, ausdrucken, herunterladen, einstellen, löschen, suchen, sortieren, kommentieren und auf mögliche Viren oder gültige Unterschriften überprüfen kann. Sinnvoll sind auch die Integration bzw. Anbindung einer E-Mail-Funktionalität, Langzeitarchivierung, die Einbindung einer Terminverwaltung zu Fristabläufen und Fälligkeitsdaten und die Anbindung der gespeicherten Objekte an vorhandene Prozesse und Anwendungen.

Die Einrichtung des elektronischen Safes kann auf einem für diese Zwecke ausgerichteten Server (bei einem Safe-Betreiber) bzw. beim Bürger/Unternehmen selbst erfolgen.

Abbildung 11: Beschreibung eines elektronische Safes (Quelle: (Breitenstrom, et al., 2008))

Der Zugang und Zugriff zum elektronischen Safe muss durch Identitätsmanagement-Dienste geschützt werden:

- Nutzung von AACS und Policy Management Services, um Rechte und Berechtigungen basierend auf der Identität von Personen bzw. für bestimmte Rollen (Behördenmitarbeiter, Einheitlicher Ansprechpartner) vergeben werden können.
- Nutzung des Logging Services, um eine Nachvollziehbarkeit hinsichtlich der Zugriffe auf Dokumente zu gewährleisten.
- Je nach Ausprägung des eSafes ist die rechtsverbindliche Kommunikation (siehe Kapitel 7.2.9) ein Bestandteil des elektronischen Safes oder muss als Dienst eingebunden werden können; ebenso kann auch die Langzeitarchivierung von Daten und Dokumenten (siehe Kapitel 7.2.6) integriert werden oder als separater Dienst eingebunden werden.

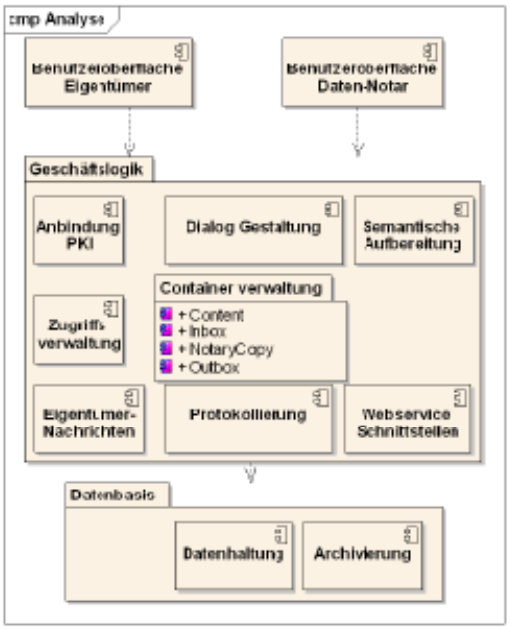


Abbildung 12: Technische Komponenten eines elektronischen Safes (Quelle: (Breitenstrom, et al., 2008))

Die Akteure bezüglich eines elektronischen Safes sind die Safe-Eigentümer (natürliche oder juristische Personen), die Zugriffsberechtigen, z.B. die Verwaltung, die Dokumente anfordert) und die Safe-Betreiber (Dienstanbieter von elektronischen Safes).

Hinsichtlich des elektronischen Safes bestehen seitens der Akteure die folgenden Berechtigungen:

- *Safe-Eigentümer* dürfen ihre eigenen Daten lesen und ihre eigenen Daten schreiben und löschen. Sind Safe-Daten für Zugriffsberechtigte zum Abruf bereitgestellt worden, so sind diese Daten bezüglich Änderungen durch den Safe-Eigentümer gesperrt. Eigentümer können mehrere eSafes bei einem oder verschiedenen Safe-Betreibern haben.
- *Zugriffsberechtigte* besitzen Leserechte auf die für sie freigegebenen Daten. Sie können diese Daten auch sperren, solange sie als Zugriffsberechtigte mit ihnen arbeiten müssen (Aufbewahrungsfristen). Zugriffsberechtigte können auch neue Daten bereitstellen.
- *Safe-Betreiber* besitzen keinen Zugriff auf die Daten.

Dokumentensafes werden ebenfalls als Komponente im Bürgerportal[10] (siehe Kapitel 8.2.3) im Rahmen der eGovernment-2.0-Strategie des Bundes angestrebt, sind jedoch noch nicht implementiert. Die Technischen Richtlinien für Bürgerportale sind vom BSI veröffentlicht worden (BSI, Bürgerportale). Der sogenannte Dokumentsafe Light ist allerdings nur eine optionale Komponente des Bürgerportals.

[10] Bürgerportale sollen von unterschiedlichen Anbietern bereitgestellt werden, die im Wettbewerb zueinander stehen und sich durch unterschiedliche Mehrwerte, die über die Bürgerportal-Dienste hinausgehen, voneinander abgrenzen können. In einem Zertifizierungsverfahren sollen alle Anbieter eines Bürgerportals gegenüber einer unabhängigen Stelle die Zuverlässigkeit der Verfahren und Prozesse nachweisen, so dass alle Bürgerportale die gleiche nachgewiesene Sicherheit besitzen.

Folgende Anforderungen werden erfüllt:

Komponente	Akteur	Anforderung	Erläuterung
eSafe	Dienstleistungs-erbringer	DL-A4	Vertrauliche Daten werden nur an Zugriffsberechtigte für den Lesezugriff bereitgestellt
	Dienstleistungs-erbringer	DL-A7	Sichere Aufbewahrung von Dokumenten
	Zuständige Behörde	ZB-A3	Autorisierter Zugriff auf die erforderlichen Verfahrensdaten und -dokumente im eSafe
	Einheitlicher Ansprechpartner	EA-A3	Autorisierter Zugriff auf die erforderlichen Verfahrensdaten und -dokumente im eSafe
	Anwender / Bürger	P-A2	Vertrauenswürdige Verwaltung von Informationen / Attributen
	Anwender / Bürger	P-A4	Zentrale Verwaltung mehrfach genutzter Informationen
	Anwender / Bürger	P-A5 / P-A6	Zugriffsmanagement
	Anwender / Bürger	P-A11	Vergeben von Vollmachten
	Anwender / Bürger	P-A17	Protokollierung des Zugriffs

7.2.2 Datennotar

Der Datennotar ist eine spezifische Ausprägung eines elektronischen Safes, der bei einem sicheren Safe-Betreiber lokalisiert ist und notarähnliche Funktionen bereitstellen kann.

Das ISPRAT-Projekt Datennotar untersucht derzeit die rechtlich-organisatorischen und technischen Maßnahmen, die geeignet sind um ein sehr hohes Schutzniveau für Daten und Unterlagen zu gewährleisten. Im Ergebnis der Arbeit wird ein Rahmenwerk zur Etablierung von Datennotaren entwickelt. Im ISPRAT-Projektantrag wurden für Datennotare die folgenden Kernaussagen definiert:

- Datennotare gewährleisten im Kern die vertrauensvolle und sichere Verwahrung digitaler Daten und Dokumente.
- Datennotare erfüllen (gesetzlich) definierte Mindeststandards zum Schutz der anvertrauten Daten und Dokumente.

- Datennotare unterliegen eindeutigen Regelungen bzgl. ihrer Funktionsweise und in den Beziehungen zu ihren Kunden.
- Datennotare unterliegen den Pflichten und genießen den besonderen Schutz notarieller Geheimnisträger.
- Die Funktion eines Datennotars könnte von zertifizierten IT-Dienstanbietern oder von anerkannten Notaren übernommen werden.

In Anlehnung an Notare kann der Datennotar ein besonderes Vertrauensverhältnis zwischen verschiedenen Akteuren schaffen. Als Trusted Third Party können Datennotare je nach Ausprägung verschiedene Funktionen ausführen, von der sicheren Verwahrung von elektronischen Dokumenten ohne Einblick in die Dokumente bis hin zur Beurkundung physischer und digitaler Unterlagen. Ebenfalls ist die Ausstellung und unparteiische Überwachung und Interpretation von Vollmachten eine weitere mögliche Funktion.

Diese aufgeführten Funktionen werden in den folgenden Abschnitten näher betrachtet. Sie werden als eigene Abschnitte beschrieben, da die Funktionen nicht notwendigerweise von einem Datennotar ausgeführt werden müssen. Folgende Anforderungen bezüglich DLR werden durch einen Datennotar erfüllt (Die Zusatzfunktionen werden in den folgenden Abschnitten betrachtet):

Komponente	Akteur	Anforderung	Erläuterung
Datennotar	Dienstleistungs-erbringer	DL-A7	Rechtssichere Aufbewahrung von Dokumenten

7.2.3 Elektronische Originaldokumente

Elektronische Dokumente können in unterschiedlichen Formen auftreten, z.B. eingescanntes Dokument als „Bild“, XML-Datensatz, PDF o.ä. Die Art des Dokuments hat Einfluss auf die elektronischen Weiterverarbeitungsmöglichkeiten der enthaltenen Informationen (medienbruchfrei oder z.B. durch menschliche Interpretation).

Zur Vereinfachung der Verwaltungsprozesse sind durch die EU-DLR keine formalen Anforderungen vorgesehen, wie etwa die Vorlage von Originaldokumenten, beglaubigten Kopien oder beglaubigten Übersetzungen, es sei denn, dies ist objektiv durch einen zwingenden Grund des Allgemeininteresses gerechtfertigt. Es ist ausreichend, elektronische Dokumente bzw. noch zu erstellende Formblätter zu übermitteln.

Bestehen Zweifel an der Echtheit eines bestimmten Dokuments bzw. dessen genauen Inhalts, dann kann die ZB bei der austellenden zuständigen Behörde nachfragen. Für diese grenzüberschreitenden Nachfragen wird das Binnenmarkt-Informationssystem (IMI) eingerichtet.

Grundsätzlich ist hier anzumerken, dass ein elektronisches Dokument nur mit einer elektronischen Signatur vor Veränderungen geschützt ist. Natürlich könnte ein sicherer Kanal das Dokument auf dem Übertragungsweg schützen, dies gilt jedoch nicht im Speicher eines Systems.

Obwohl die EU-DLR elektronische Signaturen nicht erwähnt, sollte die Umsetzung der Richtlinie die Schutzziele Integrität, Vertraulichkeit und Authentizität jederzeit gewährleisten. Für elektronische Dokumente werden daher folgende Anforderungen

gestellt:

- Eine Signatur muss geprüft werden und das Ergebnis der Prüfung muss dokumentiert werden.
- Langzeit-Archivierung muss gemäß der gesetzlichen Fristen ermöglicht werden.
- Jede Konvertierung sowie die weitere Verarbeitung muss protokolliert werden.
- Elektronische Beglaubigungen bzw. beglaubigte Übersetzungen müssen bei Bedarf möglich sein.

Komponente	Akteur	Anforderung	Erläuterung
Elektronische Dokumente	Dienstleistungs-erbringer	DL-A5	Signierte Dokumente sind vor Modifikationen geschützt, d.h. Modifikationen sind erkennbar

7.2.4 Elektronische Beglaubigung

Eine der Aufgaben von Notaren ist es, Beglaubigung von Dokumenten durchzuführen.

Mit dem Justizkommunikationsgesetz[11] wurden der Zivilprozess und die Fachgerichtsbarkeiten für eine elektronische Aktenbearbeitung geöffnet. Die Verfahrensbeteiligten - Richter, Rechtsanwälte, Bürger - haben die Möglichkeit, elektronische Kommunikationsformen gleichberechtigt neben der - herkömmlich papiergebundenen - Schriftform oder der mündlichen Form rechtswirksam zu verwenden.

