Projektabschlussbericht

A1.12 Massnahme 8 „Authentifizierung, Datenschutz und Informatiksicherheit“

V1.0 – 29.11.2012

Forschungsschwerpunkt	E-Government
Projektleiter	Thomas Selzam
Projektmitarbeiter	Martin Topfel, Fabienne Kuhn
Projektzeitraum	01.09.2012 – 01.12.2012

Management Summary

Der elektronische Umzug A1.12 (eUZ) soll 2013 in enger Zusammenarbeit mit mehreren priorisierten E-Government Vorhaben des Bundes vorangebracht werden. Der wichtigste Partner ist dabei B2.06 „Dienst für Identifikation und Berechtigungsverwaltung (IAM)“ unter Verantwortung der eCH-Fachgruppe Identity and Acessmanagement. Am Architekturworkshop des Bundes wurde im November 2012 beschlossen, dass die gesamten Funktionalitäten rund um die Authentifizierung der BenutzerInnen (EinwohnerInnen, SachbearbeiterInnen der Einwohnerdienste) des eUZ vom föderierten IAM B2.06 bereitzustellen ist. Fragen die sich daraus ergeben:

- Wie kann der zeitnahe Austausch von Einwohnerinformationen zwischen dem Umzug Service (UZS) und den Informationslieferanten (Register) über IAM B2.06 ermöglicht werden?

Der vorliegende Bericht konzentriert sich auf Fragestellungen, die sich aus dieser Abhängigkeit zwischen eUZ A1.12 und IAM B2.06. Es werden Aspekte rechtlicher, technischer und organisatorisch-prozessualer Natur beleuchtet. Dies in enger Zusammenarbeit mit der A1.12 Massnahmen 3, die sich primär mit der Abschaffung des Heimatausweises befasst, und A1.12 Massnahme 4, in welcher der Anpassungsbedarf bei den Ausländerausweisen untersucht wird. Für die Authentifizierung spielen diese beiden Massnahmen eine wichtige Rolle, werden darin doch die Neugestaltungen der analogen Authentisierungsmittel (engl. Credentials) diskutiert. Die Notwendigkeit dafür ergibt sich aus der Elektronisierung des Umzugsprozess, also der Anbietung des Dienstes für Umzugsmeldung über online Plattformen. Aus Sicht Authentifizierung stellen sich dabei folgende Kernfragen:

- Welche Authentifizierungsstärke (Qualität) ist für den Zugriff auf den Umzug Service resp. die daran angehängten Register notwendig?
- Welche Authentisierungsmittel bieten eine adäquate Sicherheit, ohne die Benutzerfreundlichkeit zu stark einzuschränken und kommen somit für den Einsatz im eUZ in Frage?

Der UZS A1.12 ist aus Sicht der primären Benutzer (EinwohnerInnen, SachberabeiterInnen der EWD) eingebettet in bestehende online Portale und EWD-Lösungen zu realisieren. Dazu ist bei der technischen Lösungsentwicklung eine enge Zusammenarbeit mit den führenden Anbietern der Lösungen auf Ebene der Gemeinden und Kantone notwendig:

- Welchen Anforderungen muss der UZS bezüglich Integrierbarkeit in bestehende Lösungen erfüllen?
- Soll und kann der UZS als gemeinsamer Dienst aus der Cloud realisiert werden?

Die rechtlichen Fragen wurden in Zusammenarbeit mit A1.12 Massnahme 10 „Gesetze in den Kantonen“ bearbeitet. Ein eUZ wird naturgemäss mit Personendaten umgehen müssen. Dies erfordert eine enge Zusammenarbeit mit Datenschutzbeauftragten von Bund und Kantonen:

- Wie kann sichergestellt werden, dass der eUZ die Anforderungen an Datenschutz und Informationssicherheit erfüllt?

Erarbeitet zwischen 09. Und 11.2012 liefert dieser Bericht Hinweise und Priorisierungen für die weiteren Massnahmen A1.12 im Jahr 2013.

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

AHVN13	Neue, 2007 eingeführte AHV-Versichertennummer mit 13 Stellen
BFM	Bundesamt für Migration
BFS	Bundesamt für Statistik
DSG	Datenschutzgesetz, SR 235.1
eCH	Verein für E-Government- und E-Health-Standards für die Schweiz
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeits-Beauftragter
EJPD	Eidgenössisches Justiz und Polizei Departement
EWD	Einwohnerdienste
EWK	Einwohnerkontrolle
EWR	Einwohnerregister
eUZ	elektronischer Umzug (Prozess)
UZS	Umzug Service (System)
IAM	Identity and Access Management; Identitätsmanagement; System für die Verwaltung von Identitäten und dem Zugriff auf Dienste
KMA	Kantonales Migrationsamt
RHG	Registerharmonisierungsgesetz
SR	Systematische Rechtssammlung
SuisseID	CH-Standard für eine elektronische Identität, umfassend Authentisierung, qualifizierte Signatur und Identitätsdaten-Nachweis
VSED	Verband Schweizerischer Einwohnerdienste
ZEMIS	Zentrales Migrationsinformationssystem
ZertES	Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur, SR 943.03

1. Einleitende Bemerkungen

Der vorliegende Bericht befasst sich ausschliesslich mit prozessualen, technischen und rechtlichen Aspekten rund um Authentifizierung und Sicherheit im elektronischen Umzugsprozess (eUZ). Die umfassende Beschreibung des Prozess findet sich im Teilberichte zu Massnahme 3 „Abfragemöglichkeit Infostar - Abschaffung Heimatschein“, der Teilbericht zu Massnahme 4 „Änderung der Ausländerausweise – Schnittstelle zu / Zugriff auf ZEMIS“ behandelt die weiteren Spezifika des Umzugs ausländischer EinwohnerInnen. In diesem Bericht finden sich einige Hinweise auf rechtliche Fragestellungen, die 2013 zu beantworten sind. Weiterführende und auf kantonale Rechtssituationen fokussierte Fragen sind dem Teilbericht zu Massnahme 10 „Gesetze in den Kantonen" zu entnehmen.

Folgenden Personen gilt unser Dank für ihre Mitarbeit bei Orientierung und Verifizierung:

Stephan Wenger (Einwohneramt der Stadt St.Gallen und Ko-Projektleitung A1.12)
Christian Dolf (BINT GmbH, Ko-Projektleitung A1.12)
Jolanda Bischoff (Einwohneramt der Stadt St. Gallen, Kernteam A1.12)
Marcel Bernet (eCH, SwissICT, /ch/open, Teilprojekt A1.12 Standardisierung)
Marco Demarmels (IHE Pharmacy Technical Committee, eCH, Lake Griffin LLC)
Steff Schnetzler (i-web.ch)
Ronny Bernold (eCH, Berner Fachhochschule)
Andreas Spichiger (eCH, Berner Fachhochschule)

2. Modellierung Prozess elektronischer Umzug

2.1 IST Prozesse

Die IST-Prozesse für den analogen Umzug werden in den Teilberichten zu Massnahme 3 „Abfragemöglichkeit Infostar - Abschaffung Heimatschein“ und Massnahme 4 „Änderung der Ausländerausweise – Schnittstelle zu / Zugriff auf ZEMIS“ behandelt.

2.2 SOLL Prozess Abgrenzung

Der modellierte Prozess berücksichtigt folgende Prämissen:

1. Der Prozess funktioniert nur für einzelne EinwohnerInnen die innerhalb der Schweiz umziehen.
2. Der Prozess wird entweder von einer umzugswilligen Person direkt im Internet (Bürger-, Gemeindeportal), oder durch eine MitarbeiterIn der Einwohnerkontrolle bei Präsenz der umzugswilligen Person am Schalter durchgeführt.
3. Es kann zeitnah, sprich möglichst in real time, auf die Daten der EWR zugegriffen werden. Dies unabhängig von der technischen Umsetzung, also auch unabhängig davon, ob der Prozess von der Website der Zuzugs- oder Wegzugsgemeinde gestartet wird.
4. Es SOLL künftig ein zeitnaher, sprich möglichst Echtzeit- Zugriff auf die diversen Register möglich sein. Somit können fast alle Attribute die für den Umzugsprozess notwendig sind, während der Anwesenheit der umzugswilligen Person (UP) am PC bzw. am Schalter (im Falle einer Bearbeitung durch einen Verwaltungsmitarbeiter in Gegenwart der UP) abgefragt, ergänzt und bestätigt werden. Dadurch ist beim Schritt E-Payment mit sehr hoher Wahrscheinlichkeit von einer erfolgreichen Durchführbarkeit des Prozesses zu rechnen.
5. Eine manuelle Prüfung des Umzugsantrags durch EWKs & KMA ist weiter notwendig. Varianten, die eine Vollautomatisierung vorsehen, wurden nicht ausgearbeitet, da man davon ausgeht, dass dem neuen System zunächst nicht blind vertraut wird und eine Sicherheitsschlaufe gewünscht wird. Später sollen die Gemeinden individuell entscheiden können, ob diese „Sicherheitsschlaufe“ beibehalten oder automatisch umgangen werden soll.
6. Die technische Umsetzung des UZS wird als Shared Service (in/aus der cloud) angepeilt, dennoch ist auch eine Einbettung als Bestandteil einer Gemeindesoftware (also dezentrale Umsetzung) denkbar.
7. Der Bund stellt die technische Grundinfrastruktur zur Verfügung, insbesondere was das Identitäts- und Zugriffsmanagement (IAM) betrifft.
8. Das für die Durchführbarkeit des Prozesses notwendige, minimale Attributeset wird auf die in Art. 6 des Registerharmonisierungsgesetzes[1] vereinbarten Attribute beschränkt[2]. Durch diese Beschränkung soll sichergestellt werden, dass ein UZS entsteht, der anschlussfähig an alle kantonalen Systeme ist:

   „Die Einwohnerregister enthalten von jeder Person, die sich niedergelassen hat oder aufhält, mindestens die Daten zu den folgenden Identifikatoren und Merkmalen:

[1] RHG

[2] Zusätzliche Attribute einzubeziehen kann aus Perspektive von einzelnen Kantonen selbstverständlich wünschbar sein. Zu bedenken gilt der lange Konsensfindungsprozess auf die RHG Attribute. Ausserdem stellen zusätzliche, kantonale Spezialanforderungen im Sinne erweiterter Attributesets den Prozess in der vorliegenden, medienbruch freien Umsetzung in Frage. Zusätzlich werden Realisierung und Pflege des UZS dadurch verteuert, die Benutzerfreundlichkeit durch manuelle Eingabe weiterer Informationen verringert.

1. **Versichertennummer** nach Artikel 50c des Bundesgesetzes vom 20. Dezember 1946 über die Alters- und Hinterlassenenversicherung (AHVG);
2. **Gemeindenummer** des Bundesamtes und amtlicher **Gemeindename**;
3. **Gebäudeidentifikator** nach dem eidgenössischen Gebäude- und Wohnungsregister (GWR) des Bundesamtes;
4. **Wohnungsidentifikator** nach dem GWR, Haushaltszugehörigkeit und Haushaltsart;
5. amtlicher **Name** sowie die anderen in den Zivilstandsregistern beurkundeten Namen einer Person;
6. alle **Vornamen** in der richtigen Reihenfolge;
7. **Wohnadresse** und **Zustelladresse** einschliesslich Postleitzahl und Ort;
8. **Geburtsdatum** und **Geburtsort**;
9. **Heimatorte** bei Schweizerinnen und Schweizern;
10. **Geschlecht**;
11. **Zivilstand**;
12. Zugehörigkeit zu einer öffentlich-rechtlich oder auf andere Weise vom Kanton anerkannten **Religionsgemeinschaft**;
13. **Staatsangehörigkeit**;
14. bei Ausländerinnen und Ausländern die **Art des Ausweises**;
15. **Niederlassung oder Aufenthalt** in der Gemeinde;
16. **Niederlassungsgemeinde oder Aufenthaltsgemeinde**;
17. bei Zuzug: **Datum und Herkunftsgemeinde** beziehungsweise Herkunftsstaat;
18. bei Wegzug: **Datum und Zielgemeinde** beziehungsweise Zielstaat;
19. bei Umzug in der Gemeinde: **Datum**;
20. **Stimm- und Wahlrecht** auf Bundes-, Kantons- und Gemeindeebene;
21. **Todesdatum**."[3]

In der vorliegenden Modellierung funktioniert der Prozess zeitnah d.h. in Echtzeit. Eine zeitlich verschobenen, asynchron Ausgestaltung ist aber mit geringem Aufwand zu erreichen. Hauptunterschied ist die Platzierung des E-Payment und die Erfassung des minimal benötigten Attributesets. Letzteres erfolgt beim zeitnahen Prozess primär über Abfrage bestehender Attribute bei den Registern. Somit müssen von den EinwohnerInnen nur wenige Informationen erfragt werden, der Prozess am online Schalter dauert relativ kurz. Mit dem E-Payment (gemeint ist nicht die Ausführung der Zahlung, sondern erst die Genehmigung zur Finanztransaktion nach erfolgreichem Umzugsprozess) Endet die notwendige Präsenz der umzugswilligen Person an Bildschirm oder EWD-Schalter. Durch die bereits erfolgte Vervollständigung des Attributesets und die allfällige Prüfung kritischer Attribute, kann zu diesem Zeitpunkt von einer hohen Wahrscheinlichkeit des erfolgreichen Prozessabschluss (für die EinwohnerInnen) ausgegangen werden.
Demgegenüber müssten beim zeitversetzten Prozess sämtliche notwendigen Attribute vorgängig von den umzugswilligen Personen abgefragt werden[4], über die Wahrscheinlichkeit des erfolgreichen Prozessabschluss' könnten keine verlässlichen Annahmen getroffen werden.