Für die elektronische Beglaubigung gelten die folgenden Erläuterungen der Bundesnotarkammer[12,13]:

„Bei der elektronischen Beglaubigung wird in Deutschland die Unterschrift und das Amtssiegel des Notars auf Papierdokumenten durch die qualifizierte elektronische Signatur ersetzt. Die Bestätigung der Notareigenschaft erfolgt durch ein entsprechendes Zertifikatsattribut. Beim Notar wird der Nachweis der Notareigenschaft und die Verbindung dieses Nachweises mit dem elektronischen Dokument dadurch realisiert, dass das Notarattribut automatisch Teil des qualifizierten Signaturzertifikats ist. Danach wird im Zertifizierungsverfahren zur Erlangung der Signaturkarte auch die Stellung als Notar durch Vorlage einer entsprechenden Bestätigung der Notarkammer festgestellt und als eigenständige Information auf der Signaturkarte des Notars abgespeichert."

Ob ähnliche Regelungen in anderen Ländern existieren und ob das entsprechende Notarattribut von anderen Ländern anerkannt wird, ist z.Zt. nicht bekannt. Grenzüberschreitende Attributnachweise sind jedoch eine grundsätzliche Anforderung an IDM Systeme.

---

[11] Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz – JKomG), Vom 22. März 2005

[12] Bundesnotarkammer, http://www.bnotk.de/Service/Empfehlungen+Hinweise/RS25-06_El-Handelsregisterverkehr.html

[13] Rundschreiben Nr. 22/2005, Elektronischer Beglaubigungsvermerk/Elektronischer Rechtsverkehr mit dem Handelsregister, http://www.berliner-notarkammer.de/bnotk/rs22_2005.pdf

Folgende Anforderungen werden durch elektronische Beglaubigungen erfüllt:

Komponente	Akteur	Anforderung	Erläuterung
Elektronische Beglaubigung	Dienstleistungs-erbringer	DL-A8	Gültigkeit von Originaldokumenten durch Beglaubigung
	Zuständige Behörde	ZB-A4	Echtheit und Gültigkeit von Dokumenten kann durch die elektronische Beglaubigung nachgewiesen werden
	Einheitlicher Ansprechpartner	EA-A4	Echtheit und Gültigkeit von Dokumenten kann durch die elektronische Beglaubigung nachgewiesen werden

Die Beglaubigung durch den „Datennotar“ oder eine andere Instanz weist jedoch nicht nach, ob das vorgelegte elektronische Dokument rechtmäßig ausgestellt worden war, z.B. kann ein Meisterbrief zwar von der Papierform in eine elektronisch beglaubigtes Dokument überführt werden, ob dieser Brief jedoch wirklich von der Handwerkskammer bzw. der Industrie- und Handelskammer ausgestellt wurde oder eine Fälschung vorliegt, kann so nicht überprüft werden. Für diesen Zweck müssten Verifikationsmöglichkeiten geschaffen werden, die bei den austellenden Institutionen in deren Registern nachprüfen können, ob das Dokument echt ist. Da dies online meist nicht möglich ist, wird für diese grenzüberschreitenden Nachfragen das Binnenmarkt-Informationssystem (IMI) eingerichtet.

7.2.5 Elektronische Vollmachten

Elektronische Vollmachten und Vertretungsbefugnis erlauben es, Rechte bzw. Rollen und Funktionen von einer Person auf eine andere zu übertragen. Da Vollmachten an keine bestimmte, gesetzliche vorgegebene Form gebunden sind, ist eine automatisierte Verarbeitung derzeit meist nicht möglich. Um Vollmachten elektronisch zu beschreiben, müssen geeignete Datenstrukturen entworfen werden, die bestimmte Attribute enthalten. Z.B. können Vollmachten auch zeitlich beschränkt sein, d.h. Ausstellungsdatum und Gültigkeitszeitraum sind wesentliche Attribute.

In Österreich sind elektronische Vollmachten bereits spezifiziert[14] worden. Eine elektronische Vollmacht besteht in Österreich aus folgenden Attributen, die auch aus deutscher Sicht sinnvoll sind:

- Vollmachtgeber
- Vollmachtnehmer
- Ausstellungsdatum
- Wirkungsbereich
- Inhalt (möglichst aus standardisierten Textblöcken bestehend)

[14] Elektronische Vollmachten in Österreich, https://demo.egiz.gv.at/plain/projekte/buergerkarte_und_eid/elektronische_vollmachten

Die elektronischen Vollmachten müssen geeignet verifiziert werden können. Ist die Vollmacht widerrufen worden, so muss dies feststellbar sein, indem der Widerrufstatus geprüft werden kann (ähnlich wie bei X.509 Zertifikaten).

Generell sind elektronische Vollmachten ein Beispiel für die Weitergabe von Attributen an Befugte. Attribute, die gemäß Rahmenarchitektur durch das Identity Attribute Data Repository verwaltet werden, können unterschiedlichen Quellen entstammen. Eine mögliche Quelle ist eine andere Person bzw. Entität, die ein Attribut für eine bestimmte Zeit an eine andere Person bzw. Entität „verleiht". Der rechtmäßige „Besitz" des Attributs muss nachprüfbar sein. Auch hier können Datennotare eingesetzt werden, um die elektronischen Vollmachten vertrauenswürdig zu verwalten.

Folgende Anforderungen werden durch elektronische Vollmachten erfüllt:

Komponente	Akteur	Anforderung	Erläuterung
Elektronische Vollmacht	Dienstleistungs-erbringer	DL-A6	Handlungsvollmachten vom DL an einen externen Bevollmäch-tigen oder den EA können erteilt werden; ggfs. kann ein Daten-notar die Gültigkeit von Vollmachten bescheinigen
	Anwender / Bürger	P-A11	Vergeben von Vollmachten

7.2.6 Langzeitarchivierung

Unter Langzeitarchivierung[15] versteht man die langfristige Aufbewahrung und die Erhaltung der dauerhaften Integrität und Verfügbarkeit von Informationen. Langzeit bedeutet für diese digitalen Ressourcen, dass Strategien und Techniken entwickelt werden, damit die Informationen erhalten bleiben.

> *'Langzeit' ist die Umschreibung eines nicht näher fixierten Zeitraumes, währenddessen wesentliche nicht vorhersehbare technologische und soziokulturelle Veränderungen eintreten, die sowohl die Gestalt als auch die Nutzungssituation digitaler Ressourcen in rasanten Entwicklungszyklen vollständig umwälzen werden.*
>
> *(Zitat aus: Grundlagen der praktischen Information und Dokumentation[16])*

Zu den Forderungen an die Langzeitarchivierung gehören die Unverfälschtheit des Dokuments bzw. der Daten, die gespeicherten Daten müssen mit einfachen Hilfsmitteln dargestellt werden können, und die Qualität der Daten müssen unverändert sein.

Langzeitarchivierung ist für Bürger und Unternehmen und insbesondere für Behörden von Relevanz, da auch elektronische Dokumente in Zukunft den gesetzlich vorgegebenen Aufbewahrungsfristen genügen müssen.

---

[15] nestor Kompetenznetzwerk Langzeitarchivierung, www.langzeitarchivierung.de

[16] Ute Schwens, Hans Liegmann: *Langzeitarchivierung digitaler Ressourcen*. In: Rainer Kuhlen, Thomas Seeger, Dietmar Strauch (Hrsg.): Grundlagen der praktischen Information und Dokumentation. 5., völlig neu gefasste Ausgabe. München: Saur, 2004, S. 567

Im Rahmen von ArchiSafe[17] wurden mehrere Konzepte und Spezifikationen erarbeitet und veröffentlicht. Diese betrachten auch die rechtlichen und sicherheitsrelevanten Aspekte wie:

- Rechtliche Rahmenbedingungen für die Verwaltung, die bei der Langzeitarchivierung elektronisch signierter Dokumente zu beachten sind
- Funktionale Anforderungen an eine dauerhafte und rechtssichere elektronische Ablage
- Metadaten, die für eine Ablage von elektronischem Schriftgut erforderlich sind
- Geeignete Langzeitdokumentenformate
- Signaturen und Signaturverifikationsdaten
- Schutzprofil (PP-0049) nach den Common Criteria

Langzeitarchivierung kann als Funktion eines elektronischen Safes oder als Funktion eines Datennotars in die entsprechende Komponente integriert sein. Ebenfalls ist die Realisierung als eigener Dienst möglich, z.B. wird *"ArchiSafe"* von der "Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung" (KBSt) als *"Einer-für-Alle"* (EfA)-Dienst unterstützt und finanziell gefördert[18].

Folgende Anforderungen werden durch Langzeitarchivierung teilweise erfüllt:

Komponente	Akteur	Anforderung	Erläuterung
Langzeit-archivierung	Dienstleistungs-erbringer	DL-A7	Einhaltung von Aufbewahrungsfristen
	Zuständige Behörde	ZB-A5	Ein- und Ausgangs-dokumente und Bescheide sicher aufbewahren, Aufbewahrungsfristen einhalten

7.2.7 Fallmanagement

*Beim **Fallmanagementsystem** handelt es sich um das System zum Kontaktmanagement und zum Management der damit verbundenen Fälle (Aufträge von DLs). Generell ist bei der Gestaltung des Fallmanagements der Umfang, die Frage der Zugriffsmöglichkeiten und -rechte sowie die Positionierung zu klären.*

Zitat aus (von Lucke, J., Eckert, K.-P., Breitenstrom, C., 2008)

Im einfachsten Fall fungiert ein elektronischer Safe als Fallmanagementsystem für einen Safe-Eigentümer. Ein DL kann seine Anträge verwalten und mit dem EA bzw. den zuständigen Behörden die notwendigen Daten und Dokumente sicher austauschen bzw. den Zugriff gewähren. Das Fallmanagement wird hier überwiegend manuell ausgeführt, indem der DL die erforderlichen Aktionen bezüglich seines Falles selbst initiiert.

Wird das Fallmanagement durch den EA für alle anfragenden DLs ausgeführt, dann

[17] Projekt ArchiSafe http://www.archisafe.de
[18] Siehe http://www.archisafe.de/s/archisafe/index

reicht ein elektronischer Safe wie in Abschnitt 7.2.1 beschrieben funktional nicht aus. Ein EA verwaltet viele Anträge (Fälle) und muss daher Funktionen wie Kontaktmanagement mit DL und ZB, Management der einzelnen Fälle, Statusabfragen, Dokumentenverwaltung, Übermittlung von Informationen, Aufgaben und Zwischenständen, anonymisierte Daten für Statistiken, etc. ausführen.

Die Zuständige Behörde muss ebenfalls ein Fallmanagement durchführen. Ist die Zuständige Behörde eine einzelne Behörde, dann kann das Fallmanagement behördenintern ausgeführt werden.

Ist die Zuständige Behörde virtuell zu sehen, dann müssen verschiedene Behörden interagieren und das Fallmanagement behördenübergreifend realisieren. Hier kann die Interaktion z.B. durch einen Workflow zwischen beteiligten Behörden etc. durchgeführt werden. Eine weitere Möglichkeit wäre, eine dezentrale **Fallakte**, die unten beschrieben wird. In jedem Fall verwaltet die ZB ähnlich dem EA viele Anträge (Fälle) und muss daher ebenfalls Funktionen wie Kontaktmanagement mit DL und EA, Management der einzelnen Fälle, Statusabfragen, Dokumentenverwaltung, etc. ausführen.

Die Realisierung eines Fallmanagements kann als zentrales behördenübergreifendes System oder als Verbund verschiedener Fallsysteme der einzelnen Behörden erfolgen.

Betrachtet man ein Fallmanagementsystem hinsichtlich der Anforderungen und Einbindung von Identitätsmanagement- und Sicherheitsdiensten, so sind folgende Funktionen identifizierbar:

- Administrative Dienste für die Stammdatenverwaltung, Rollenverwaltung und Verwaltung von weiteren Attributen, um die Authentisierung, Autorisierung und Zugriffsverwaltung durchzuführen
- Authentisierung des Eigentümers (ggfs. mit unterschiedlicher Qualität je nach auszuführender Funktion
- Authentisierung der Akteure, falls noch andere auf das Fallmanagement zugreifen dürfen
- Vergeben von Rollen bzw. Rechten für Akteure
- Autorisierung und Zugriffsteuerung für den Zugriff auf die Dokumente und Daten im elektronischen Safe bzw. Fallmanagementsystem
- Personalisierte Verwaltungsleistungen und –prozesse, basierend auf den Identitätsinformationen
- Signaturen, Signaturprüfung von Dokumenten, Zeitstempel
- Protokollierung/Logging von Zugriffen
- Rechtssichere (nicht-abstreitbare) Zustellung von Bescheiden

Folgende Anforderungen werden durch das Fallmanagement (teilweise) erfüllt:

Komponente	Akteur	Anforderung	Erläuterung
Fallmanage-ment	Zuständige Behörde	ZB-A5	Erforderlich für die sichere Verwaltung und Bearbeitung von Fällen
	Einheitlicher Ansprechpartner	EA-A5	Erforderlich für die sichere Verwaltung und Bearbeitung von Fällen, sofern vom EA ausgeführt

7.2.8 Fallakte

Die **Fallakte** ist eine *virtuelle* Akte die für einen Verwaltungsvorgang erstellt und ergänzt wird. In Anlehnung an ähnliche Konzepte, die im eHealth Bereich mit den Gesundheits-, Patienten[19]- bzw. Fallakten[20] verfolgt werden, dient sie einem behördenübergreifenden Informations- und Datenaustauch bezüglich eines Falles. In der Fallakte ist keine zentrale und damit von einem einzigen Akteur kontrollierte Datenhaltung vorgesehen. Vielmehr werden Technologien bereitgestellt, über die einzelnen Behörden, EAs, ggfs. auch ausländische Instanzen, ihre jeweiligen, lokal vorgehaltenen Daten selektiv den anderen Behörden zur Verfügung stellen können. Alle Behörden haben so die gleiche Sicht auf die für einen Vorgang relevanten Daten eines Bürgers/Unternehmens und können sich hierdurch besser über einzuleitende Vorgänge abstimmen und eine angemessene Arbeitsteilung definieren. Auch die Beratung des Bürgers/Unternehmens durch seine primären Ansprechpartner (in der Regel für EU-DLR der EA) wird durch die unmittelbare Verfügbarkeit von Daten der beteiligten ZB erleichtert.

Identitätsmanagement ist eine wesentliche Voraussetzung für die unternehmens-/ personenbezogene Zuordnung von Daten zu Fallakten, sowie für Authentisierung, Autorisierung und Zugriff auf die Informationen in der Fallakte.

Da in Deutschland Personenkennzeichen für eine eindeutige Zuordnung zwischen Objekt (Attribut, Fallinformation, Dokument) und Person im globalen verteilten Kontext nicht existieren, muss die Zuordnung durch andere eindeutige Merkmale erfolgen, wie z.B. dienstanbieter- oder bereichsspezifische Kennzeichen.

Im FRESKO-Lösungsvorschlag[21] (FRESKO: Flexibler Einfacher Sicherer Kommunikations-Prozessor) für Prozessketten bzgl. der Meldepflichten für Arbeitgeber wird in einer zukünftigen Ausbaustufe ein „Daten-Pointer-Netzwerk“ (DPN) beschrieben, das die redundante Datenhaltung bei vielen Behörden vermeiden soll, indem ein Register der bei den verschiedenen Behörden vorhandenen Datenbestände verfügbar ist. Mit dessen Hilfe können weitere Behörden auf diese Bestände bzw. Auszüge oder Sichten der Datenbestände zugreifen. Der Zugriff über das DPN ist immer mit der Prüfung der Zulässigkeit der Weitergabe und einer Protokollierung verbunden. Die technische Realisierung wurde jedoch noch nicht spezifiziert, jedoch könnte das FRESKO DPN zukünftig die Realisierung von verteilten Fallakten in Behörden unterstützen.

Folgende Anforderungen werden durch die Fallakte erfüllt:

Komponente	Akteur	Anforderung	Erläuterung
Fallakte	Zuständige Behörde	ZB-A5	Verteiltes System für die sichere Verwaltung und Bearbeitung von Fällen
	Einheitlicher Ansprechpartner	EA-A5	Verteiltes System für die sichere Verwaltung und Bearbeitung von Fällen

[19] eHealth, Gesundheitskarte, http://www.dimdi.de/static/de/ehealth/index.htm
[20] Die elektronische Fallakte, http://www.fallakte.de/
[21] BMI, E-Government 2.0, Forschungsauftrag für "Prozessketten zwischen Wirtschaft und Verwaltung"

7.2.9 Rechtsverbindliche Kommunikation

Kommunizieren DLs mit den EAs und ZBs, so kann dies einerseits mit Portalen, andererseits auch durch E-Mail-Kommunikation erfolgen. Allen Transaktionen gemeinsam ist jedoch die Anforderung, dass eine rechtsverbindliche elektronische Zustellung von Dokumenten bzw. Bescheiden gerade im Behördenumfeld eine wesentliche Rolle spielt um auch Fristen wahren und nachweisen zu können.

Um verbindliche Transaktionen auszuführen, müssen diese überwacht werden, damit zu einem späteren Zeitpunkt ein Nachweis möglich ist. Um Rechtssicherheit zu erreichen, muss sogar eine Beweisbarkeit dieser Transaktionen sichergestellt sein. Nachweisbar können dabei die Urheberschaft der Informationen und die Kommunikationsvorgänge (Nachweisbarkeit des Versands, Zustellung an einen Empfänger) für Beweissicherung und Protokollierung sein.

Für die rechtsverbindliche Kommunikation ist in der Bundesrepublik De-Mail[22] vorgesehen (siehe auch Kapitel 8.2.3 Bürgerportal). Nachrichten und Dokumente sollen dabei zuverlässig und vor Veränderungen geschützt in einem sicheren Kommunikationsraum zwischen registrierten Nutzern versendet werden können.

Für eine grenzüberschreitende Kommunikation im DLR Umfeld eignet sich De-Mail allerdings weniger, da De-Mail nur für registrierte Bürger/Unternehmen/Behörden vorgesehen ist. Ausländische Dienstanbieter[23] können jedoch qualitativ gleichwertige und funktional äquivalente Dienste anbieten, wobei ebenfalls die Prüfung und Anerkennung der Vertrauenswürdigkeit durch eine zuständige Stelle des Mitgliedstaats erfolgen muss.

Folgende Anforderungen werden durch die rechtsverbindliche Kommunikation erfüllt:

Komponente	Akteur	Anforderung	Erläuterung
Rechtsverbind-liche Kommu-nikation	Zuständige Behörde	ZB-A6	Bescheide können rechtssicher zugestellt werden
	Dienstleistungs-erbringer	EA-A6	Bescheide können rechtssicher zugestellt werden

7.3 Vertrauens- und Sicherheitsdienste

Mit der Serviceorientierung wird es möglich, sicherheitsbezogene Dienste wie Identitätsmanagement und auch zentrale Sicherheitsdienste wie eine Public Key Infrastruktur (PKI) auf standardisierte Weise in einer SOA-Umgebung zur Verfügung zu stellen (BSI, 2008), (BITKOM Arbeitskreis SOA Security). Im Idealfall werden, die Identitäts- und Sicherheitsfunktionen von den Fachanwendungen getrennt, um einerseits die Anwendungs- und Dienstentwicklung zu vereinfachen und andererseits

[22] Bürgerportale, De-Mail, http://www.cio.bund.de/DE/E-Government/E-Government-Programm/Buergerportale/buergerportale_node.html

[23] Bürgerportalgesetz Gesetzentwurf, §19 Gleichstellung ausländischer Dienste, http://www.cio.bund.de/cae/servlet/contentblob/318348/publicationFile/15856/gesetzentwurf_buergerportalgesetz_download.pdf

eine hohe Flexibilität zu erreichen. Die technische Umsetzung der Sicherheitsanforderungen und -richtlinien kann auf verschiedene Arten erfolgen.

Das BSI führt für eine serviceorientierte Architektur (SOA) drei Möglichkeiten ein (BSI, 2008):

- durch die Anwendungslogik, so dass die Sicherheitsmethodik in der Anwendung etwa für die feingranulare Zugriffskontrolle verbleibt.
- durch die Verwendung von Sicherheitsdiensten (Security als Service), so dass Sicherheitsdienste von jedem berechtigen Dienst/Anwendung genutzt werden können und damit wieder verwendbar sind.
- durch eine Proxyschicht vor den Diensten und Anwendungen (Security als Infrastruktur), so dass sicherheitsrelevante Funktionen aus Diensten und Anwendungen ausgelagert und durch die Infrastruktur gewährleistet werden.

Eine wesentliche Voraussetzung für die DLR-Umsetzung ist es, dass das Vertrauen der beteiligten Akteure bezüglich der sichereren Umsetzung der DLR-Infrastruktur gewährleistet wird.

Vertrauensdienste unterstützen nicht nur die technischen Aspekte, sondern insbesondere auch nicht technische Vereinbarungen, um ein Vertrauensverhältnis zwischen den beteiligten Akteuren zu etablieren. Dazu werden Verträge unterzeichnet, Absprachen getroffen und Richtlinien verabschiedet.

Security Governance *kümmert sich um Strategie, Definition, Durchsetzung und Steuerung von organisatorischen Regeln, Richtlinien und Standards zur konsequenten Sicherung der Dienste und Geschäftsprozesse mittels geeigneter Steuerungs- und Kontrollmaßnahmen.*

Security Compliance *umfasst die Einhaltung von Verhaltensmaßregeln, Gesetzen und Richtlinien sowie Sicherheitseinstellungen und vergleicht sie mit den vorgegebenen Security Policies, was gegebenenfalls zur Korrektur von Abweichungen führt.*

Abbildung 13: Definition Security Governance und Compliance (Quelle: (BITKOM Arbeitskreis SOA Security))

Um Security Governance und Security Compliance zu gewährleisten, ist der Schutzbedarf der DLR-Prozesse zu ermitteln, um die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen zu schützen. Bei einer Schutzbedarfsfeststellung werden die potentiellen Schäden von IT-Sicherheitsvorfällen hinsichtlich der Beeinträchtigung von Vertraulichkeit, Integrität oder Verfügbarkeit betrachtet. In den BSI-Standards 100-x (BSI-Standards zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit) wird dabei eine Einteilung in die drei Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“ eingeführt.

Werden Identitäts- und Sicherheitsdienste in verschiedenen DLR-Prozessen genutzt oder miteinander komponiert, so ist es erforderlich, dass der Schutzbedarf eines Prozesses durch jeden beteiligten Dienst oder Komponente in gleicher oder höherer Stärke unterstützt wird, da sich ansonsten Sicherheitslücken ergeben und schwach gesicherte Komponenten Angriffsziele darstellen. Für eine sichere Komposition sind daher Konzepte erforderlich, damit ein Dienstanbieter den Nachweis erbringen kann, dass der Dienst einen gewissen Sicherheitslevel einhält. Dies ist eine wichtige Voraussetzung bezüglich der Überprüfung der Einhaltung von Sicherheitsanforderungen.