[3] BFS (2008)
[4] In der vorliegenden Modellierung (siehe Anhang) würde also bei einem ok nach Schritt 2.c) direkt zu 2.g) und weiter zu Schritt 5) gesprungen. Dort müssten sämtliche, für den eUZ notwendigen Informationen der umzugswilligen Person abgefragt werden. Als nächstes folgte E-Payment, womit der Präsenzteil der Person am Bildschirm endet und der asynchrone Prozessteil der Überprüfung der angegebenen Informationen gestartet wird.

2.3 Prozess Modellierung elektronischer Umzug

Der modellierte eUZ besteht aus drei Phasen:

I. Authentifizierung und Start Umzug Service
II. Erfassung weiterer und Prüfung Attribute
III. Ummeldung

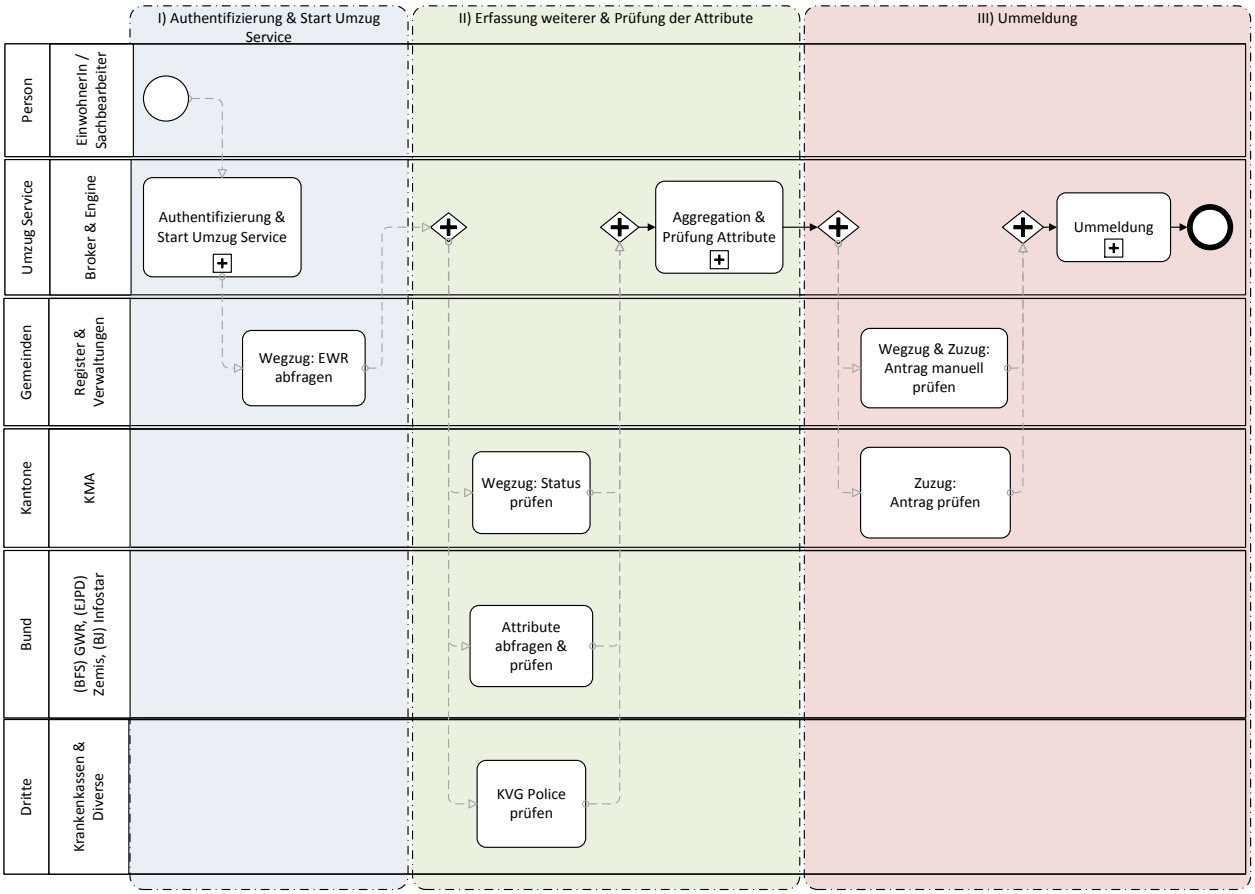


Abbildung 1 Überblick Gesamtprozess elektronischer Umzug

Im vorliegenden Teilbericht zur Massnahme 8 wird auf I) Authentifizerung & Start Umzug Service detailliert eingegangen. Weitere Erläuterungen zu den Prozessteilen II und III finden sich in den Teilberichten zu den A1.12 Massnahmen 3 & 4. Die vollständigen Modellierungen und Beschreibung (ohne Diskussion) zu den Prozessschritten befinden sich ausserdem im Anhang zu diesem Bericht.

I. Authentifizierung und Start Umzug Service

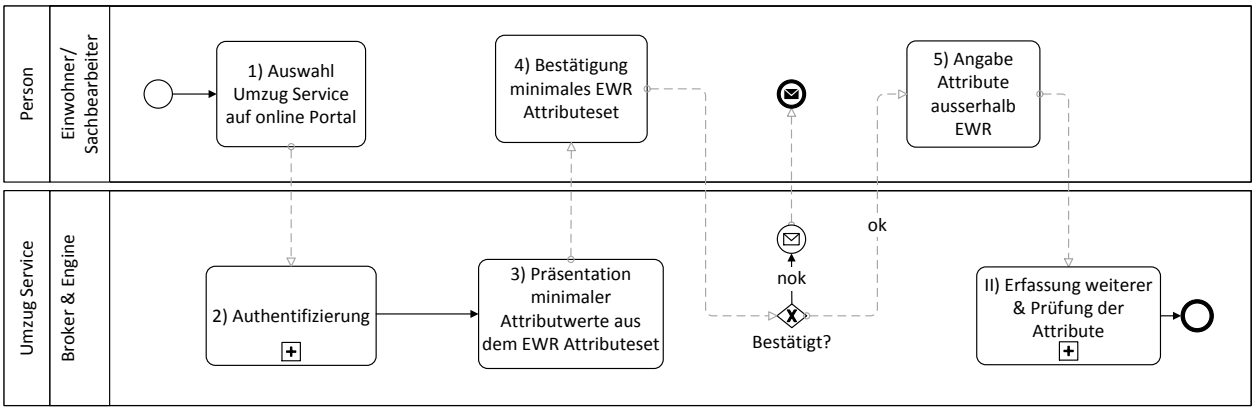


Abbildung 2 Teilschritt I: Start Umzug Service und Authentifizierung

Beschreibung Prozessphase I. Start Umzug Service und Authentifizierung:

1) Auswahl Umzug Service auf online Portal
   Die Person wählt den UZS auf dem online Portal der Wegzugs- oder Zuzugsgemeinde, der Post oder des Bundes aus. Wo der Prozess gestartet wird ist nicht entscheidend.
2) Authentifizierung
   Dieser Prozess behandelt die Authentisierung und Authentifizierung der umzugswilligen Person bzw. oder der in Stellvertretung agierenden SachbearbeiterIn.
3) Präsentation minimaler Attributwerte aus dem EWR Attributeset
   Die Person bekommt nun Name, Vorname und Adresse aus dem EWR Attributeset angezeigt. Wurden mehr als ein passendes Attributeset beim EWR der Wegzug Gemeinde gefunden (keine eindeutige Zuweisung möglich), so werden aus den gefundenen Attributesets jeweils Name, Vorname und Adresse angezeigt[5].
4) Bestätigung minimales EWR Attributeset
   Mit dem Wählen eines Attributesets bestätigt die Person die Zugehörigkeit von ersterem zu sich bzw. zu der am Schalter befindlichen EinwohnerIn[6].
   Wird die Auswahl von der Person als inkorrekt angeben bzw. keines der angezeigten Auswahlmöglichkeiten als zu ihr zugehörig bestätigt, so erfolgt eine Aufforderung, den Prozess analog am Schalter der Gemeinde durchzuführen. Dies führt zur Beendigung des Online Umzugs.
5) Angabe Attribute ausserhalb EWR
   Die Person muss die Zuzugsadresse (Strasse, Ort und PLZ) sowie das Umzugsdatum angeben. Allenfalls können hier zusätzliche Attribute angegeben werden, die nicht im minimalen Attributeset vom EWR enthalten sind (z.B. Angaben zur KVG Police, EWID Nummer etc.).

[5] Gemäss Datenschutzbeauftragtem des Kantons Zürich, kann aus dem EWR voraussetzungslos Name, Vorname und Adresse einer Person an Private mitgeteilt werden (DSB ZH (2012)). Es gilt zu prüfen, ob diese Voraussetzungen in allen anderen Kantonen ebenfalls zutreffen.
[6] Rechtlich ist hier abzuklären, ob und wenn ja, was der Person bezüglich möglicher Auswirkungen von absichtlicher Angabe falscher Informationen mitzuteilen ist.

Subprozess I.2) Authentifizierung

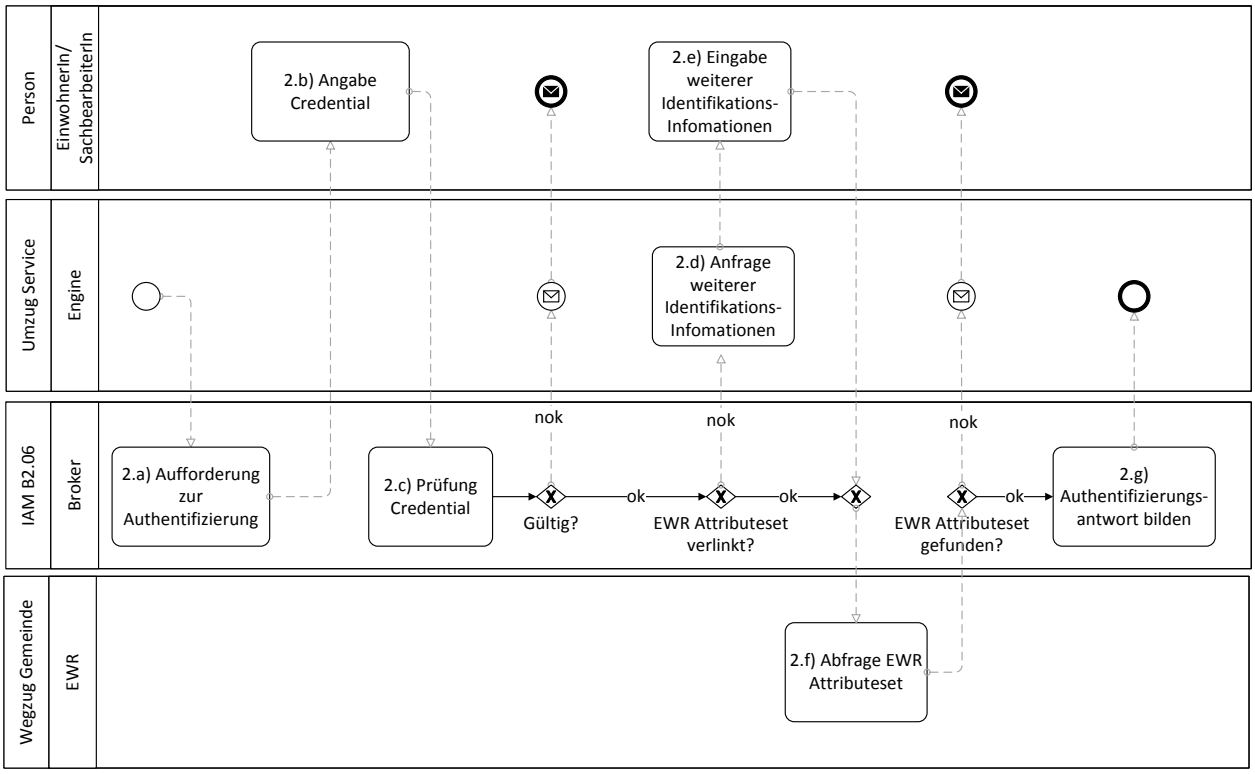


Abbildung 3 Subprozess I.2) Authentifizierung

Beschreibung Subprozess I.2) Authentifizierung:

2.a) Aufforderung zur Authentisierung

Die Person wird vom IAM B2.06 aufgefordert sich mit einem Credential zu authentisieren.

2.b) Angabe Credential

Die Person gibt das zur Authentisierung notwendige Credential an und sendet die Informationen an IAM B2.06 zurück.

2.c) Prüfung Credential

Die Person wird authentifiziert und es wird geprüft ob bereits ein EWR Attributeset bei IAM B2.06 verlinkt ist. Falls eine entsprechende Verlinkung gefunden wird, weiter mit 2.f). Falls nicht, weiter mit Schritt 2.d).

Wurde kein gültiges Credential gefunden, erfolgt über den UZS eine Meldung an die Person (Credential angeben, Credential beschaffen oder Umzug analog am Schalter durchführen).

2.d) Anfrage weiterer Identifikationsinformationen

Ist kein Link zu einem EWR vorhanden, so wird die Person angefragt, weitere Identifikationsinformationen anzugeben.

2.e) Eingabe weiterer Identifikationsinformationen

Wenn im IAM B2.06 noch kein EWR Attributeset mit der Identität der Person verlinkt ist, wird letztere zur Angabe weiterer Identifikationsattribute aufgefordert. Diese umfassen z.B. den amtlichen Namen, Vornamen, Geburtsdatum, Geburtsort und die Wegzug Gemeinde.