Sicherheitsdienste wie Vertraulichkeits- und Integritätsdienste schützen Informationen, Dokumente, Nachrichten oder deren Elemente vor unerlaubter Einsichtnahme (Vertraulichkeit) und Manipulation (Integrität). Mit Vertraulichkeits- und Integritätsdiensten sollen Informationen, Dokumente, Nachrichten oder deren Elemente vor Einsichtnahme (Vertraulichkeit), Manipulation (Integrität) und weiteren Risiken (Fälschung des Absenders, Wiedereinspielen von bereits gesendeten Informationen) geschützt werden können. Dies kann durch Verwendung von kryptographischen Mechanismen (Signieren und Verschlüsseln der Nachrichten, Daten oder deren Elementen) oder durch andere Maßnahmen (sichere Transportkanäle) erreicht werden. Die qualifizierte elektronische Signatur kann für die Sicherung der Integrität eines Dokuments verwendet werden. Sie ist allerdings zusätzlich auch ein Nachweis der Authentizität des Unterzeichnenden und sollte mit einem „bewussten" Unterzeichnungsakt einhergehen.

Identifizierungs- und Registrierungsdienste, sowie die **Authentifizierung** wurden in Kapitel 7.1.5 vorgestellt. Allerdings besitzen nicht nur menschliche Benutzer eine Identität, sondern auch Dinge, Ressourcen, Dienste und Komponenten, die ebenfalls identifizierbar sein müssen. In der DLR-Welt können dies beispielsweise Dokumente, Fälle (Vorgänge) oder Identitätsmanagementdienste sein.

Ist ein Nutzer authentifiziert, so kann mit **Autorisierungsdiensten** entschieden werden, was dieser Nutzer darf. Die Autorisierung umfasst die Zuweisung und Überprüfung von Zugriffsrechten auf Daten, Dokumente, Informationen, Informationselemente, Dienste und Ressourcen. Anhand einer Fallakte wird beispielsweise ersichtlich, dass bestimmte Informationselemente dieser Akte von unterschiedlichen Berechtigten mit unterschiedlichen Berechtigungen zugreifbar sein müssen. Je nach Gestaltungsoption der Fallakte ist die konkrete Ausprägung des Berechtigungskonzepts jedoch unterschiedlich. Um nicht für jeden Nutzer einzeln festlegen zu müssen, wofür er autorisiert ist, werden diese in Gruppen zusammengefasst oder ihnen Rollen zugeteilt.

Auch für die DLR-Welt sind bestimmte Rollen wie Mitarbeiter eines einheitlichen Ansprechpartners, anfragender Dienstleistungserbringer oder Mitarbeiter bei der zuständigen Behörde erkennbar, ohne dass bereits ein Rollenkonzept und die zugehörigen Berechtigungen festgelegt wurden. Die Entscheidung, ob ein Zugriff erlaubt wird, ist nicht immer nur von der Authentifizierung und der jeweiligen Gruppe oder Rolle abhängig, sondern kann auch durch weitere Attribute gesteuert werden. So können Handlungsvollmachten vom Dienstleistungserbringer DL an den Einheitlichen Ansprechpartner EA erteilt werden. Auch die Erteilung einer Erlaubnis zum Zugriff auf den persönlichen Safe oder auf Daten im Fallmanagement wäre denkbar. Besonders sensitive personenbezogene Daten wie die im DLR Art. 33 referenzierten Informationen über die Zuverlässigkeit von Dienstleistungserbringern (Informationen über Disziplinar- oder Verwaltungsmaßnahmen, strafrechtliche Sanktionen, Insolvenz oder Konkurs mit betrügerischer Absicht, über IMI europaweit verfügbar) haben einen hohen oder sehr hohen Schutzbedarf und dürfen nur autorisierten Personen zugänglich sein.

Mit **Überwachungs- und Nachweisdiensten** sollen Verbindlichkeit, Nichtabstreitbarkeit und Unleugbarkeit gewährleistet werden. Nachweisbar können dabei die Urheberschaft der Informationen, die Kommunikationsvorgänge (Nachweisbarkeit des Versands, Zustellung an einen Empfänger) für Beweissicherung und Protokollierung sein. So kann auch verbindlich festgestellt werden, wer, wann, auf was zugegriffen hat. Zeitstempeldienste dienen dem Nachweis von Zeitpunkten eines bestimmten Ereignisses wie etwa dem Empfang eines Dokuments. Geeignete Auditingdienste für sicheres Logging sind ebenfalls erforderlich, um nachzuweisende

Ereignisse (Anmeldeversuche, Verletzungen einer Policy, Ausfälle von Security Servern, Zugriffe auf sensitive Daten) fälschungssicher dokumentieren zu können. Die Auditing Policy legt das Verhalten der Dienste fest. Da Überwachung, Nachweis und Datenschutz derzeit kontrovers diskutiert werden, muss das Identitätsmanagement beide Zielsetzungen so umsetzen, dass die beteiligten Parteien vertrauenswürdig miteinander kommunizieren können. Dies kann nur durch nachvollziehbare Geschäftsbedingungen, Richtlinien und Schutzmaßnahmen in der DLR-Infrastruktur umgesetzt werden.

7.4 Fazit

In diesem Kapitel wurden anhand des konkreten Beispiels der EU-Dienstleistungsrichtlinie die Rahmenarchitektur und das Prozessmodell konkretisiert und erläutert.

Es wurden verschiedene Komponenten und Dienste eingeführt, die auf der Rahmenarchitektur und dem Prozessmodell basieren und bestimmte Funktionen für verschiedene Akteure im EU-DLR Kontext bereitstellen. Dies sind eIDs und Authentifizierung im grenzüberschreitenden Kontext, elektronische Safes um Bürger bei der sicheren und vertrauenswürdigen Verwaltung und Freigabe ihrer elektronischen Dokumente gegebenenfalls mit Langzeitarchivierung zu unterstützen, elektronische Beglaubigungen zum Zertifizieren von elektronischen Dokumenten, elektronische Vollmachten für die zeitlich befristete Weitergabe von Attributen bzw. Rechten an vertrauenswürdige Dritte, Fallmanagement und Fallakten für Dienstanbieter um verschiedene Vorgänge datenschutzgerecht in verteilten Umgebungen zu verwalten und rechtsverbindliche Kommunikation für nachweisbares Senden bzw. Empfangen zwischen Akteuren.

Vertrauens- und Sicherheitsdienste dienen der vertrauenswürdigen Verwaltung und Kommunikation in verteilten Umgebungen.

Die vorgestellten Komponenten und Dienste sind jedoch nicht nur für die EU-DLR Umsetzung sinnvoll, sondern dienen als „Bausteine“ für ein umfassendes Identitäts- und Sicherheitsmanagement für verschiedene bürgerfreundliche Anwendungen in Wirtschaft und Verwaltung.

Im folgenden Kapitel werden ausgewählte konkrete technische Komponenten, Initiativen und Standards hinsichtlich ihrer Einordnung in Rahmenarchitektur und Prozesslandkarte betrachtet.

8. Initiativen und Entwicklungen

Basierend auf der Rahmenarchitektur und der Prozesslandkarte werden im diesem Kapitel verschiedene Initiativen und Entwicklungen hinsichtlich ihrer funktionalen Beiträge und Eigenschaften für ein bürgerfreundliches Identitätsmanagement betrachtet.

Zielsetzung ist es, konkrete technische Entwicklungen, Initiativen und Standards zu untersuchen, um festzustellen, welche Komponenten und Dienste des Identitätsmanagements durch diese hauptsächlich abgedeckt werden.

Die Auswahl der betrachteten Entwicklungen wurde durch aktuelle Diskussionen in Fachbeiträgen und Presse über Identitätsmanagement beeinflusst und ist keineswegs vollständig.

8.1 Beschreibung von Initiativen

In diesem Abschnitt werden die wichtigsten Initiativen für Identitätsmanagement eingeführt.

8.1.1 Liberty Alliance

Die Liberty Alliance[24] ist ein globales „Identity Consortium“ das im Jahr 2001 gegründet wurde, mit dem Ziel Standards für föderatives Identity Management zu entwickeln. Heute sind fast 150 Mitglieder aus der ganzen Welt der Liberty Alliance beigetreten.

Die Liberty Alliance betrachtet Identität aus einer ganzheitlichen Perspektive, die Technologie, Geschäftsprozesse und Privatheit umfasst, um den Aufbau eines vertrauenswürdigen globalen Internet für Verbraucher und Unternehmen weltweit zu fördern. Alle Spezifikationen und Frameworks sind online[25] verfügbar.

Ursprünglich hatte sich die Liberty Alliance mehr auf die Sicht der Unternehmen hinsichtlich des Identitätsmanagements konzentriert, jedoch wird das Portfolio von Standards ständig erweitert. Die Spezifikationen umfassen heute unter anderem das Liberty Alliance Identity Assurance Framework, Liberty Alliance Identity Governance Framework, Identity Federation Framework, Identity Web Services Framework, Collection of Identity Services Interface Specifications, usw.

Einordnung in Rahmenarchitektur und Prozesslandkarte:

Die Aktivitäten und Standards der Liberty Alliance sind für alle Akteure, d.h. Anwender, Dienstanbieter und Attribut-Zertifizierer, relevant. Standardisiert werden im Wesentlichen die Authentisierungs- und Autorisierungsdienste, deren Datenstrukturen und Austauschformate, Interaktionen zwischen Akteuren und die technische Umsetzung in Web Services.

8.1.2 Information Card Foundation

Die Information Card Foundation und im deutschsprachigen Raum die Information

[24] Liberty Alliance Web site, http://www.projectliberty.org/

[25] Liberty Alliance Specifications, http://www.projectliberty.org/liberty/specifications__1

Card Foundation DACH-Initiative[26] fokussiert auf den Aufbau eines Netzwerks für die Verbreitung und den Austausch von Informationen über die Technologie der Information Cards.

„Information Card" ist ein offener Standard zur sicheren Authentisierung im Internet. Information Cards ersetzen den klassischen Anmeldeprozess mit Benutzernamen und Passwort durch eine innovative Technologie, die es dem Nutzer ermöglicht seine digitalen Identitäten selbst zu verwalten und mit höchster Sicherheit an verschiedensten Akzeptanzstellen im Internet einzusetzen.

Einordnung in Rahmenarchitektur und Prozesslandkarte:

Information Cards sind eine mögliche Realisierung eines Identity Attribute Data Repository des Anwenders/Bürgers. Information Cards dienen der Authentisierung im Internet.

In den spezifischen Entwicklungen (siehe Kapitel 8.2.6 Nutzerzentrierte Entwicklungen) werden auch der Attribute Certification Service zur Initiierung der Zertifizierung von Attributen beim Attribut-Zertifizierer und der Authentication Service für die Authentisierung beim Dienstanbieter realisiert.

8.1.3 OSIS

Unter dem Namen „The Open-Source Identity System (OSIS)“[27] arbeitet eine Gruppe von Open Source-Entwicklern, die Identitätsmanagement-Systeme/Projekte interoperabel gestalten möchten, indem eine interoperable Identitäts-Schicht für das Internet aus kommerziellen und Open Source Lösungen entwickelt wird. OSIS hat einige Tabellen veröffentlicht, die Testergebnisse bezüglich der Interoperabilität von verschiedenen Protokollen, Entwicklungen und Systemen liefern. Aktuelle Projekte umfassen z.B. die Interoperabilität von Information Card und OpenID-Implementierungen und das Testen von identitätsrelevanten Protokollen wie zum Beispiel SAML, Information Cards, OpenID und WS-Federation.

Einordnung in Rahmenarchitektur und Prozesslandkarte:

OSIS Entwicklungen dienen der Interoperabilität der jeweiligen Authentisierungs- und Autorisierungsdienste.

8.2 Beschreibung von Standards, Entwicklungen und Produkten

8.2.1 Elektronischer Personalausweis

Beschreibung:

Neben den hoheitlichen Ausweisfunktionen wird der neue elektronische Personalausweis die "Online-Authentisierung" von eBusiness- und eGovernment-Dienstanbietern und dem Bürger als Ausweisinhaber unterstützen (wie schon in Kapitel 7.1.2. erwähnt).

Durch Online-Authentisierung wird es berechtigten Dienstanbietern ermöglicht, auf sichere Art und Weise unter der Kontrolle des Inhabers bestimmte im Chip gespeicherte Daten auszulesen. Dabei muss sich der Dienstanbieter durch ein

[26] Information Card Foundation DACH-Initiative, http://www.informationcard.de/ , Information Card Foundation, http://informationcard.net/

[27] OSIS, http://osis.idcommons.net/wiki/Main_Page

Zertifikat als berechtigt ausweisen. Dies ermöglicht eine sichere gegenseitige Identifizierung.

Eine weitere, optionale Anwendung des elektronischen Personalausweises ist die Signaturfunktion, wie sie bereits heute auf separaten Signaturkarten zu finden ist. Diese Anwendung wird vom Ausweisinhaber nachträglich bei Bedarf aktiviert.

Abbildung 14: Funktionen des elektronischen Personalausweises (Quelle: Bundesministerium des Inneren[28])

Einordnung in Rahmenarchitektur und Prozesslandkarte:

Der elektronische Personalausweis ist ein Teil eines Identity Attribut Data Repository, das die hoheitlichen Identitätsattribute enthält. Der Zugriff auf dieses Repository wird durch zertifizierte Kartenleser und standardisierte Protokolle unterstützt (siehe auch eCard-API im folgenden Abschnitt).

Die Berechtigung für den Zugriff auf die Attribute des elektronischen Personalausweises wird durch Berechtigungszertifikate realisiert, d.h. eine Realisierung des Authorization Data Repositories als Datenspeicher für Berechtigungen bei Dienstanbieter oder Attribut-Zertifizierer.

Gemäß Prozesslandkarte ist die Authentisierung von Nutzern das wesentliche Einsatzgebiet.

8.2.2 eCard-API

Beschreibung:

Die eCard-Strategie der Bundesregierung förderte eine vielseitige Verwendung der im Rahmen der verschiedenen Kartenprojekte der Bundesverwaltung ausgegebenen und genutzten Chipkarten. Für die Realisierung der Strategie wurde als Baustein das eCard-API-Framework spezifiziert.

Das Ziel des eCard-API-Frameworks[29] ist das Bereitstellen einer einfachen und

[28] Der elektronische Personalausweis, http://www.bsi.de/fachthem/elekausweise/epersausweis.htm

[29] BSI, eCard-API-Framework, http://www.bsi.de/literat/tr/tr03112/api/1.0/teil1.pdf

homogenen Schnittstelle, um in verschiedenen Anwendungen eine einheitliche Nutzung von unterschiedlichen Chipkarten (eCards) wie elektronische Gesundheitskarte und elektronischer Personalausweis zu ermöglichen.

Das eCard-API-Framework wird in die folgenden Ebenen untergliedert:

- Application-Layer: Im Application-Layer befinden sich die verschiedenen Anwendungen, die das eCard-API-Framework für den Zugriff auf die eCards und damit verbundene Funktionen nutzen wollen.
- Identity-Layer: Der Identity-Layer umfasst das eCard-Interface und das Management-Interface und somit Funktionen für die Verwaltung und Nutzung Digitaler Identitäten sowie für das Management des eCard-API-Frameworks
- Service-Access-Layer: Der Service-Access-Layer bietet insbesondere Funktionen für kryptographische Primitive und biometrische Mechanismen in Verbindung mit kryptographischen Token.
- Terminal-Layer: Der Terminal-Layer übernimmt die Generalisierung von konkreten Lesertypen und verschiedenen Schnittstellen sowie die Kommunikation mit der Chipkarte.

Einordnung in Rahmenarchitektur und Prozesslandkarte:

Das eCard-API-Framework unterstützt die Authentifizierung eines Nutzers mittels Chipkarten bei einem Dienstanbieter. Für den Nutzer wird die eCard-API in einem Bürger-Client[30] umgesetzt.

Für den Dienstanbieter unterstützt das eCard-API den autorisierten Zugriff auf bestimmte Attribute auf der jeweiligen Chipkarte. Dazu besitzt der Dienstanbieter ein Zugriffszertifikat (dies entspricht dem Berechtigungszertifikat für den elektronischen Personalausweis), das der Authentisierung und Autorisierung des Dienstanbieters dient.

8.2.3 Bürgerportal

Beschreibung:

Ab 2010 sollen so genannte Bürgerportale[31] einen vertrauenswürdigeren Geschäftsverkehr im Internet ermöglichen. Die Bundesregierung hat einen diesbezüglichen Gesetzentwurf[32] verabschiedet. Im Mittelpunkt der Bürgerportale steht künftig der Service "De-Mail". De-Mail soll eine rechtsverbindliche elektronische Kommunikation ermöglichen, die im Streitfall auch vor Gerichten Beweiskraft hat. Dies umfasst zum Beispiel Garantien für eine unverfälschte Übermittlung der Inhalte, die Möglichkeit einer korrekten Identifikation der Kommunikationspartner und die zweifelsfreie Nachvollziehbarkeit des Versands einer Nachricht. De facto etabliert De-Mail eine geschlossene Benutzergruppe für den abgesicherten E-Mail-Verkehr. De-Mail-Anbieter müssen in einem staatlichen Zertifizierungsverfahren nachweisen, dass sie die Anforderungen an Sicherheit und Datenschutz erfüllen.

Das Konzept wird ergänzt durch eine sichere Dokumentenablage (De-Safe) und einen Identitätsnachweis (De-Ident). De-Safe unterstützt die veränderungssichere und

---

[30] Gemäß BSI ist der Bürger-Client eine Middleware, die die Kommunikation zu Kartenlesegerät, Chipkarte und der Serverkomponente eID-Server herstellt.

[31] BMI, http://www.cio.bund.de/cln_093/sid_1D9A89F50EAB25CED61CFB0C0FA07D2A/DE/E-Government/E-Government-Programm/Buergerportale/buergerportale_node.html

[32] Gesetzentwurf Bürgerportale, http://www.cio.bund.de/

dauerhafte Speicherung von elektronischen Dokumenten. De-Ident stellt auf Anforderung des Nutzers so genannte Ident-Nachweise durch einen Anbieter aus.

Die Technischen Richtlinien sind durch das BSI veröffentlicht worden[33], jedoch sind noch keine Produkte für das Bürgerportal vorhanden.

Einordnung in Rahmenarchitektur und Prozesslandkarte:

Das Bürgerportal mit der Komponente De-Mail, und optional De-Safe und De-Ident ist für die rechtsichere Kommunikation zwischen Bürgern, Dienstanbietern und Attribut-Zertifizierern konzipiert. Hauptanwendungsbereich ist daher die Nachvollziehbarkeit von Ereignissen (Logging Service).

De-Safe ist eine mögliche Umsetzung eines eSafes aus Kapitel 7.2.1, jedoch mit minimalem Funktionsumfang.

De-Ident ist ein Attributnachweis, der vom Nutzer ausgewählte und freigegebene Identitätsdaten enthält und mittels De-Mail an eine andere De-Mail-Adresse gesendet wird. Die Attribute werden qualifiziert elektronisch signiert, um die Korrektheit der übermittelten Daten zu bestätigen.

8.2.4 S.A.F.E.

Beschreibung:

S.A.F.E.[34] (Secure Access to Federated E-Justice/E-Government) ist ein Projekt im Rahmen von Deutschland-Online zur Realisierung einer wirtschaftlichen Kommunikationsinfrastruktur für das E-Government. Definiert wird ein technisches Rahmenwerk für eine interoperable und sichere Nutzung Digitaler Identitäten über administrative Domänengrenzen (Trust-Domain) hinweg. Technisch setzt S.A.F.E. auf dem Web Service Stack („WS-*“) von OASIS und W3C auf und konkretisiert die eingesetzten Standards durch entsprechende Profile, um die Interoperabilität zu verbessern. Bestehende Identitätsinfrastrukturen werden durch standardisierte Schnittstellen gekapselt. Das S.A.F.E.-Konzept ist zweistufig aufgebaut:

- Generische, Fachdomänen-übergreifende Schnittstellen-Definition
- Justiz-spezifische Ausprägung mit Erweiterungen zur Ablösung des aktuellen Registrierungsservers

Das Grobkonzept und die Feinkonzeption stehen zur Verfügung.

Einordnung in Rahmenarchitektur und Prozesslandkarte:

Das S.A.F.E.-Konzept beschreibt ein technisches Rahmenwerk für einen ganzheitlichen Umgang mit Identitäten im Kontext von Web Service basierten E-Government-Kommunikationen. Das technische Rahmenwerk definiert lediglich Schnittstellen in Form von Kommunikationsprotokollen mit dem Ziel, eine technische Interoperabilität zu gewährleisten. Es macht dagegen weder Vorgaben zur konkreten Realisierung der Dienste noch zu organisatorischen oder rechtlichen Richtlinien und Prozessen.

Das S.A.F.E.-Konzept entspricht daher einem möglichen technischen Umsetzungskonzept für die in diesem Dokument vorgeschlagene Rahmenarchitektur und die Prozesse der Prozesslandkarte. Die einzelnen Funktionen von S.A.F.E.

[33] BSI, http://www.bsi.bund.de/fachthem/egov/buergerportal.htm

[34] S.A.F.E. http://www.deutschland-online.de/DOL_Internet/broker.jsp?uMen=404209ab-8d40-9114-fbf1-b1ac0c2f214a

wurden nicht im Detail hinsichtlich ihrer Abbildbarkeit auf die Komponenten und Dienste der Rahmenarchitektur untersucht.

8.2.5 SAML

Beschreibung:

Die Security Assertion Markup Language (SAML) ist eine XML-basierte Sprache für Sicherheitsbestätigungen. Sie stellt Funktionen bereit, um sicherheitsbezogene Informationen zu beschreiben und zu übertragen. SAML ist daher eine „gemeinsame Sprache", in der Dienste/Provider Sicherheitsinformationen kommunizieren können, ohne ihre internen Sicherheitsarchitekturen zu verändern. Der SAML Standard umfasst dabei mehrere Konzepte die in Abbildung 15 dargestellt sind.