2.f) Abfrage EWR Attributeset

Beim EWR der verlinkten (2.c) bzw. angegebenen (2.e) Gemeinde (Wegzug) wird das entsprechende Attributeset der Person abgefragt. Das Attributeset bzw. die Fehlermeldung („kein passendes Attributeset gefunden“) wird an IAM B2.06 übermittelt.

Wurde kein passendes Attributeset gefunden, erfolgt über den UZS eine Meldung an die Person (zu definieren: soll der eUZ abgebrochen und die Person zur analogen Durchführung aufgefordert werden (entspricht vorliegender Modellierung) oder soll ein Loop eingebaut werden, bei dem die Person zur Überprüfung der angegebenen Informationen (primär Wegzug Gemeinde) aufgefordert wird?). an den UZS.

2.g) Authentifizierungsantwort bilden

Wurde (mindestens) ein passendes EWR Attributeset geliefert, bildet IAM B2.06 mit diesem und der Bestätigung der Gültigkeit des Credentials die Authentifizierungsantwort und übermittelt diese an den UZS.

Wird der Subprozess I.2) Authentifizierung erfolgreich abgeschlossen, so verfügt der UZS über die bestätigte, elektronische Identität der umzugswilligen Person, sowie über mindestens ein EWR Attributeset.

III. Ummeldung

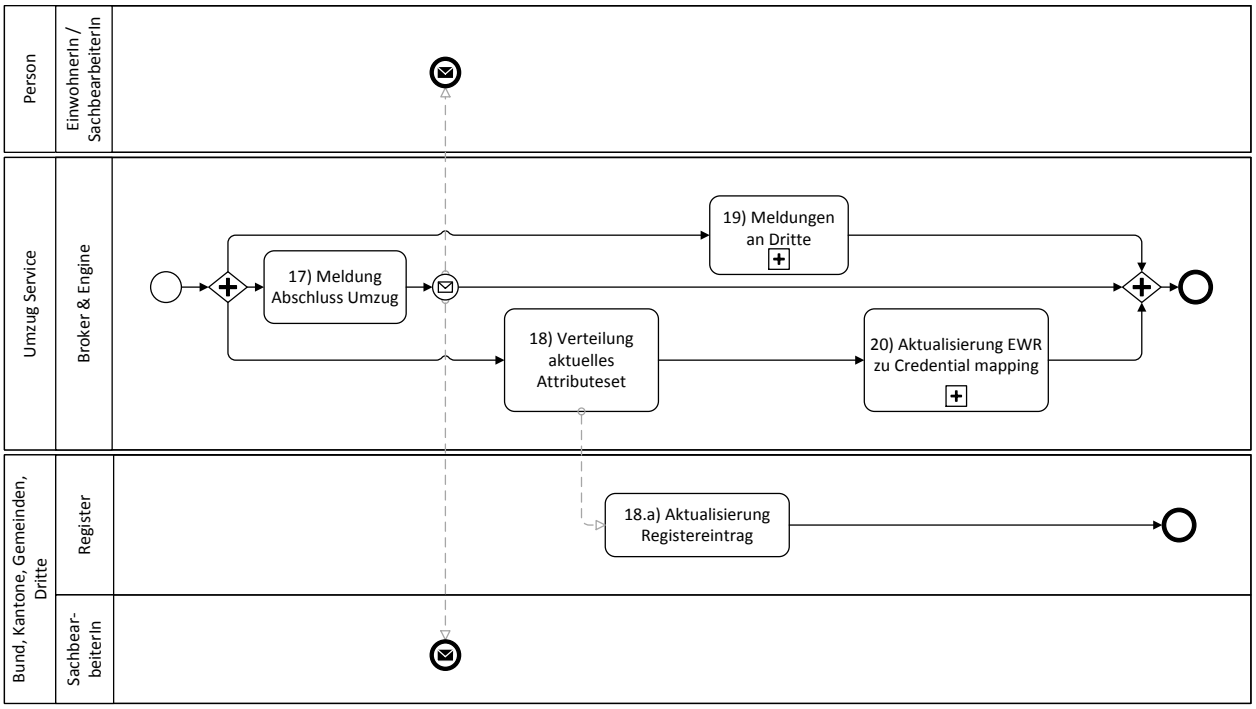


Abbildung 4 III. Ummeldung – Abschluss elektronischer Umzug

Beim Abschluss des eUZ ist aus Sicht Authentifizierung der Subprozess 20) „Aktualisierung EWR zu Credential mapping“ von Bedeutung. Hierbei muss im IAM B2.06 die Verknüpfung der elektronischen Identität mit dem neu bei der Zuzug Gemeinde liegenden EWR Attributeset aktualisiert werden (bzw. sollte zuvor noch keine solche Verknüpfung bestanden haben, wird diese nun gemacht).

Die konkrete Ausgestaltung dieses Subprozesses ist 2013 in Zusammenarbeit mit IAM B2.06 zu klären.

3. Lösungsentwicklung

3.1 A1.12 im Kontext der Koordination priorisierter Vorhaben

In Übereinstimmung mit den Beschlüssen des Architekturworkshops Bund vom 05./06.11.2012 wird der eUZ als konkreter Anwendungsfall auf den gemeinsamen Infrastrukturdiensten folgender priorisierten Vorhaben aufbauen:

B2.13: Dienste zum Einsatz von Referenzdaten in den Öffentlichen Verwaltungen
B2.02: Behördenverzeichnis
B1.14: E-Government Landkarte Schweiz
B1.13: eCH-Prozessplattform für Gemeinden und Kantone
B2.06: Dienst für die Identifikation und Berechtigungsverwaltung

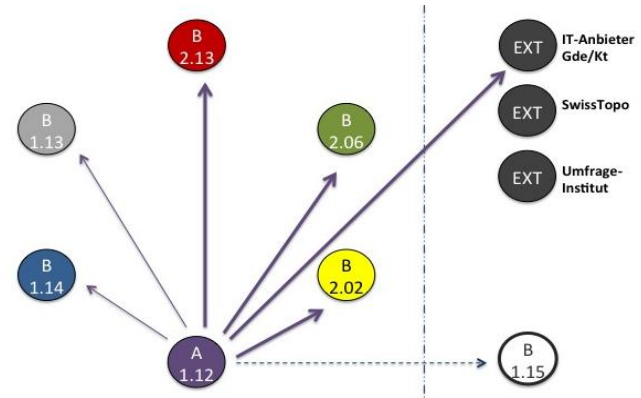


Abbildung 5 Kontextdiagramm priorisierte Vorhaben

Das im Workshop erarbeitete Kontextdiagramm bezeichnet für A1.12 die erwarteten starken Abhängigkeiten von B2.02, B2.13 und B2.06, sowie den externen Anbietern von Portal- und Verwaltungslösungen.

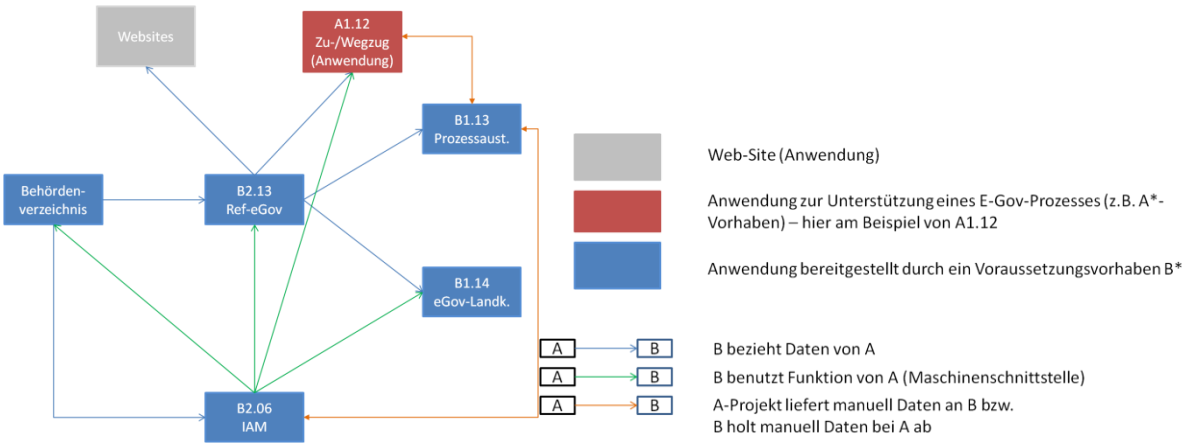


Abbildung 6 Anwendungssystemarchitektur

Die Abhängigkeit von B2.06 „Dienst für die Identifikation und Berechtigungsverwaltung“ wird im folgenden Abschnitt dargelegt. B2.06 wird ein föderiertes Identitäts- und Zugriffsmanagement System (IAM) für den Gebrauch in E-Government Anwendungen über alle föderalen Ebenen hinweg aufbauen. Daneben werden die Lösungen von B2.02 und B2.13 als Lieferanten von Referenzdaten zum Einsatz kommen.

3.2 Umzug Service A1.12 und IAM B2.06

IAM B2.06 wird voraussichtlich auf dem eCH Best Practice Rahmenkonzept SuisseTrustIAM[7] beruhen. Als Kernelement ist dafür 2013 eine Vermittlerplattform schaffen, welche die Verbindung zu allen für den eUZ benötigten Register und Datenbanken herstellt und regelt. Diese Arbeiten werden für die reine IAM Funktionalität notwendig sein, können aber voraussichtlich für die Vermittlerfunktion in A1.12 ausgebaut werden. Sollte dies nicht der Fall sein, müsste für A1.12 eine separate Vermittlerplattform mit redundanten Verbindungen, vertraglichen Regelungen und betrieblichem Aufwand geschaffen werden, was im Sinne nachhaltiger Entwicklung nicht zu begrüssen wäre.

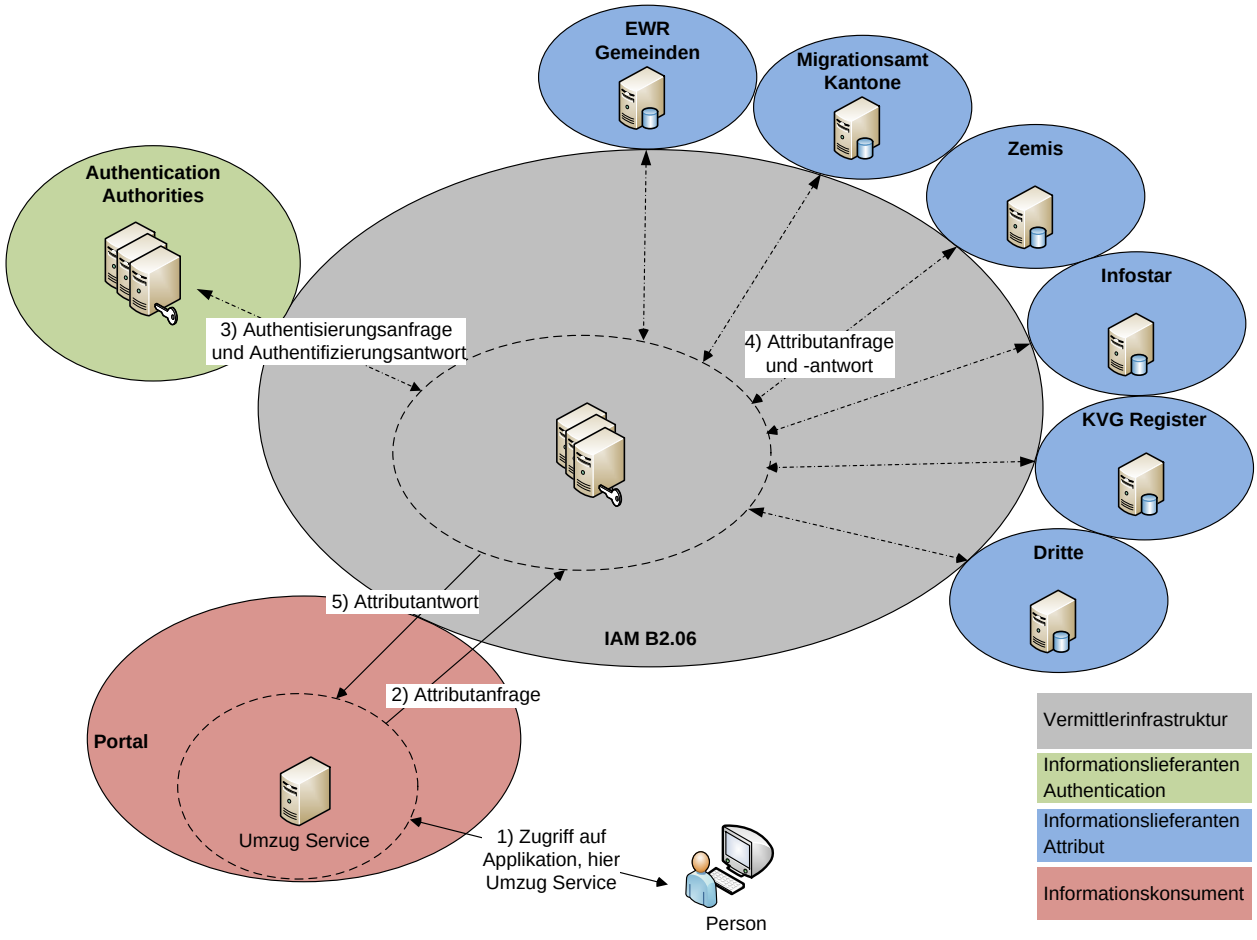


Abbildung 7 Umzug Service – IAM B2.06 Grundszenario

Der Aufbau des IAM für A1.12 ist in drei Elemente aufgeteilt. Das erste Element sind die Register, sie bilden die Grundlagen in dem sie die vom Bund definierten Daten bereitstellen. Das zweite Element ist der IAM Broker, der die Beziehungen und die Informationsvermittlung zwischen den Informationslieferanten und Informationskonsumenten regelt. Das dritte Element stellen die Benutzerportale - Bürger- und Verwaltungsportale von Gemeinden, Kantonen und allenfalls Dritten[8] - dar.