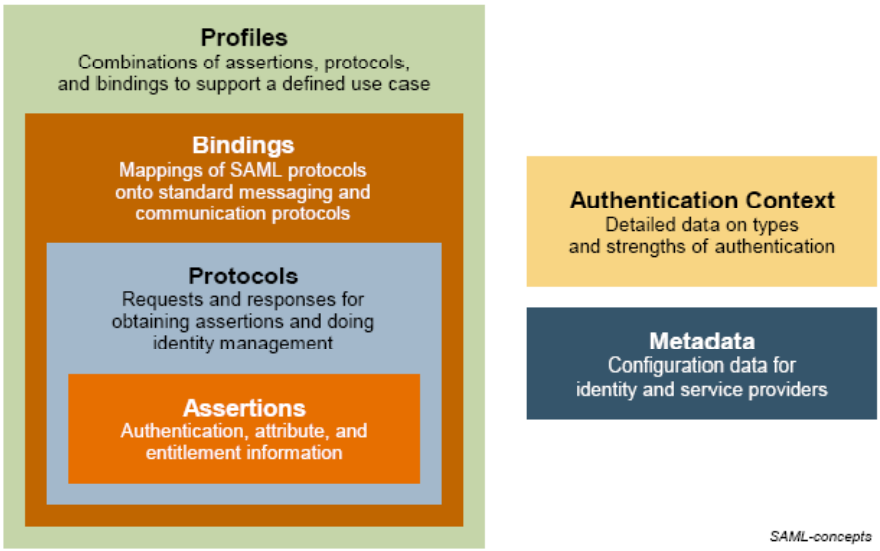


Abbildung 15: SAML Konzepte (Quelle: SAML 2.0 Technical Overview[35])

SAML Assertions: Eine SAML Assertion ist ein XML-Dokument mit bestimmter Syntax, das eine Aussage bezüglich Identität oder Berechtigung trifft. Verschiedene Assertions sind möglich:

- *Authentication*: Aussage bezüglich bestimmter Identitäts- und Authentifizierungsattribute eines Nutzers;
- *Attribute*: Aussage über bestimmte statische (z.B. Rolle, Mitgliedsstatus) oder dynamische (z.B. Kontostand, Ort) Attribute eines Nutzers;
- *Authorization Decision*: Aussage über bestimmte Berechtigungen eines Nutzers, die festlegen, ob und wie auf eine spezifische Ressource zugegriffen werden darf.

Einordnung in Rahmenarchitektur und Prozesslandkarte:

SAML definiert oder implementiert keine neuen kryptografische Verfahren und enthält ebenfalls keine neue Technik für Authentifizierung und Autorisierung. SAML Assertions sind ein Austauschformat, um Attribute einer Digitalen Identität zu zwischen Entitäten zu kommunizieren. Dabei können auch Aussagen über den Kontext der Attribute, z.B. dem verwendeten Authentifikationsverfahren getroffen werden.

---

[35] OASIS, SAML 2.0 Technical Overview, 13 März 2007, http://www.oasis-open.org/committees/download.php/23920/sstc-saml-tech-overview-2.0-cd-01.pdf

Bezüglich der Rahmenarchitektur sind die durch SAML kommunizierbaren Attribute im Identity Attribute Data Repository oder User Authorization Repository enthalten. SAML Assertions dienen dem Nachweis von Authentifizierungs- bzw. Autorisierungsattributen. Die SAML Assertions werden vom Attribut-Zertifizierer ausgestellt.

8.2.6 Nutzerzentrierte Entwicklungen

Beschreibung:

Ein neuer Lösungsansatz für die einfache und sichere Nutzung von Attributen der Digitalen Identität ist das sogenannte nutzerzentrierte Identitätsmanagement. Der Grundgedanke ist, dem Nutzer die alleinige Kontrolle über seine persönlichen Daten und deren Übermittlung an Dienstanbieter zu übergeben. In Anlehnung an die breite Verwendung von Geschäftskarten wie Kreditkarten, EC-Karten und Visitenkarten wird dem Nutzer eine elektronische Brieftasche mit sogenannten „Information Cards“ zur Verfügung gestellt. „Information Cards“ sind eine bildliche Darstellung von Identitätsattributen in Form von rechteckigen Icons. Das Ziel von „Information Cards“ ist es, dem Benutzer eine Auswahl von Identitätsattributen zu präsentieren, damit er eine geeignete auswählen kann, um einen Dienst/Ressource bei einem Dienstanbieter zu nutzen.

Verschiedene Implementierungen und Ausprägungen von Information Cards sind verfügbar, wie z.B. Microsoft CardSpace, Open Source Higgins und OpenID. Die Funktionalität der Implementierungen ist unterschiedlich, z.B.:

- *CardSpace* ist Bestandteil des Microsoft .NET Frameworks. CardSpace ist eine Information Card Technologie zur Identitätsverwaltung und kann zur Authentifizierung und/oder Identifizierung gegenüber Webseiten und Web Services genutzt werden. Unter Windows Vista wird CardSpace mitgeliefert, bei Windows XP kann es nachträglich installiert werden. CardSpace unterstützt verschiedenen Typen von Information Cards, nämlich P-Cards, die vom Nutzer selbst ausgestellt werden, und M-Cards, die von einem Attribut-Zertifizierer ausgestellt werden.
- *Higgins* definiert eine Identity Management Framework, um Nutzern eine einheitliche Schnittstelle für verschiedene Identitätsdaten anzubieten. Im Higgins Datenmodell werden Identitätsdaten in Identitäts-, Profil- und Beziehungsdaten unterschieden. Identitätsdaten dienen der Identifikation und Authentifikation, Profildaten können Vorlieben, Interessen, Wunschlisten usw. sein, Beziehungsdaten beinhalten Verbindungen zwischen verschiedenen Attributen.
- *OpenID* hat den einfachen Grundgedanken, dass sich ein Nutzer über eine eindeutige URL identifiziert, die ihm “gehört”. Was OpenID macht, ist die URL (Identitätsattribute) eines Benutzers zu prüfen. Um eine OpenID zu erhalten registriert man sich bei einem OpenID Provider (ein Attribut-Zertifizierer) und hinterlegt dort die Attribute, die man potenziell an andere Webseiten weitergeben will.

Einordnung in Rahmenarchitektur und Prozesslandkarte:

Alle nutzerzentrierten Entwicklungen sind mögliche Realisierungen eines Identity Attribute Data Repository des Anwenders/Bürgers. Unterschiedlich ist der Speicherort der jeweiligen Attribute, dies kann bei dem Nutzer selbst oder bei einem Attribut-Zertifizierer sein. Der Zugriff auf die Attribute seiner Digitalen Identität wird vom Nutzer kontrolliert, d.h. der Nutzer entscheidet, welche Attribute an einen Dienstanbieter

übermittelt werden.

Eingesetzt werden die nutzerzentrierten Entwicklungen, um eine einfache Authentifizierung des Nutzers bei einem Dienstanbieter zu ermöglichen. Die nutzerzentrierten Entwicklungen umfassen jedoch nicht Autorisierungsentscheidungen bei dem Dienstanbieter und bieten bisher auch keine Kontrolle über die Weitergabe der Attribute, nachdem der Dienstanbieter diese erhalten hat.

8.2.7 Produkte für Identitätsmanagement

In der vorliegenden Studie werden Produkte für das Identitätsmanagement nicht im Einzelnen betrachtet.

Hier sei auf die CSC-Studie „Identity Management – A Comparison of Identity Management Solutions“ verwiesen (Steinacker, 2009).

In der CSC-Studie werden Identity Management Lösungen hinsichtlich der Unterstützung verschiedener Funktionalitäten und Dienste analysiert, wie z.B. Unterstützung des Managements von Identitäten, Zugriffsmanagement, Rollenmanagement und Governance. In der Studie wird deutlich, dass Identitätsmanagement Produkte nicht funktional gleich sind, sondern verschiedene Produkte bestimmte funktionale Schwerpunkte setzen.

8.3 Fazit

In diesem Kapitel wurde eine Auswahl von konkreten technische Entwicklungen, Initiativen und Standards hinsichtlich ihrer funktionalen Einordnung bezüglich Rahmenarchitektur und Prozesslandkarte untersucht.

Generell ist festzustellen, dass die beschriebenen Standards und Entwicklungen jeweils nur Teilbereiche des Identitätsmanagements abdecken. Auch Identitätsmanagement-Produkte sind funktional unterschiedlich, mit unterschiedlichen Schwerpunkten.

Die vorgestellten Initiativen und Entwicklungen decken die folgenden Funktionen für das Identitätsmanagement ab:

- Elektronischer Personalausweis – Authentifikation
- eCard API – Authentifikation, teilweise Autorisierung
- Bürgerportal/De-Mail – Authentifikation und Auditing
- S.A.F.E. – Administration, Authentifikation, Autorisierung und Audit
- SAML – Authentifikation und Autorisierung
- Nutzerzentrierte Entwicklungen – Authentifikation, teilweise Autorisierung
- Identitätsmanagement-Produkte - je nach Funktionsumfang: Administration, Authentifikation, Autorisierung und Audit

Identitätsmanagement ist als Verbund von Komponenten und Diensten zu sehen, die technisch unterschiedlich realisiert werden können. Da bisher Schnittstellen und Protokolle zwar vorhanden aber noch nicht aufeinander abgestimmt sind, sind Interoperabilitätsaspekte aus technischer, organisatorischer, semantischer und rechtlicher Sicht zukünftig noch detaillierter zu untersuchen.

Im folgenden Kapitel wird ein Ausblick auf die aktuellen Entwicklungen wie SOA und Cloud Computing gegeben.

9. Ausblick

Ein Ziel der vorliegenden Studie war es, weitere Schritte zu identifizieren, die die Umsetzung eines bürgerfreundlichen Identitätsmanagements fördern und möglich machen.

Als erster Schritt ist eine Publikation der Ergebnisse dieser Studie notwendig. In Kap. 8 wurden bereits existierende Initiativen und Entwicklungen beschrieben, die durch die vorliegenden Ergebnisse ergänzt werden sollten.

Um die Ergebnisse auch im europäischen Umfeld in die entsprechenden Gremien einbringen zu können und die weitere Entwicklung zu beeinflussen, sollten die Ergebnisse auch in diesem Umfeld dargestellt werden,

Wir empfehlen, die in dieser Studie entwickelte Rahmenarchitektur mit den dort festgelegten Modulen und Komponenten, in die entsprechenden Gremien einzubringen.

Die erarbeiteten Ergebnisse können Unternehmen, insbesondere Dienstanbieter und Attribut-Zertifizierer, als Unterstützung für eine zukünftige Entwicklung ihrer Produkte dienen, um die entsprechenden Dienste und Funktionen für Bürger bereitzustellen. Hierzu sind die Ergebnisse in entsprechend geeigneter Form, vorzugsweise auf Englisch, darzustellen.

Hierin liegen auch die Chancen für den Bürger: dass sich auf der Basis der vorliegenden Ergebnisse ein Wettbewerb zwischen den existierenden und neuen Attribut-Zertifizierern entwickelt, der dem Bürger die Wahl zwischen verschiedenen Anbietern bietet und so zu einer entscheidenden Verbesserung im Sinne des bürgerfreundlichen Identitätsmanagement beiträgt.

Für Entwicklungen wie SOA und Cloud Computing sind weitere Untersuchungen notwendig, die ein bürgerfreundliches Identitätsmanagement in dem jeweiligen Kontext untersuchen. In den folgenden Abschnitten werden einige dieser Themen angerissen, um die entsprechenden Fragestellungen aufzuzeigen.

9.1 Federation

Der Begriff Föderation, engl. Federation, bedeutet im Allgemeinen ein Bündnis oder einen Verbund von verschiedenen Organisationen (Wahrig, 2002).

Im Kontext des Identitätsmanagement ist damit zunächst einmal der Verbund von Organisationen, ursprünglich von Unternehmen, gemeint, von denen ein Unternehmen dem anderen einen Dienst anbietet, somit in unserem Sprachgebrauch einen Dienstanbieter darstellt, und die Mitarbeiter der anderen Organisationen diese Dienste nutzen können.

Im engeren Sinne, insbesondere bei Verwendung des englischen Begriffs Federation, sind damit die organisatorischen, technischen und rechtlichen Vereinbarungen gemeint, die notwendig sind, um die Nutzung der angebotenen Dienste zu ermöglichen, ohne dass der Dienstanbieter die Identitäten der Dienstnutzer eigenständig verwalten muss.

Damit wurde den immer wachsenden Herausforderungen begegnet, dass Unternehmen ihre Anwendungen und Dienste Dritten wie Kunden, Partnern oder sogar konkurrierenden Unternehmen öffnen (müssen), um ihre Geschäfte durchführen zu

können. Dies sollte in einer sicheren und in Übereinstimmung mit den geltenden Regelungen Art und Weise geschehen.

Diese Anforderungen stellen einen weiteren potentiellen Aufwand für die Verwaltung von internen und externen Nutzern dar, der explodieren kann, je mehr Unternehmen sich zusammenschließen.

So kann z.B. ein Unternehmen, das Produkte herstellt und vertreibt, seinen Kunden eine eigene Anwendung, den Dienst, zur Verfügung stellen, sodass die Kunden ihre Bestellungen direkt mit dieser Anwendung aufgeben können. Federation belässt die Verwaltung der Identitäten dann bei dem Kunden-Unternehmen. Die beiden Unternehmen haben sich organisatorisch, technisch und vertraglich darauf geeinigt, welche Attribute an den Dienstanbieter geliefert werden müssen und wie ein Attributzertifikat aussehen muss, um vom Dienstanbieter akzeptiert zu werden. Damit ist der Kunde meist selbst in der Rolle des Attribut-Zertifizierers.

Federation lässt zu, dass die (partiellen) Identitäten und die entsprechenden Attribute einmal bei einer Instanz verwaltet werden und die Arbeit dazu nicht vervielfältigt wird.

Damit stellt Federation keinen neuen Sachverhalt dar, sondern einen speziellen Blick auf die in den vorangegangenen Kapiteln beschriebenen Sachverhalte. Auch hier ist Vertrauen zwischen den beteiligten Instanzen das wesentliche Element, das zwischen dem Dienstanbieter und dem Dienstnutzer herrschen muss, damit der einzelne Nutzer als Mitarbeiter des Unternehmens z.B. einen vereinfachten Zugang (Simplified Sign-On) zu den Diensten erhält.

Für die Unternehmen bedeutet dies, dass sie eine Vertrauensbeziehung zwischen den beteiligten Partnern entwickeln und erhalten müssen und dass sie entsprechende Vereinbarungen treffen müssen, um diese Vertrauensbeziehung abzusichern und Detailfragen wie Sicherheit, Datenschutz personenbezogener Daten, Haftungsfragen und Verrechnungsmodalitäten zu klären.

Bezüglich des Datenschutzes personenbezogener Daten kann Federation sogar zu einer Verbesserung führen, da je nach (technischer) Ausprägung die Verbreitung personenbezogener Daten deutlich reduziert werden kann.

Des Weiteren müssen auch die technischen Spezifikationen festgelegt, die technische Infrastruktur dazu entwickelt und der tägliche Betrieb der Federation Dienste durchgeführt werden

Für eine Beschreibung der aktuellen technischen Standards wie WS* zu Federation sei auf die einschlägige Literatur, z.B. (Fumy, Walter; Sauerbrey, Joerg, 2006) oder (Mezler-Andelberg, 2008) verwiesen.

9.2 Service-Oriented Architecture

Der Begriff Service-Oriented Architecture (SOA) beschreibt den Entwurf und die Struktur eines IT Systems, in dem die einzelnen Module Dienste anbieten, die, richtig zusammengesetzt (»orchestriert«), die Geschäftsprozesse unterstützen und beliebig wieder verwendbar sind (Hurwitz, 2007).

Der SOA-Leitfaden (BITKOM Arbeitskreis SOA-Technologies, 2009) definiert eine SOA als „ein Konzept, welche das Geschäft und die IT eines Unternehmens nach Diensten strukturiert, welche modular aufgebaut sind und flexibel zur Umsetzung von Geschäftsprozessen genutzt werden können“.

Nach (Mezler-Andelberg, 2008) lässt sich eine SOA gut mit dem Bauen mit

Legosteinen vergleichen und daran entsprechende Vor- und Nachteile beschreiben:

Vorteile des Bauens mit Lego-Steinen	Nachteile des Bauens mit Lego-Steinen
Lego-Steine sind vollständig kompatibel	Lego-Steine sind nur untereinander kompatibel
Lego-Steine sind robust	Die Stärken der Lego-Steine sind ein Nachteil für die Hersteller
Lego-Steine sind wiederverwendbar	Lego-Bauwerke haben eine begrenzte Stabilität
Lego-Steine sind miteinander kombinierbar	Jeder kann mit Lego-Steinen spielen, aber nicht jeder kann Lego-Land aufbauen

Tabelle 7: Analogie SOA und Lego-Steine (nach (Mezler-Andelberg, 2008))

Für ein Identitätsmanagement bedeutet SOA keine neuen Funktionen; die in den vorangegangenen Kapiteln diskutierten Elemente werden (noch) stärker im Kontext modularer Dienste betrachtet. Ein wesentliches Element ist auch hier das Vertrauen zwischen Dienstanbieter und Attribut-Zertifizierer.

9.3 Identity Management und »The Cloud«

In jüngster Zeit ist der Begriff »Cloud Computing« als weiteres Thema aufgetaucht, in dem viele Facetten stecken und bei dem es unterschiedliche Meinungen über die genauen Inhalte gibt. Um den Nebel der Wolke ein wenig zu lichten, werden im Folgenden kurz die grundlegende Eigenschaften der »Cloud« vorgestellt; diese Darstellung orientiert sich an dem empfehlenswerten Artikel des Berkeley RAD Labors (Armbrust, 2009).

Cloud Computing *bezieht sich sowohl auf die Anwendungen, die über das Internet als Dienste angeboten werden, als auch auf die Hardware und die System-Software in den Rechenzentren, die diese Dienste anbieten.*

Die Dienste selbst werden seit langem als ***Software as a Service*** *(SaaS) bezeichnet. Die* ***Cloud*** *umfasst die Hardware und die System-Software in den Rechenzentren.*

Wenn nun eine »Cloud« der Öffentlichkeit zugänglich gemacht wird und die Dienste leistungsabhängig, z.B. nach Prozessornutzung pro Stunde oder Speicherplatz pro Tag, bezahlt werden müssen, dann spricht man von einer ***Public Cloud****; der angebotene Dienst heißt* ***Utility Computing****. Unter* ***Private Cloud*** *versteht man Rechenzentren, die ihre Dienste einem Unternehmen oder Organisation anbieten, aber nicht der allgemeinen Öffentlichkeit zugänglich machen.*

Daher wird als ***Cloud Computing*** *die Summe der SaaS und Utility Computing bezeichnet, schließt aber explizit Private Clouds aus.*

Damit gibt es Anbieter von SaaS ebenso wie deren Nutzer als auch Anbieter und Nutzer von Utility Computing.

Abbildung 16: Definition von Cloud Computing nach (Armbrust, 2009)

So erweitert Cloud Computing den Servicegedanken auch auf Infrastruktur und Plattformen. Hinsichtlich des Identitätsmanagements gibt es daher vergleichbare Dienste wie unter Federation und SOA. Dennoch bedürfen hier einige Aspekte weiterer Untersuchungen, da diese in SOA und Federation so nicht auftreten. Hier seien nur einige Beispiele genannt.

- Wie können Identitätsmanagementdienste zwischen Anbietern von Utility Computing und deren Nutzern aussehen und entsprechendes Vertrauen geschaffen werden?
- Wie lässt sich dieses Vertrauen auf die Nutzer von SaaS übertragen? Beispiel: Ein SaaS-Nutzer weiß nicht, dass der SaaS-Anbieter die Identitätsdaten den Nutzer bei einem Utility Computing-Anbieter lagert und dies möglicherweise in einem Land, in dem die entsprechenden rechtlichen Bedingungen nicht dem Land des SaaS-Nutzers entsprechen.

Für eine sichere und bürgerfreundliche Nutzung des Cloud Computing ist die Beantwortung dieser und weitere Fragen zwingend notwendig; hier sind noch tiefgreifende Untersuchungen und Studien notwendig, die die Gedanken der vorliegenden Studie weiter entwickeln.

10. Literaturverzeichnis

Armbrust M. et al. Above the Clouds: A Berkeley View of Cloud Computing [Online]. - 10. February 2009. - 05. July 2009. - www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf.

BITKOM Arbeitskreis SOA Security SOA und Security [Online]. - http://soa-know-how.de/index.php?id=45&tx_bccatsandauthors[catid]=181.

BITKOM Arbeitskreis SOA-Technologies SOA-Leitfaden - Online Version [Online] // SOA-Know-How.de. - 2009. - http://www.soa-know-how.de/index.php?id=45.

BITKOM Chipkartenprojekte in Deutschland und Europa – eine Zwischenbilanz nach drei Jahren E-Card-Strategie der Bundesregierung [Online]. - 02. 04 2008. - 08. 01 2009. - http://www.bitkom.org/files/documents/StN_Entwurf_Chipkartenprojekte_D_EU_fin.pdf.

Breitenstrom Christian, Brunzel Marco und Klessmann Jens FOKUS White Paper eSafe [Online]. - 19. 12 2008. - http://www.fokus.fraunhofer.de/de/elan/_docs/_HPPGruppe/FOKUS_White_Paper_eSafe_081219_V1.pdf.

BSI SOA-Security-Kompendium, Sicherheit in Service-orientierten Architekturen, Bonn 2008. [Online]. - 2008. - http://www.bsi.de/literat/studien/soa/SOA-Security-Kompendium.pdf.

BSI, Bürgerportale Bürgerportale – eine Infrastruktur für sichere Kommunikatio; Technische Richtlinien [Online]. - https://ssl.bsi.bund.de/fachthem/egov/buergerportal.htm.

Bund-Länder-Ausschuss Dienstleistungswirtschaft Anforderungsprofil für „Einheitliche Ansprechpartner". - Berlin : Bundesministerium für Wirtschaft und Technologie, 1. 10 2007.

EU-DLR Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates über Dienstleistungen im Binnenmarkt [Online]. - 12. 12 2006. - 24. 02 2009. - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:376:0036:0068:DE:PDF.

Europäische Kommission Handbuch zur Umsetzung der Dienstleistungsrichtlinie [Buch]. - Luxemburg : Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaft, 2007. - ISBN 978-92-79-05979-7.

Ferraiolo David F., Kuhn D. Richard and Chandramouli Ramaswamy Role-Based Access Control, Second Edition [Book]. - Norwood, MA : Artech House, 2007.

Fumy, Walter; Sauerbrey, Joerg Enterprise Security [Buch]. - Erlangen : Publicis Corporate Publishing, 2006.

Hristova Ralitsa Die Bedeutung des Personenidentifikators in der Entwicklung des E-Government [Online]. - 10. 02 2005. - 24. 02 2009. - http://www.alexandria.unisg.ch/EXPORT/DL/13203.pdf.

Hühnlein Detlef Identitätsmanagement - Eine visualisierte Begriffsbestimmung [Journal] // DuD. - 2008. - S. 161-163.

Hurwitz J. et al. Service Oriented Architecture for Dummies [Buch]. - Indianapolis : Wiley Publishing, Inc., 2007.