[7] eCH (2012)
[8] Vorstellbar ist eine Einbettung des UZS auch auf Portalen von z.B. Umzugsfirmen, Post, Telekommunikationsunternehmen etc.

Die IAM B2.06 Vermittlerplattform im eUZ zwei Aufgaben:

- BürgerInnen bzw. SachbearbeiterInnen der Einwohnerkontrolle werden vor dem Zugriff auf den UZS sicher authentifiziert.
- Die Informationen (Attribute) der umzugswilligen Person werden aus den Registern von Bund, Kantonen und Gemeinden (sowie allenfalls an IAM B2.06 angeschlossenen Dritten[9]) abgefragt.

Die Umsetzung des IAM für den eUZ über B2.06 würde wie folgt aussehen:

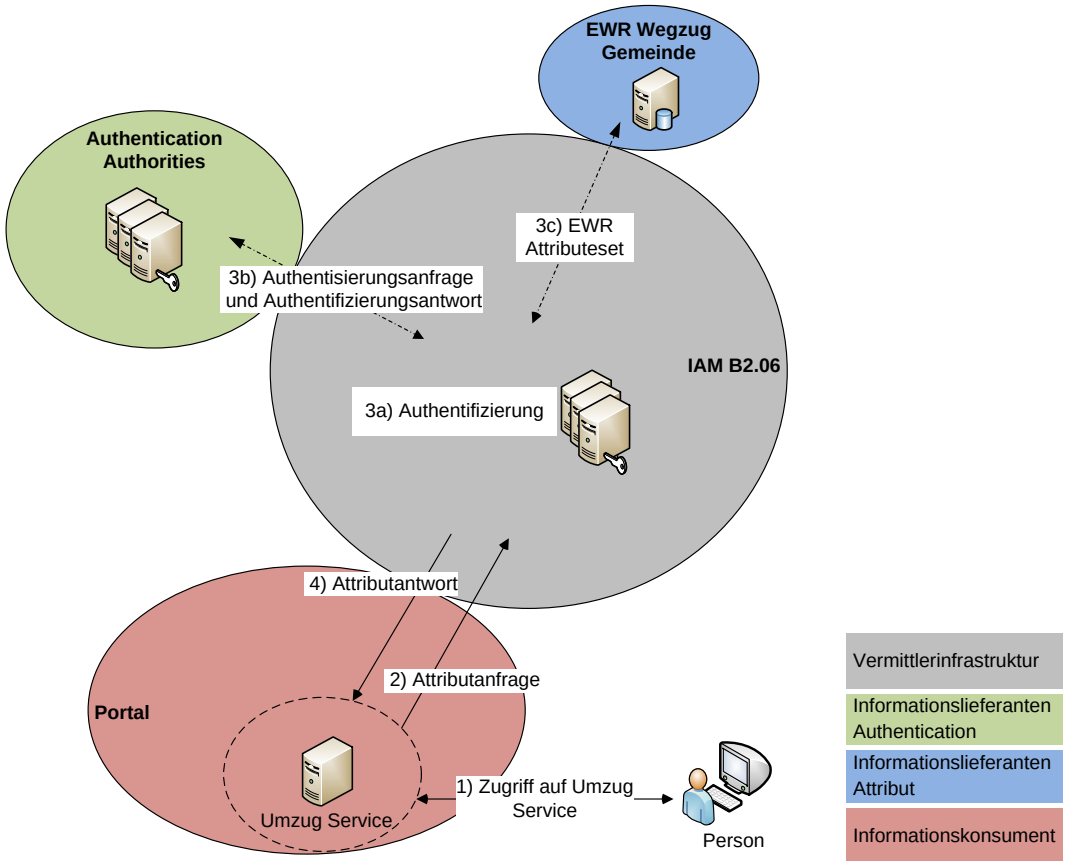


Abbildung 8 Visualisierung Subprozess I.2) Authentifizierung über IAM B2.06

Ablauf der Authentifizierung:

1) Person will auf UZS zugreifen, der in einem Portal eingebettet ist.
2) Person wird zur Authentifizierung als Einwohner einer CH Gemeinde aufgefordert (Umleitung auf IAM)
3a) Person wird zur Angabe eines Credentials mit bestimmter Qualität aufgefordert.
3b) Person wird mittels Credential authentifiziert.
3c) EWR Datensatz der authentifizierten Person wird vom EWR der Wegzug Gemeinde abgerufen.
4) EWR Datensatz wird an UZS übermittelt.
5) UZS speichert den Datensatz transient.

Grundsätzlich besteht für die Authentifizierung der EinwohnerInnen im eUZ die Herausforderung, dass auf

[9] Bezüglich der Übermittlung von Daten an Dritte innerhalb der öffentlichen Verwaltungen bei denen noch keine Verbindung mittels sedex besteht stellt sich die Frage, ob ein Anschliessen an die Vermittlerplattform von IAM B2.06 möglicherweise kosteneffizienter ist, als der Anschluss an sedex.

nationaler Ebene kein frei benutzbarer, eineindeutiger Personenidentifikator zur Verfügung steht. Mit der AHVN13, die Teil des EWR Attributeset ist, existiert ein solcher, jedoch ist die Anwendung an eine gesetzliche Grundlage gebunden. Mittelfristig könnte angestrebt werden, eine solche Grundlage für den UZS zu schaffen. 2013 bietet sich hierzu durch die anstehenden ZertES Revision(en) ein window of opportunity.

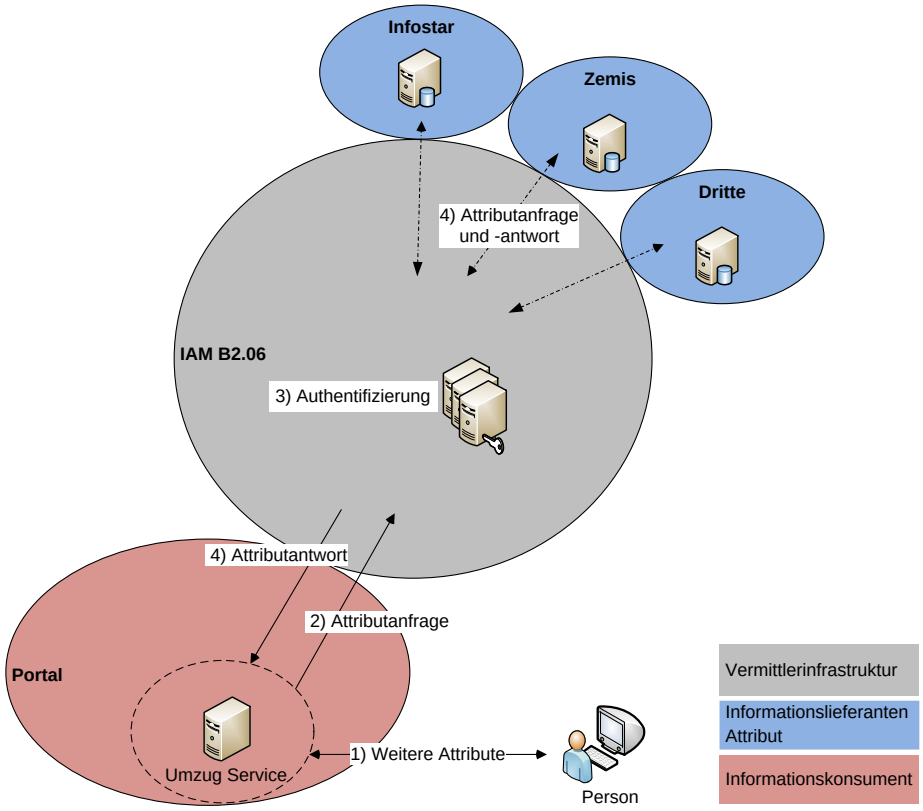


Abbildung 9 Visualisierung Erfassung und Prüfung von Attributen über IAM B2.06

Ablauf der Erfassung und Prüfung von Attributen über IAM B2.06:

1) Person gibt weitere Attribute zur nachfolgenden Prüfung an (EWID Nummer, KVG Police, Zuzugsadresse, Umzugsdatum).
2) UZS fragt bei IAM B2.06 um die zusätzlichen Attribute der Person an (Bestätigung oder Attributwert).
3) Person ist bereits authentifiziert.
4) Benutzer Attribute werden abgefragt und bei Vorhandensein geliefert.
5) UZS ergänzt den Datensatz und speichert ihn transient.

Der eUZ nach A1.12 ist der eigentliche Anwendungsfall, um via IAM B2.06 auf die Daten der verschiedenen Datenquellen von Bund, Kantonen und Gemeinden zuzugreifen. A1.12 ist in der vorliegenden Konzeption nur umsetzbar, wenn die drei Komponenten Datenlieferanten (Register, Datenbanken), IAM Vermittlerplattform und Benutzerportale zur Verfügung stehen und miteinander kommunizieren können. Um die Funktionalität des UZS zu gewährleisten, muss IAM B2.06 realisiert werden.

3.3 Zusammenspiel UZS, IAM B2.06, sedex

Die Übermittlung der eigentlichen Attribute läuft über die vom Bund zur Verfügung gestellte Informatik Plattform sedex. Diese gewährleistet einen sicheren und lückenlosen Transport von Daten zwischen den angeschlossenen Einheiten. sedex garantiert die Vertraulichkeit, Integrität und gesicherte Herkunft der Daten und macht die Übermittlung über den ganzen Prozess nachvollziehbar[10].

Sedex wird derzeit von den EWR zur Übermittlung statistischer Daten ans BFS benutzt. Ab Ende 2014 wird Infostar keine schriftlichen Meldungen mehr absetzen, sondern nur noch elektronisch mit den Gemeinden kommunizieren. Ab diesem Zeitpunkt müssen alle Gemeinden die aktive Kommunikation via sedex (also Senden und Empfangen von Nachrichten) in ihrer Software implementiert haben.

In der technischen Realisierung könnte das System eUZ aus 3 zusammenarbeitenden, jedoch funktional getrennten Elementen bestehen:

- Umzug Service Engine: Diese behandelt die Kommunikation mit den Benutzern, stellt die zu versendenden Anfragen (IAM) und Attributesets (sedex) zusammen und verarbeitet die eintreffenden Antworten (IAM) und Attributesets (sedex)
- IAM B2.06: Authentifizierung und Lieferung der Attribute der EinwohnerInnen
- Sedex: Übermittlung der Attributesets zwischen UZS und verschiedenen Registern

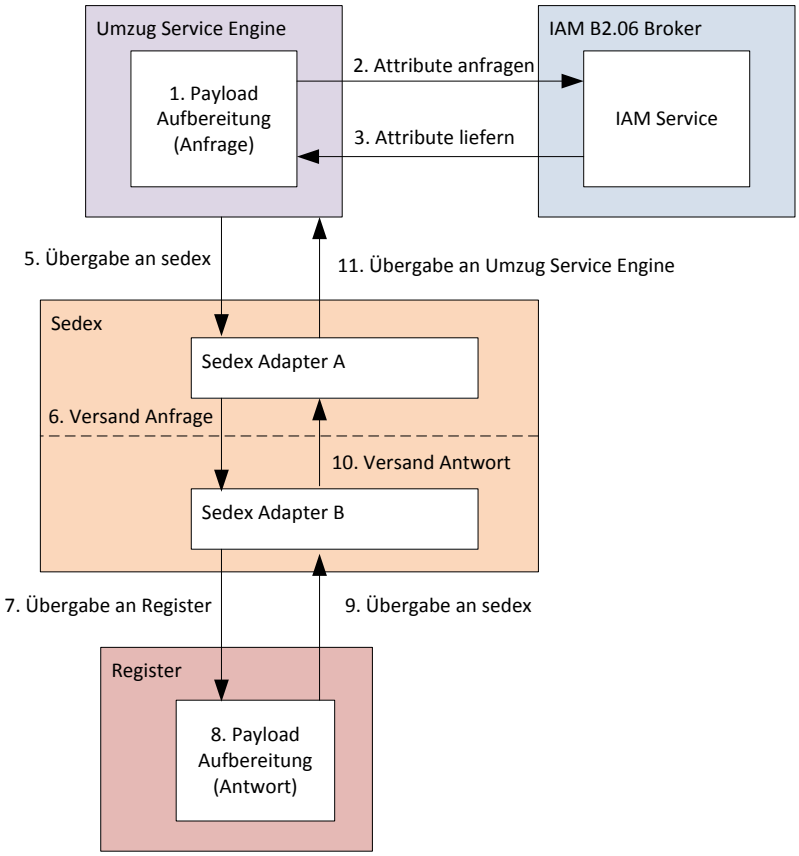


Abbildung 10 Übermittlung der Attributesets mittels sedex

[10] BFS (2012)

3.3.1 sedex: Kommunikationsprinzip

Normalfall:

- Gemeinde Applikationen haben ein eigene Benutzerverwaltung
- Dateisystem benutzt Active Directory für die Benutzerverwaltung
- Sedex-Adapter benutzt Zertifikate für die Sender- und Empfängerverwaltung

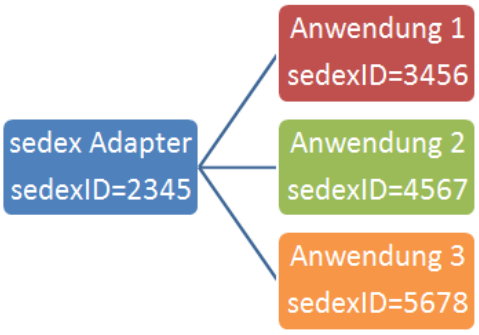
Ein Benutzer will Daten von einer Gemeinde zu einer anderen senden und startet die Gemeinde-Applikation. Die Applikation fordert den Benutzer auf sich zu authentisieren. Nachdem der Benutzer erfolgreich authentifiziert wurde, startet er die Funktion „Daten senden“ in der Applikation. Die Applikation exportiert die Daten aus der eigenen Datenbank in eine Datei (payload) und generiert zusätzlich einen sedex-Umschlag (envelope). Sie speichert diese auf der Windows Freigabe Outbox, falls sie einen entsprechenden Benutzer im Active Directory hat und auch die nötigen Berechtigungen besitzt, um auf den Ordner Outbox zu zugreifen. Der sedex-Adapter besitzt auch einen Active Directory Benutzer und greift in einem vordefinierten Zeitintervall auf den Outbox Ordner zu und sucht dort nach zu übermittelnden Daten. Sind Daten vorhanden, so werden diese mit dem PrivatKey des Senders signiert und mit dem PublicKey des Empfängers verschlüsselt. Anschliessend übermittelt der sedex-Adapter die Daten (payload) an die Empfängeradresse die im Umschlag (envelope) steht.

Auf Empfängerseite nimmt wieder ein sedex-Adapter die Nachricht entgegen, entschlüsselt sie und überprüft die Signatur. Falls der sedex-Adapter einen gültigen Active Directory Benutzer hat und über die entsprechenden Rechte verfügt, so speichert er die Daten in die Inbox des entsprechenden Benützers. Die Gemeinde-Applikation bei der Empfänger Gemeinde benötigt ebenfalls einen Active Directory Benutzer und die nötigen Recht und holt sich die in der Inbox gespeicherten Daten. Die Applikation importiert diese in ihre Datenbank und stellt dies dann zur Verfügung. Benutzer die auf diese Daten zugreifen möchten, müssen sich wiederum mit einem Benutzer der Gemeinde-Applikation authentisieren und authentifizieren.

3.3.2 Identifizierung der sedex-Teilnehmer

Ein sedex-Adapter hat eine sedexID, die ihn identifiziert. Auch der Teilnehmer (z.B. eine Gemeindesoftware) hat eine sedexID. Wenn hinter dem sedex-Adapter nur eine Anwendung läuft, so spricht man von einem physischen Anschluss oder einem physischen Teilnehmer. Dabei stimmen die sedexIDs überein.

Wenn jedoch mehr als eine Anwendung hinter dem sedex Adapter betrieben wird, werden diese logisch angeschlossen. Daher wird diese Anbindung als logischer Anschluss oder logischer Teilnehmer bezeichnet. Die sedexID des sedex-Adapters und die sedexID des Teilnehmers unterscheiden sich hier. Das Mapping zwischen den sedexIDs wird durch sedex organisiert und verwaltet.



Die sedexID kann mit der Postadresse einer Person verglichen werden, um den Unterschied zwischen physischem und logischem Anschluss zu erklären. Wohnt die Person in einem Einfamilienhaus, so ist es nicht so wichtig wie der Name der Person ist, aber die Adresse muss stimmen. Wohnt die Person aber in einem Mehrfamilienhaus, so muss die Adresse und der Name der Person bekannt sein, da sonst nicht klar ist in welchen Briefkasten die Post zugestellt werden soll.

3.3.3 Technische Herausforderungen beim Einsatz von sedex für den eUZ

1. Authentifizierung und Nachvollziehbarkeit

Sedex bietet zwar den verschlüsselten und signierten Transport der Daten an, jedoch gibt es einige Schwächen bei der Nachvollziehbarkeit. Da sedex nur zwischen den einzelnen sedex-Adaptern die Nachvollziehbarkeit gewährleisten kann, treten bis zum Benutzer zwei Authentifizierungsbrüche auf: Erstens zwischen sedex-Adapter und Dateisystem und zweitens zwischen Dateisystem und Applikation. Somit ist eine Nachvollziehbarkeit zwar zwischen zwei Organisationen (sedex-Adapter zu sedex-Adapter) gegeben, jedoch kann so nur mit erheblichem Aufwand festgestellt werden „wer“ (Benutzer) eine Aktion durchgeführt hat.

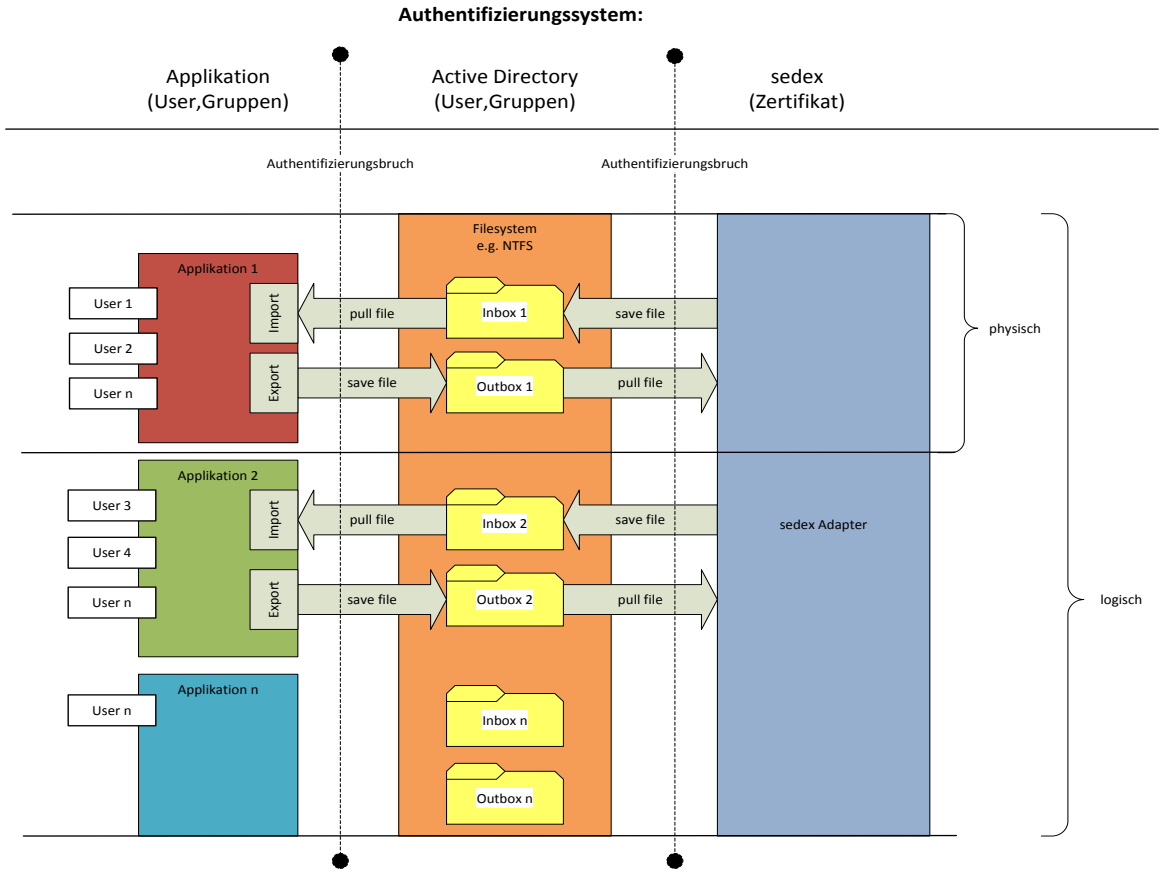


Abbildung 11 Authentifizierung und Nachvollziehbarkeit bei sedex

Für Absicherung der Kommunikation nach dem sedex-Adapter ist jeweils die Organisation selber verantwortlich, so dass sedex dort nicht für die sichere und nachvollziehbare Kommunikation herbeigezogen werden kann. Ob sedex somit die Anforderungen an Auditierbarkeit eines Systems, das schützenswerte Personendaten überträgt erfüllt, ist daher fraglich. Hier empfiehlt sich der Verweis auf Überlegungen aus dem E-Health Bereich, insbesondere zum IHE ATNA Profil[11].

[11] IHE (2012), IHE (2012.1)

2. Asynchrone Kommunikation

Eine weitere technische Herausforderung ist die zeitnahe Kommunikation. Da die Daten nicht direkt übertragen werden und das Intervall des Sendens und Abholens jeweils individuell eingestellt werden kann, ist eine zeitnahe Kommunikation nicht per se garantiert. So kann die Kommunikation zwar nur einige Sekunden dauern, jedoch auch mehrere Minuten bis Stunden.

3. Adressierung des sedex Payload durch den UZS

Aktuell wird das Verzeichnis mit allen sedex Adressen vom Bundesamt für Statistik (BFS) betrieben. Wenn die Gemeinde A dem BFS die Statistikdaten über sedex liefert, so geschieht die Adressierung bei der Gemeinde manuell. Das heisst die Adresse des BFS wird einmal manuell in der Gemeindesoftware eingelesen oder der Gemeindesoftwarehersteller hat diese schon vorkonfiguriert. Da die Adressierung beim UZS jedoch deutlich mehr Register betrifft und dynamisch erfolgen soll, muss ein Adressbuch zur Verfügung gestellt werden.
In der ursprünglichen STIAM Konzeption, auf welcher IAM B2.06 aufbauen soll, ist die reine Referenzierungsfunktionalität nicht angedacht. Über den IAM können dort nur Attribute bestätigen werden, die zu einem Subjekt zugeordnet sind. Daher muss 2013 in Zusammenarbeit mit oben genannten B-Vorhaben geklärt werden, wie die sedex-Adressierung beim UZS realisiert werden kann. 2013 ist folglich zu klären, an welcher Stelle, durch welches System und wie die Referenzdaten der sedex Adapter verwaltet und zur Verfügung gestellt werden. Der UZS A1.12 benötigt diese Informationen zwingend für die Adressierung des Payload, sprich den Versand der Attributesets.

3.4 Authentisierungsmittel, Credentials

Eine der Grundfragen bei der Authentifizierung der Personen bei der Benutzung des UZS liegt beim Einsatz möglicher, elektronischer Authentisierungsmittel. Dabei gibt es zwei ausschlaggebende Aspekte:

- Welche Authentifizierungsstärke ist rechtlich notwendig?
- Welche Authentisierungsmittel sind für die EinwohnerInnen brauchbar?

Der Hauptfokus bei der Authentifizierung liegt hier bei den Einwohnern als Berechtigte des Prozesses. Für Mitarbeitende der Einwohnerbehörden, die in Stellvertretung für sich am Schalter befindliche EinwohnerInnen den Prozess durchführen, stellen sich obige Fragen eher sekundär. Hier kann davon ausgegangen werden, dass die vorhandenen Authentisierungsmethoden bei den internen Verwaltungsportalen adäquat sind, die Herausforderung also primär in der technischen Übertragung der Authentifizierung liegt.

Aus Perspektive der EinwohnerInnen stehen die beiden Aspekte kritisch zueinander: Aus rechtlicher Perspektive muss die Authentifizierung eine adäquate Qualität ausweisen um die Einhaltung der Datenschutzvorschriften und die Informationssicherheit gewährleisten. Dieser Qualitätsanspruch führt dabei schnell dazu, dass technisch und prozessual (die Beschaffung und den Einsatz betreffend) sehr hohe Ansprüche gestellt werden, was schnell die Benutzung des Authentisierungsmittels verkompliziert.

Für die Tauglichkeit eines Authentisierungsmittels im UZS sind zudem einige Einschränkungen zu beachten. So kann zum Beispiel davon ausgegangen werden, dass (wie im analogen Prozess) die EinwohnerInnen üblicherweise nicht lange vor dem eigentlichen Umzug an die Meldung bei den Behörden denken, sondern eher nach erfolgtem Wohnortswechsel. Insofern sind etwaige Authentisierungsmittel, die Tage oder Wochen vor der elektronischen Umzugsmeldung über einen separaten Prozess durch die EinwohnerInnen bestellt werden müssen, nicht als primäres Mittel denkbar (betrifft z.B. SuisseID, MobileID). Selbstverständlich kann der Einsatz solcher, in der Regel qualitativ sehr hohen Authentisierungsmittel ebenfalls angeboten werden. Um die Nutzbarkeit des UZS aber realistisch, das heisst zeitliche flexibel zu gestalten, müssen auch andere Mittel einsetzbar sein.

Mögliche Alternativen (zum Teil nicht mehr existent) wurden bereits 2006 im PoC Umzugservice ZH/SG[12] geprüft. Es empfiehlt sich eine Revalidierung der Ergebnisse nach heutigen Gesichtspunkten, insbesondere aus Sicht Technik und Datenschutz. Insbesondere die Anwendbarkeit eines Kreditkarten basierten Verfahrens könnte interessant sein, da dort die sichere Identifikation der Person lange vorher durch Institutionen mit hoher Vertrauenswürdigkeit erfolgte[13][14].

Im Rahmen von B2.06 wird gegenwärtig ein Qualitätsmodell entwickelt, das generische Methoden zur Bewertung von Authentisierungsmitteln ermöglichen wird. Für 2013 empfiehlt sich daher auch hier eine enge Zusammenarbeit um sicherzustellen, dass adäquat sichere und benutzerfreundliche Authentisierungsmittel für definiert werden, die zur life Schaltung des eUZ zur Verfügung stehen.

3.5 Datenschutz und Informationssicherheit

Grundsätzliche Anforderungen:

- Der UZS erfüllt die Datenschutzanforderungen des Bundes[15] und die Datenschutzanforderungen der Kantone.
- Der UZS wird als Vermittlerdienst umgesetzt. Für die Bearbeitung der Attributesets durch die UZS Engine wird die Datenhaltung auf minimal notwendige Nachvollziehbarkeits- bzw. Governance, Risk & Compliance-Anforderungen beschränkt. Es werden keine schützenswerten Personendaten persistiert.
- Für den eUZ werden ausschliesslich Daten erhoben, die für eine Ummeldung erforderlich sind. Die Personendaten werden grundsätzlich in den bestehenden Datenbanken (EWR, ZEMIS, Infostar etc.) belassen bzw. persistiert. Die Daten werden vom UZS nur im Rahmen der von der umzugswilligen Person angeforderten Leistungserbringung zwischen den berechtigten Partnern ausgetauscht.
- Es ist prinzipiell eine aktive. Zustimmung der umzugswilligen Person erforderlich (user centric approach).

Im Rahmen der Erarbeitung des SOLL Prozesses, sind Hinweise auf rechtlich zu hinterfragende Datenerhebungen bei bestehenden IST Prozessen aufgetaucht. Entsprechend kantonaler oder kommunaler Praxis können heute (besonders) schützenswerte Personendaten unnötiger und teilweise vermutlich ungerechtfertigter Weise erhoben und persistiert werden. In solchen Fällen ist damit zu rechnen, dass die Umsetzung des eUZ stellenweise auch Anpassungen in der bestehenden Praxis der Datenerhebungen und Verwendung beim analogen Umzug nach sich ziehen wird.

To Do 2013:

Die Ausprägung der Datenschutzfragen wird stark abhängig von der tatsächlichen Umsetzung des UZS sein. Wird er als Dienst aus der Cloud angeboten? Betrieben von Bund, Kantonen oder Privaten? Wie sieht das exakte Zusammenspiel mit IAM B2.06 aus?

Nach Abschluss der SOLL Modellierung inkl. sämtlicher Subprozesse, sind die Datenflüsse umfassend zu untersuchen. Es gilt deutlich zu machen, welche Attribute wo bearbeitet, woher und wohin übermittelt werden, wer Datenhalter ist und wer die Hoheit über die Daten innehat. Danach sind in Zusammenarbeit mit Datenschützern des Bundes und (aller) Kantone die spezifischen Anforderungen für alle Teil- und den Gesamtprozess zu spezifizieren (Verschlüsselung, Monitoring, Nachvollziehbarkeit etc.).

Eine möglicherweise grössere Herausforderung könnte sich dabei aus der notwendigen Haltung von (besonders) schützenswerten Personendaten für die Dauer der Prozess Durchführung ergeben. Dies betrifft im Speziellen die Zeitdauer zwischen dem Abschicken des Ummelde –Antrags durch die umzugswillige Person (Abschluss E-Payment) und dem Abschluss des eUZ. Auf Grund der manuellen Bearbeitung des

[12] SIEMENS (2006)
[13] SIEMENS (2005)
[14] Allenfalls könnten hier vertragliche Hürden existieren, z.B. die eine Anwendung der Authentifizierung ausserhalb des Zahlungsverkehrs nicht zulassen. Solchen könnte durch Anpassung des Prozesses begegnet werden, etwa indem über eine Verbindung von Authentifikation und E-Payment.
[15] DSG

Antrags (Einwohnerdienste, Migrationsämter) können hier mehrere Tage, eventuell gar Wochen vergehen. Es ist in Zusammenarbeit mit Datenschützern zu eruieren, wie die Haltung der Personendaten im System während dieser Zeit zu gestalten ist.

Als Leitlinien für die weitere Orientierung 2013 können die Ausführungen zu ZEMIS (ZEMIS-Verordnung, SR 142.513, Abschnitt 6) und Infostar (Zivilstandsverordnung, SR 211.112.2, 9. Kapitel), sowie die im Rahmen von B2.06 und SuisseTrustIAM gemachten bzw. zu machenden Überlegungen dienen.

3.6 Informatiksicherheit

Überlegungen zu Verfügbarkeit, Durchgängigkeit und Sicherheit der eigentlichen Systeme sind bei der technischen Realisierung des UZS zu beachten. Der eUZ funktioniert nur über mehrere Systeme hinweg und weist, insbesondere in der zeitnahen Umsetzung, entsprechende Abhängigkeiten auf. Fragen die bezüglich Verfügbarkeit und Performance zu beantworten sind:

- Was ist die Belastbarkeit / Performanz der Systeme?
- Können die Systeme die zu erwartende Mehrbelastung bewältigen?
- Was ist die Verfügbarkeit der Systeme?
- Wie werden das übergreifende Monitoring und die Benachrichtigung gelöst?
- Wer ist für den eUZ verantwortlich, wer treibt den Prozess voran?
- Was ist, wenn eine Komponente im Prozess länger ausfällt?
- Was geschieht mit einem angestossenen eUZ beim Ausfall von sedex?
- Gibt es organisatorische Umgehungslösungen?
- Garantieren diese die Medienbruchfreiheit?

Grundsätzlich sollte hier davon ausgegangen werden können, dass die für den eUZ notwendigen Systeme gängigen Standards zur Informatiksicherheit entsprechen. Es sollte jedoch geprüft werden, ob diese den Anforderungen der Bearbeitung und Übermittlung von schützenswerten Personendaten in einem durchgängigen, medienbruchfreien und hoch verfügbaren Prozess genügen.

Für 2013 empfiehlt es sich mehrere Pilotversuche und systemische Evaluationen durchzuführen. Dabei kann möglicherweise auf Erfahrungen aus den Tests zum Online Schalter St. Gallen (Hacker Angriffe, Eindringen in Systeme, Zugriff auf schützenswerte Ressourcen etc.) zurückgegriffen werden.

3.7 Einbettung in Portale

Aus primärer Nutzerperspektive, also aus Sicht der EinwohnerInnen, ist der eUZ sinnvollerweise kontextuell eingebettet in umfassenden Dienstleistungsportalen umzusetzen. Dies können Einwohner- bzw. Bürgerportale ebenso wie Portale von Drittanbietern (z.B. Post, Umzugsunternehmen etc.) sein.

Aus sekundärer Nutzerperspektive, also aus Sicht der EWD, ist die Möglichkeit der Einbettung in bestehende Verwaltungssoftware, also in erster Linie die EWK-Lösungen, eine zu erfüllende Voraussetzung.

Entsprechend muss die Realisierung durch die Anbieter der unterschiedlichen Benutzerportale erfolgen. Dies bedingt im Weiteren, dass die Anbieter auch für die Berücksichtigung unterschiedlicher E-Payment Systeme bestehende Lösungen integrieren können.

Es empfiehlt sich allenfalls eine technische Beschreibung des Prozesses, um den Anbietern eine automatische Verarbeitung zu ermöglichen. Dadurch kann die Aktualität der Implementierungen auch bei Veränderungen des Prozesses sichergestellt werden.

Für Einbettung in bzw. Verbindung zu den EWK-Lösungen ist eine erste Anforderung, dass die entsprechenden Prozesse und Schnittstellen beschrieben werden. Es muss sichergestellt werden, dass alle Schnittstellen zu Kantonen, Bund und Dritten über eine Serviceplattform angeboten werden, von wo sie dann von den Anbietern direkt angesprochen werden können.

Derzeit dürften die meisten Schnittstellen jedoch noch nicht in Echtzeit anbindbar sein. Ausserdem werden Herausforderungen aufgrund des lokalen Betriebs der EWK-Lösungen und fehlende DMZs auftreten. Besondere Herausforderungen dürften sich bei der Implementierung in umfassendere Lösungen (z.B. Geres), bei der Definition und Einhaltung von Systemgrenzen ergeben. Es ist daher mit einer längeren Übergangs- bzw. Implementierungsdauer zu rechnen. Im Architekturworkshop Bund wurde nicht umsonst festgehalten, dass A1.12 eine deutliche Abhängigkeit von den externen Anbietern der Lösungen aufweist.

2013 ist ausserdem zu klären, ob der UZS als Hintergrunddienst aus der Cloud oder als dezentral implementierter Code auf der Infrastruktur der Portalbetreiber zu realisieren ist. Es empfiehlt sich für die technische Umsetzung die Zusammenarbeit mit allen oder zumindest den führenden Anbietern von Bürgerportalen und EWK-Lösungen zusammenzuarbeiten.

Bezüglich der Authentifizierung ist eine Zusammenarbeit mit den Anbietern und B2.06 gefordert. Es gilt hierbei Fragen zu klären, wie eine externe Authentifizierung über B2.06 mit den EWK-Lösungen ermöglicht, bzw. wie bestehende Authentifizierungsmethoden (Login Einwohnerportal, Verwaltungssoftware) mit IAM B2.06 verbunden werden können.

4. Zu berücksichtigen 2013

Aufgrund der beschlossenen Auslagerung des IAM an den von B2.06 zu schaffenden Dienst, ist 2013 die enge Zusammenarbeit mit IAM B2.06 zwingend notwendig. Ausserdem sind die generellen Aspekte rund um Betrieb, Finanzierung, Zuständigkeiten, Verantwortlichkeiten etc. für den Einsatz von IAM B2.06 beim eUZ zu klären. Daneben sind jedoch auch frühzeitig Überlegungen zu alternativen Authentifizierungsmöglichkeiten anzustellen, sollte IAM B2.06 nicht termingerecht zur life Schaltung des eUZ zur Verfügung stehen.

Folgende Aspekte sind 2013 priorisiert abzudecken:

Attribut Übermittlung:

- Sicherstellen der Anbindung aller notwendigen Register an die IAM Plattform.
- Sicherstellen der zeitnahen Attributantwort von EWR, Infostar, Zemis.
- Klärung der autoritativen Datenquelle bei Divergenzen zwischen EWR, Infostar und Zemis.
- Klärung (mit B2.02, B2.13, B1.14) über die Verwaltung und Bereitstellung der Referenzdaten der sedex Adapter zur Adressierung des Payload beim Versand der aktualisierten Attributesets.

Authentisierungsmittel, Credentials:

- Klärung der Anforderungen (Qualität, Benutzerfreundlichkeit etc.) an Credentials für den eUZ.
- Definition existierender Credentials für den Einsatz im eUZ.
- Klärung der Einsatzmöglichkeiten von bestehenden Authentifizierungen von Einwohnerportalen und Einwohnerkontrolllösungen mit IAM B2.06.
- Klärung der Problematik unterschiedlicher Namensschreibweisen bei der eindeutigen Identifikation von Personen.
- Klärung des initialen mapping von Credential zu EWR Attributeset.
- Klärung des Prozesses der Aktualisierung des Credential zu EWR mapping.
- Klärung der Einsatzmöglichkeiten der AHVN13 / Sozialversicherungsnummer beim eUZ, Zusammenarbeit bezüglich Anforderungen an Rechtsetzung.

Datenschutz:

- Nach erfolgter Verifikation des SOLL Prozesses (inkl. sämtlicher Teilprozesse) muss eine vollständige Analyse der Datenflüsse, detailliert nach Attributen, Bearbeitung, Übermittlung, Haltung etc. gemäss DSG erfolgen. Die Datenflüsse sind danach mit Datenschutzbeauftragten der Kantone und des Bundes zu verifizieren.

Technische Realisierung:

- Klärung der grundlegenden Konzeption von Cloud basiert (aaS) oder dezentral betrieben.
- Klärung der Anforderungen an die Einbettbarkeit in bestehende Lösungen von online Portalen und EWD-Lösungen.

4.1.1 Weitere Herausforderungen: Recht

Verantwortlichkeit:

- Wer ist für das Vorantreiben des eUZ verantwortlich?
- Wer übernimmt bei welchem Schritt im eUZ die Verantwortung?
- Wie sieht die rechtliche Situation bezüglich Stellvertretung der verschiedenen Beteiligten (EinwohnerIn, EWK, KMA, etc.) durch den UZS bei den einzelnen Prozessschritten aus?

Datenschutz:

- Können Infostar, Zemis, EWR bei der Ummeldung mit einem einheitlichen Attributeset beliefert werden?
- Erlaubt der Datenschutz die Übertragung von Attributesets an Register von Dritten?

Nachvollziehbarkeit, Auditierbarkeit:

- Was muss der eUZ bezüglich Governance, Risk & Compliance erfüllen?
- Wie kann die Nachvollziehbarkeit der Kommunikation zwischen Beteiligten sichergestellt werden, die nicht über sedex miteinander verbunden sind?

IAM B2.06:

- Darf die Authentifizierung der EinwohnerInnen an ein externen IAM Service ausgelagert werden?
- Besteht diesbezüglich Rechtsetzungsbedarf?
- Welche Regelungen werden zwischen IAM B2.06 und UZS benötigt?
- Was sind die rechtlichen Voraussetzungen für die Anbindung des UZS an die notwendigen Register?

Credential:

- Welche Authentifizierungsstärke ist rechtlich notwendig?
- Welches elektronische Credential kann als Äquivalent zur analogen Identifikation angesehen werden?
- Können Credentials der EK-Lösungen aus rechtlicher Perspektive im UZS verwendet werden?

Grundsätzlich besteht für die Authentifizierung der EinwohnerInnen im eUZ die Herausforderung, dass auf nationaler Ebene kein frei benutzbarer, eineindeutiger Personenidentifikator zur Verfügung steht. Mit der AHVN13, die Teil des EWR Attributeset ist, existiert ein solcher, jedoch ist die Anwendung an eine gesetzliche Grundlage gebunden. 2013 bietet sich hierzu durch die anstehenden ZertES Revision(en) ein window of opportunity. Wiederum ist hierbei die Zusammenarbeit mit B2.06 zu suchen.

4.1.2 Weitere Herausforderungen: Technik

- Welche weiteren Register müssen zeitnah abgefragt werden können werden?
- Können diese ebenfalls über IAM B2.06 mit dem UZS verbunden werden?
- Können über IAM B2.06 auch Daten zurück zu den Registern gesendet werden?
- Wie werden Datenquellen von Dritten aus der Privatwirtschaft an den UZS angebunden?
- Kann / soll dazu sedex zum Einsatz kommen?
- Lassen sich die „Meldungen an Dritte“ allenfalls standardisiert umsetzen?

4.1.3 Weitere Herausforderungen: Organisation, Prozesse

- Wie wird die Ablösung der analogen Authentisierungsmittel durch die digitalen umgesetzt?
- Wie wird der Support beim eUZ (24/7, ganze Schweiz) organisiert.
- Wer ist dazu gemäss Leistungsauftrag legitimiert?
- Stehen die entsprechend notwendigen Ressourcen zur Verfügung?
- Abschaffung Heimatschein: Wie und wo wird der EWR-Eintrag Initial zur Person verlinkt?
- Subprozesse: Wo stellen sich welche weiteren Anforderungen an Authentifizierung?

5. Vorschlag Umsetzungsbegleitung

Für die Flankierung der Führungsprozesse von A1.12[16] schlagen wir für 2013 folgende Priorisierung und Umsetzung vor:

5.1 Priorisierung 2013

Recht	Technik	Organisation, Prozesse
• Datenschutz: Sicherstellung der Konformität des eUZ • Sicherstellung der Zugriffsrechte auf alle notwendigen Register	• Realisierung von IAM B2.06 • Sicherstellung des Echtzeit Zugriffs auf EWR, Infostar, Zemis • Sicherstellung der Einbettung in bestehende online Portale und EWD-Lösungen	• Definition von Authentisierungsmitteln (elektronisch & analog)

5.2 Umsetzung 2013

1. Validierung der Authentifizierungs- und Referenzierungsprozesse
   (1. Quartal 2013)

   - Zusammenarbeit mit B2.06 und den weitere priorisierten B-Vorhaben
   - Technische und prozessuale Realisierbarkeit des Konzepts prüfen
   - Umsetzung IAM B2.06 begleiten
   - Adressierung des sedex Payload durch den UZS zu klären

2. Institutionalisierung Arbeitsgruppe „Datenschutz und Credentials“
   (1. Quartal 2013)

   - Zusammenarbeit mit Datenschützern des Bundes und der Kantone institutionalisieren
   - Gesamtprozess (anhand der vollständigen Datenflüsse) auf Verträglichkeit mit bzw. Einhaltung der Datenschutzbestimmungen überprüfen
   - Zusammenarbeit mit B2.06 und Datenschützern: Möglichkeiten bezüglich Authentisierungsmittel für die EinwohnerInnen zu definieren.

3. Institutionalisierung Arbeitsgruppe „Technische Realisierung“
   (2013 ff.)

   - Zusammenarbeit mit den führenden Anbietern von EK-Lösungen, online Portalen institutionalisieren
   - Möglichkeiten der Implementierung validieren
   - Technische Spezifikationen festzulegen

[16] Dolf, C. (2012)

6. Anhang

6.1 Quellennachweis

BFS (2008) Die Harmonisierung amtlicher Personenregister - Kantonale und kommunale Einwohnerregister. Amtlicher Katalog der Merkmale. Version 01.2008, online unter: http://www.bfs.admin.ch/bfs/portal/de/index/news/publikationen.html?publicationID=3032

BFS (2012) Registerharmonisierungsgesetz, sedex, online unter: http://www.bfs.admin.ch/bfs/portal/de/index/news/00/00/02.html

DSB ZH (2012) Datenschutzbeauftragter des Kantons Zürich, online unter: https://review.datenschutz.ch/datenschutz/content/01_02_08_04.php?cid=1.4.2).

Dolf, C. et al. (2012) A1.12 Fachkonzept (Status: In Arbeit).

Dolf, C. et al. (2012.1) A1.12 Projektauftrag

Dolf, C. et al. (2012.2) Pflichtenheft Massnahme 8 „Authentifizierung, Datenschutz und Informatiksicherheit“

eCH (2012) Best Practice Rahmenkonzept SuisseTrustIAM

IHE (2012) IT Infrastructure (ITI) Technical Framework Volume 1 (ITI TF-1) Integration Profiles, online unter: http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Vol1.pdf

IHE (2012) IT Infrastructure Technical Framework, Volume 2a (ITI TF-2a), Transactions Part A – Sections 3.1 – 3.28, online unter: http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Vol2a-2.pdf

KdK (2012) B1.02 Rechtsgrundlagen: Abschlussbericht Lösungsansätze und Massnahmen

SIEMENS (2006), Program HUSKY, GUIDE PoC ZH/SG Relocation Service, Release 1.0

SIEMENS (2005), Proof of Concept Relocation Service Zürich / St. Gallen, Lösungsvorstellung, Integration VISA 3D-Secure.

SR 142.513 Verordnung über das Zentrale Migrationsinformationssystem (ZEMIS-Verordnung)

SR 211.112.2 Zivilstandsverordnung (ZStV)

SR 235.1 Bundesgesetz über den Datenschutz (DSG)

SR 431.02 Bundesgesetz über die Harmonisierung der Einwohnerregister und anderer amtlicher Personenregister (Registerharmonisierungsgesetz, RHG)

6.2 Unterlagen SOLL Prozess elektronischer Umzug

6.2.1 BPMN Modellierungen SOLL Prozess elektronischer Umzug

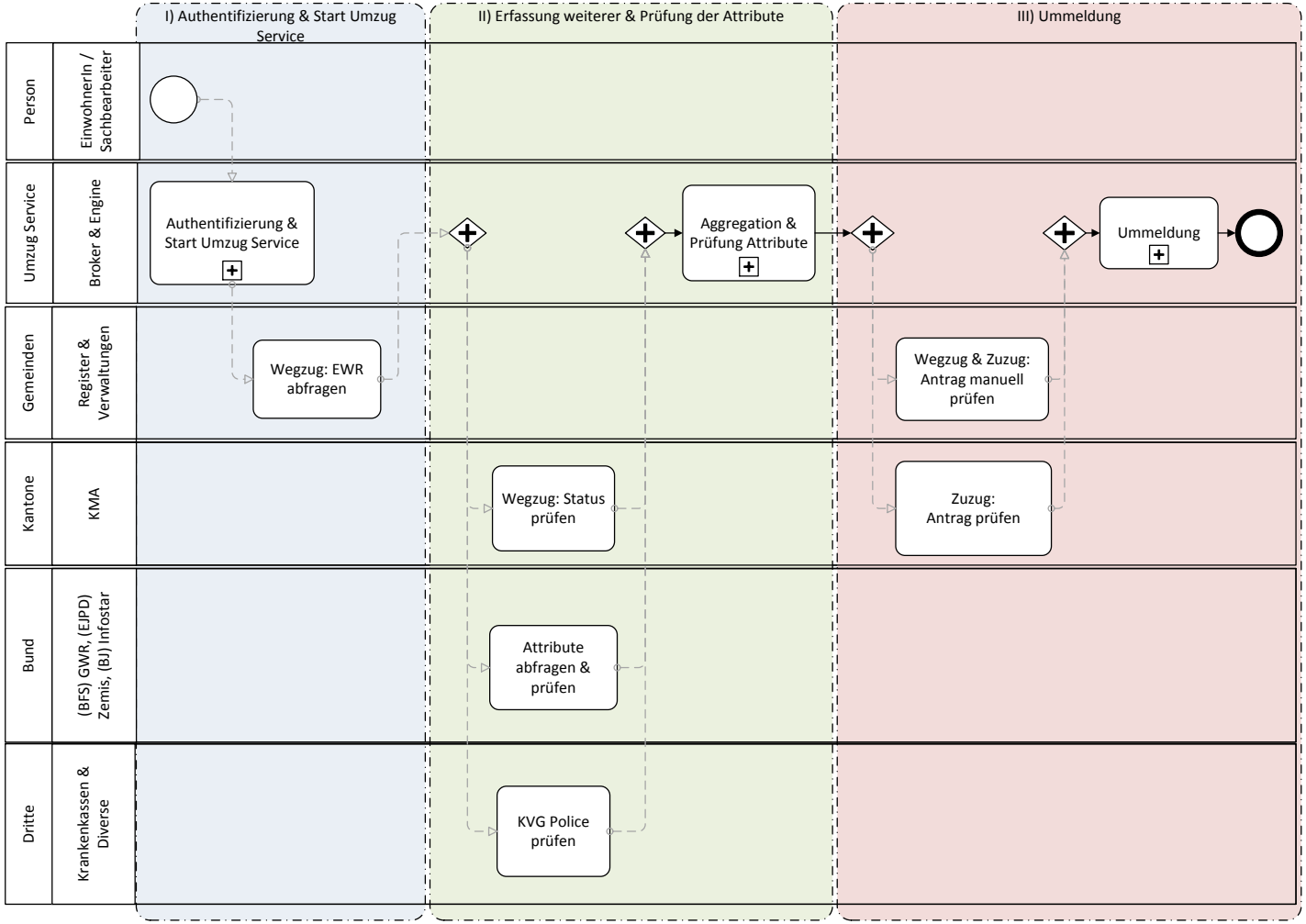


Abbildung 12 - Abbildung 12 A1.12 SOLL - Überblick, zeitnah, minimal

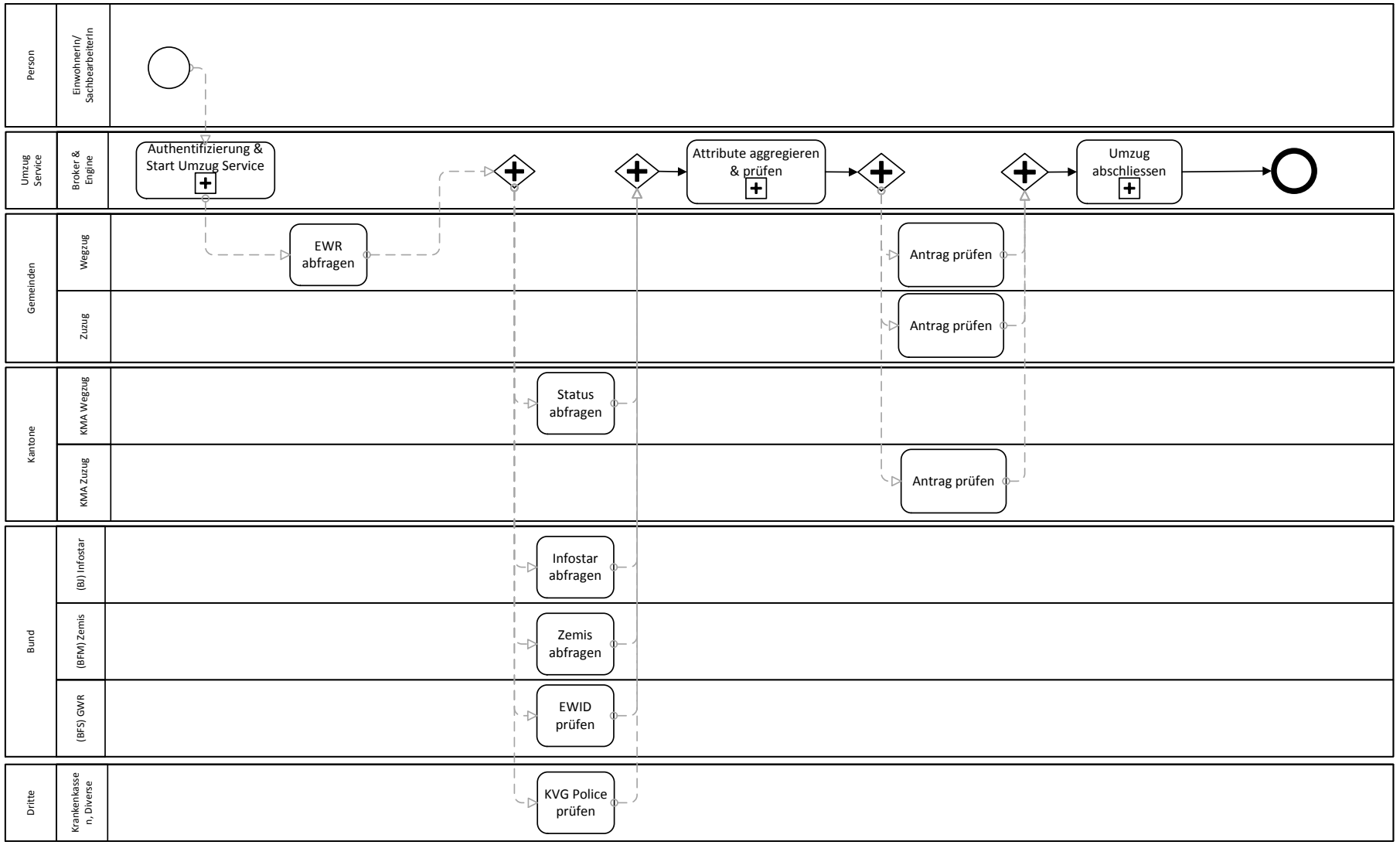


Abbildung 13 A1.12 SOLL - Überblick, zeitnah, detailliert

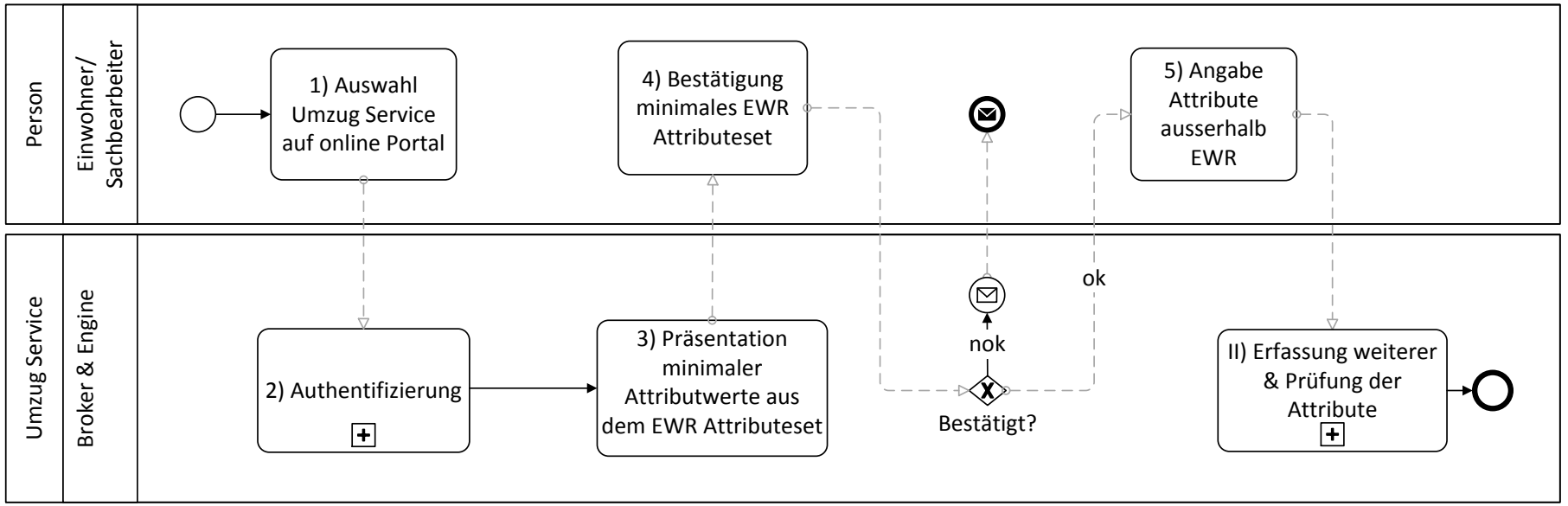


Abbildung 14 A1.12 SOLL - I. Authentifizierung & Start Umzug Service

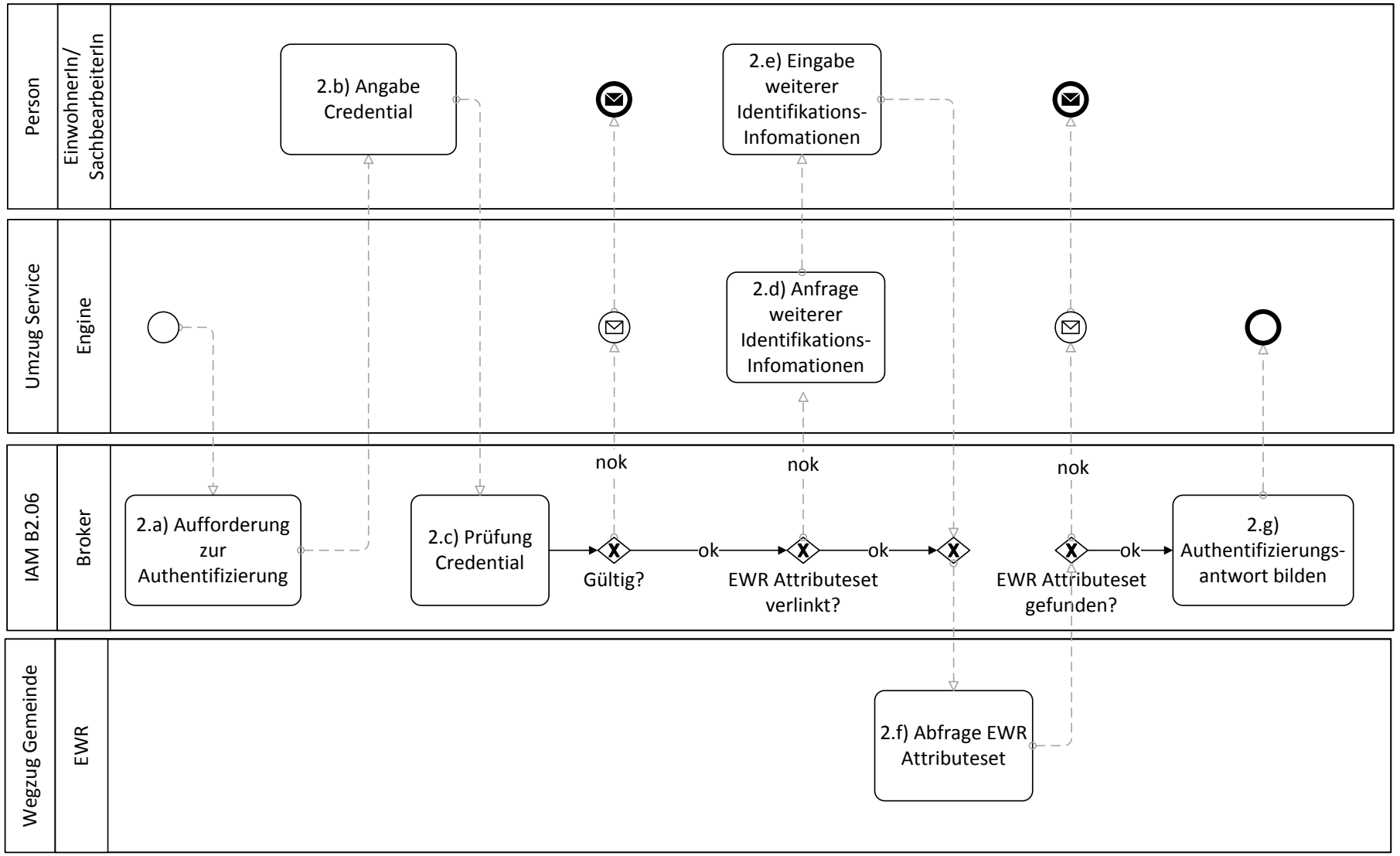


Abbildung 15 A1.12 SOLL - Subprozess I.2) Authentifizierung

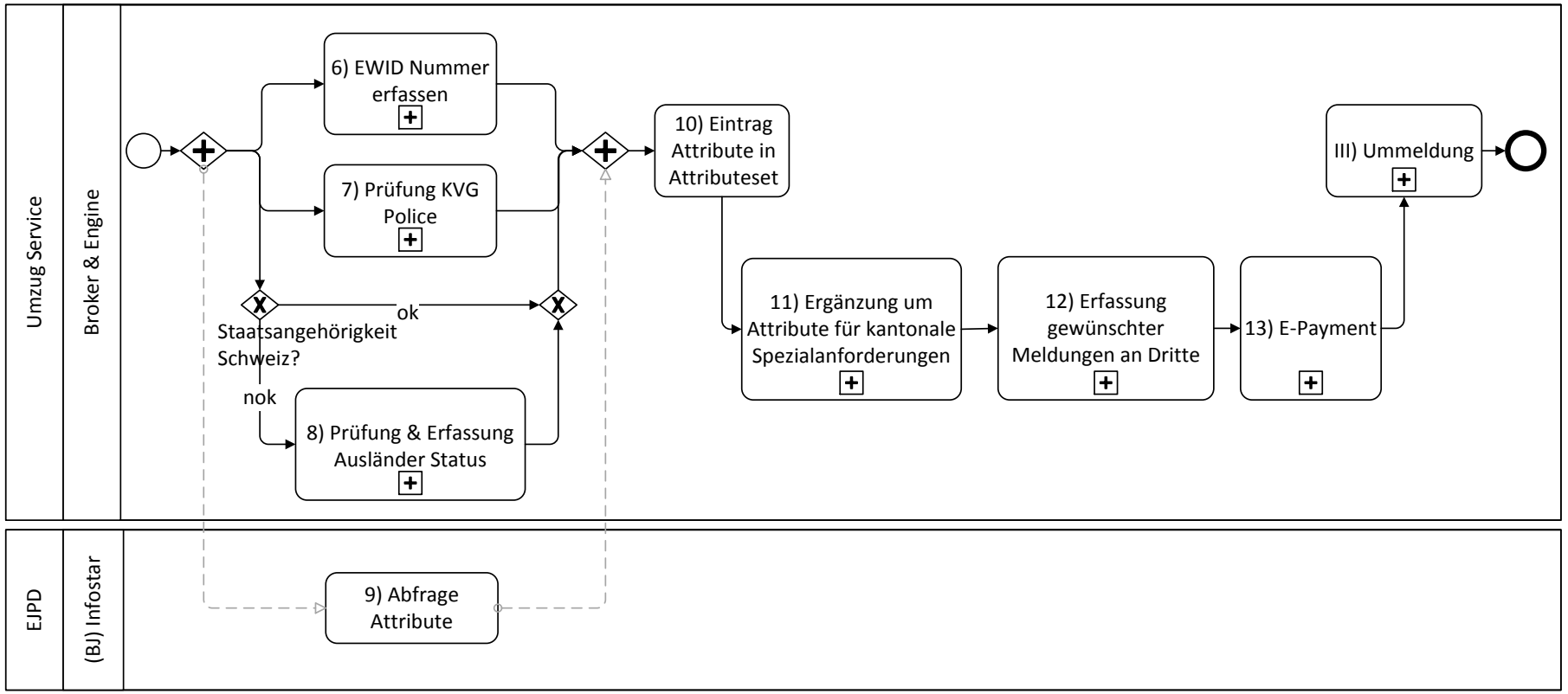


Abbildung 16 A1.12 SOLL - II. Erfassen weiterer & Prüfung der Attribute

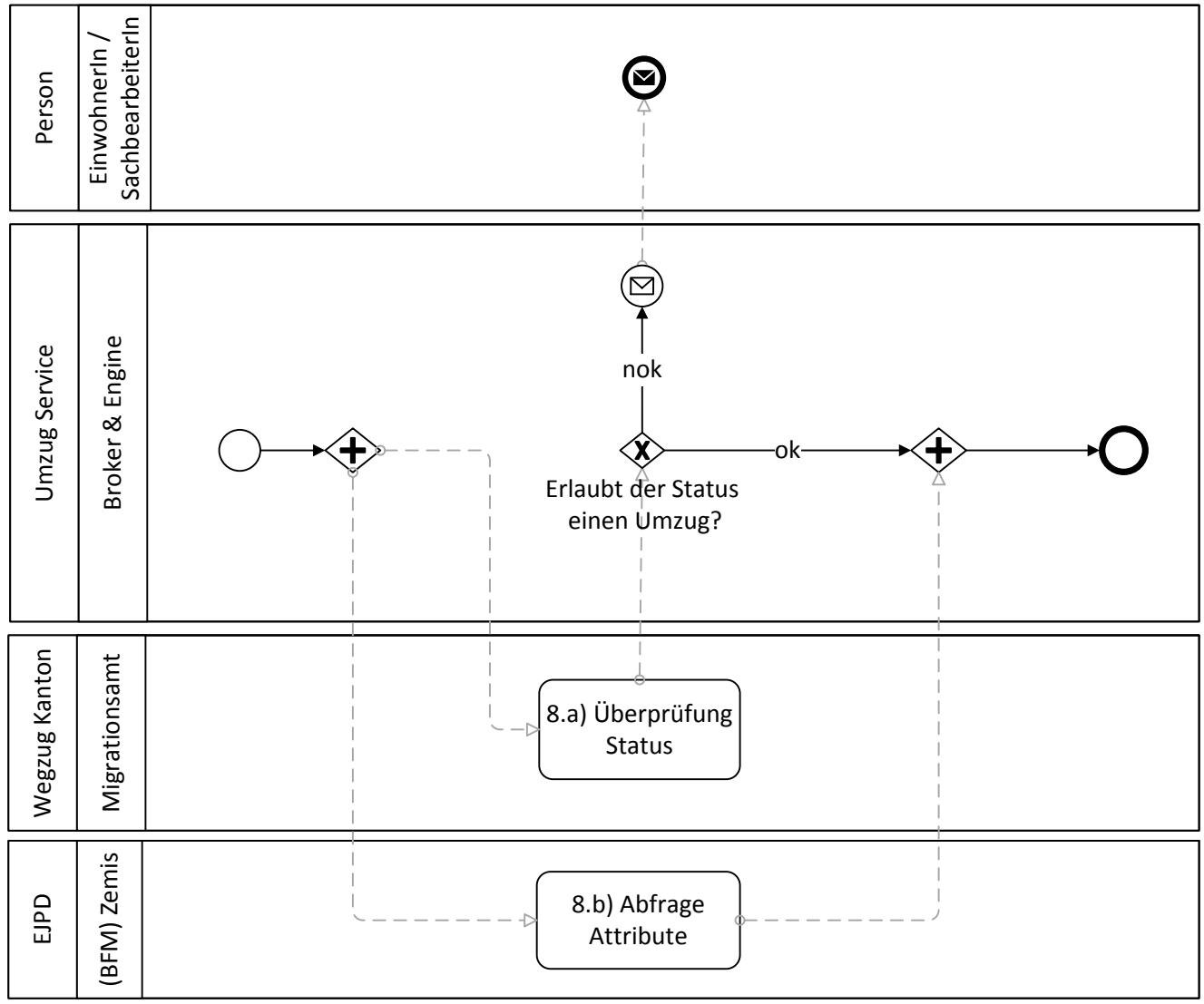


Abbildung 17 A1.12 SOLL - Subprozess II.8) Prüfung & Erfassung Ausländer Status