IDABC eID Interoperability for PEGS Proposal for a multilevel authentication mechanism and a mapping of existing authentication mechanisms [Online]. - 12 2007. - http://ec.europa.eu/idabc/servlets/Doc?id=29622.

IDABC eID Interoperability for PEGS; Common specifications for eID interoperability in the eGovernment context [Online]. - 12 2007. - 24. 02 2009. - http://ec.europa.eu/idabc/servlets/Doc?id=30989.

ISPRAT Whitepaper Elektronisches Identitätsmanagement [Online]. - 11 2008. - 09. 01 2008. - http://www.isprat.net/html/downloads/it_gipfel_2008/ISPRAT_Whitepaper_Elektronische_%20Identitaeten.pdf.

Kommission der Europäischen Gemeinschaften i2010 – Eine europaeische Informationsgesellschaft fuer Wachstum und Beschaeftigung. [Online]. - 01. 06 2005. - 24. 02 2009. - http://eur-lex.europa.eu/LexUriServ/site/de/com/2005/com2005_0229de01.pdf.

Lahno B. Sonderthema: Vertrauen [Journal] // Helaba Geschäftsbericht 2008. - 2008. - S. 73-83.

Mezler-Andelberg C. Identity Management - Eine Einführung [Buch]. - Heidelberg : dpunkt.verlag, 2008.

OMG Object Management Group [Online] // Business Process Modeling Notation, V1.1, OMG Document Number: formal/2008-01-17. - January 2008. - 19. March 2009. - http://www.omg.org/spec/BPMN/1.1/PDF.

Steinacker Angelika et al. CSC Study Identity Management - A Comparison of Identity Management Solutions [Bericht]. - 2009.

STORK project D2.1 Framework Mapping of Technical/Organisational Issues to a Quality Scheme [Online]. - 13. 10 2008. - http://www.eid-stork.eu/dmdocuments/D2.1_v_1%205-def._1.pdf.

STORK project D2.3 Quality authenticator scheme [Online]. - 03. 03 2009. - http://www.eid-stork.eu/dmdocuments/D2.3_final._1.pdf.

von Lucke, J., Eckert, K.-P., Breitenstrom, C. IT-Umsetzung der EU-Dienstleistungsrichtlinie – Gestaltungsoptionen, Rahmenarchitektur und technischer Lösungsvorschlag, White Paper, Version 2.0 für den DOL-DLR-Projektbericht zur Blaupause [Buch]. - Stuttgart : IRB Verlag, 2008. - S. 194. - ISBN: 978-3-8167-7765-6.

Wahrig Wahrig Deutsches Wörterbuch [Buch]. - München : Wissen Media Verlag GmbH, 2002.

11. Anhang

11.1 Abkürzungsverzeichnis

AACS	Application Access Control Structure
API	Application Programming Interface
BPMN	Business Process Modeling Notation
DL	Dienstleistungserbringer (EU-DLR)
EA	Einheitlicher Ansprechpartner (EU-DLR)
EAL	Evaluation Assurance Level
ECC	European Citizen Card
eID	Electronic Identity
EU-DLR	Europäische Dienstleistungsrichtlinie, Richtlinie 2006/123/EG
FRESKO	Flexibler Einfacher Sicherer Kommunikations-Prozessor
HW	Hardware
IDABC	Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens (EU Programm)
IDM	Identitätsmanagement
IMI	Internal Market Information System, Binnenmarkt-Informations-system
LDAP	Lightweight Directory Access Protocol
PEGS	Pan-European eGovernment Services
PEPS	Pan-European Proxy Service
PKI	Public Key Infrastructure
QAA	STORK Quality Authentication Assurance Framework
S.A.F.E.	Secure Access to Federated E-Justice/E-Government
SAML	Security Assertion Markup Language
SSO	Single Sign-On
STORK	“Secure identity across borders linked” – EU CIP Projekt
SW	Software
ZB	Zuständige Behörde (EU-DLR)

11.2 Glossar

Begriff	Erläuterung
Anonymität	Anonymität besteht, wenn in einem Geschäftsprozess *Attribute* einer *Entität* verwendet werden, die nur Informationen umfassen, die nicht eindeutig einer Person oder einem Objekt zugeordnet werden können.
Attribut	Ein Attribut ist eine bestimmte, mit einem Namen versehene, Eigenschaft einer *Entität*. (Hühnlein, 2008)
Attribut Provider	Siehe *Attribut-Zertifizierer.*
Attribut-Zertifizierer	Der Attribut-Zertifizierer bestätigt die vertrauenswürdige Zuordnung eines *Attributs* zu einer bestimmten *Entität*.
Authentifizierung	Authentifizierung ist das Prüfen einer bestimmten Menge von behaupteten *Attributen* einer *Entität*. Es gibt verschiedene Authentifizierungsmethoden mit unterschiedlicher Stärke, z.B. Username/Passwort, kryptografische Verfahren, biometrische Verfahren.
Autorisierung/ Zugriffskontrolle	Nach erfolgreicher *Authentisierung* können Dienste nur dann genutzt werden, wenn der Nutzer auch dazu berechtigt ist. Ein *Dienstanbieter* kann den Zugang zu Ressourcen/Diensten kontrollieren. Detaillierte Zugriffsentscheidungen können in der Fachanwendung basierend auf verschiedenen *Attributen* wie z.B. Identität, Zugangsmedium, Rolle und Uhrzeit erfolgen.
Benutzer/ Nutzer / Bürger / Anwender	Die Benutzer sind die Inhaber einer Digitalen Identität, deren Attribute von ihnen für die Nutzung von Diensten bei *Dienstanbietern* verwendet werden.
Dienstanbieter / Service Provider / Relying Party	Ein Dienstanbieter (Relying Party, Service Provider) bietet Dienste für Benutzer an. Ein Dienstanbieter verwendet bestimmte *Attribute* zur *Authentifizierung* des Benutzers und fällt dann gegebenenfalls eine Autorisierungsentscheidung, um dem Benutzer den Zugriff auf Informationen oder Ressourcen zu gewähren oder zu verweigern. Typische Beispiele für Dienstanbieter sind Websites von Banken, Online-Händlern und -Auktionen im Internet sowie Online-Dienste im eGovernment oder eBusiness Umfeld.
Entität	Eine Entität ist eine natürliche oder juristische Person oder ein Objekt, z.B. eine technische Komponente, ein Dienst, Daten, das durch seine Attribute charakterisiert wird. (Hühnlein, 2008)

Begriff	Erläuterung
Federation	Zwei Identifikatoren eines Nutzers aus verschiedenen administrativen Domänen werden föderiert, um die Authentisierung des Nutzers mit einem einzigen Identifikator für beide Domänen zu ermöglichen. (Hühnlein, 2008) Hierfür ist es erforderlich, dass die Dienstanbieter erzeugte Identifikatoren bilateral austauschen und ein gegenseitiges Vertrauensverhältnis besteht. Alternativ kann eine vertrauenswürdige dritte Partei mit der Federation beauftragt werden. Um Datenschutz in Bezug auf Attribute zu gewährleisten, sollten dem Nutzer Mechanismen zur Verfügung stehen, um zu kontrollieren, welche Attribute zwischen den Dienstanbietern ausgetauscht oder von der vertrauenswürdigen dritten Partei an sie preisgegeben werden.
Identifikator	Ein Identifikator besteht aus mindestens einem Attribut und bezeichnet eine Identität in einem bestimmten Kontext eindeutig. Z.B. sind Personenkennzeichen national eindeutige Identifikatoren für Personen.
Identifizierung/ Registrierung	Identifizierung und Registrierung eines Nutzers dienen der Zuordnung von Attributen zu einer Digitalen Identität. Die Identifizierung und Registrierung kann auf unterschiedliche Art erfolgen (persönliches Erscheinen, email, Webformular usw.) und von unterschiedlichen Registrierungsinstanzen vorgenommen werden (Behörde, kommerzieller Anbieter, Webregistrierung durch Nutzer usw.). Die Qualität/Stärke der Identifizierung und Registrierung ist daher unterschiedlich. Entscheidend ist, dass der erreichbare Sicherheitslevel für Authentifizierung und Dienstnutzung nicht höher sein kann, als der Sicherheitslevel von Identifizierung und Registrierung.
Digitale Identität	Eine Digitale Identität ist eine Menge von Attributen, die eine Person oder ein Objekt von anderen Personen oder Objekten unterscheiden und mit der sich eine Person oder ein Objekt in der digitalen Welt bewegt. Zu einer Digitalen Identität können Identifizierungsattribute wie personenbeschreibende Merkmale, biometrische Kenndaten oder kryptografische Schlüssel gehören. Ebenso können Informationen zu einer Identität gehören, die fest mit einer Person verbunden sind, z.B. Anschrift, Geburtsort oder Angaben zum Familienstand. Darüber hinaus können Identitäten anwendungsbezogene Informationen umfassen. Dazu zählen unter anderem durch Dritte vergebene Identifikationsdaten, z.B. Kundennummern, die eine Identität mit einem Geschäftsvorgang verbinden und eine Person oder ein Objekt in diesem Rahmen für einen Dritten wiedererkennbar machen.

Begriff	Erläuterung
Identitätsmanage-ment	Die Kernaufgabe des Identitätsmanagements ist es, die Attribute der Digitalen Identität vertrauenswürdig zu erzeugen und während ihrer Lebensdauer auch vertrauenswürdig zu verwalten.
Identity Provider	Siehe *Attribut-Zertifizierer*.
Privatheit	Privatheit dient dem Schutz eines Benutzers gegen Enthüllung und Missbrauch seiner Identitätsdaten durch andere Benutzer oder Dienste.
Pseudonymität	Pseudonymität besteht, wenn in einem Geschäftsprozess *Attribute* einer *Entität* verwendet werden, die nur Informationen umfassen, die für den Dienstanbieter nicht eindeutig der Digitalen Identität einer Person oder eines Objekts zugeordnet werden können. Allerdings kann es möglich sein, dass eine vertrauenswürdige dritte Partei diese eindeutige Zuordnung in Streitfällen treffen kann. Dienstanbieterspezifische und bereichsspezifische Identifikatoren sind mögliche Pseudonyme, wenn keine weiteren personenbezogenen Daten mit diesen Identifikatoren verknüpft werden. In den Transaktionen zwischen Nutzer und Dienstanbieter können Pseudonyme wiedererkannt werden.
Rollen	Eine Rolle („role“) ist ein semantisches Konstrukt, mit dem die jeweiligen Berechtigungsvorgaben beschrieben werden. Benutzer („user“) können Rollen einnehmen, und Berechtigungen („permission“) sind an die Rollen gekoppelt. Berechtigungen ihrerseits bestehen wiederum aus Operationen („operations“), die auf Objekten („object“) ausgeführt werden. Die Berechtigungen einer Rolle werden durch Zugriffsregeln basierend auf den Attributen der Entität und weiteren kontext-spezifischen Daten ermittelt. Für weitergehende Details sei auf (Ferraiolo, et al., 2007) ver-wiesen.
Single Sign-On	Single Sign-On erlaubt die einmalige Authentifizierung für die Nutzung verschiedener Dienste bzw. Ressourcen. Technisch kann Single Sign-On unterschiedlich realisiert werden, z.B. als eine einheitliche Benutzerkennung oder durch Zusammenführung (*Federation*) von Benutzerkennungen mit oder ohne Interaktion des Nutzers. Single Sign-Out erlaubt das gleichzeitige „Ausloggen“ aus verschiedenen Sessions.

Impressum

Herausgeber

Fraunhofer-Institut für
Offene Kommunikationssysteme FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin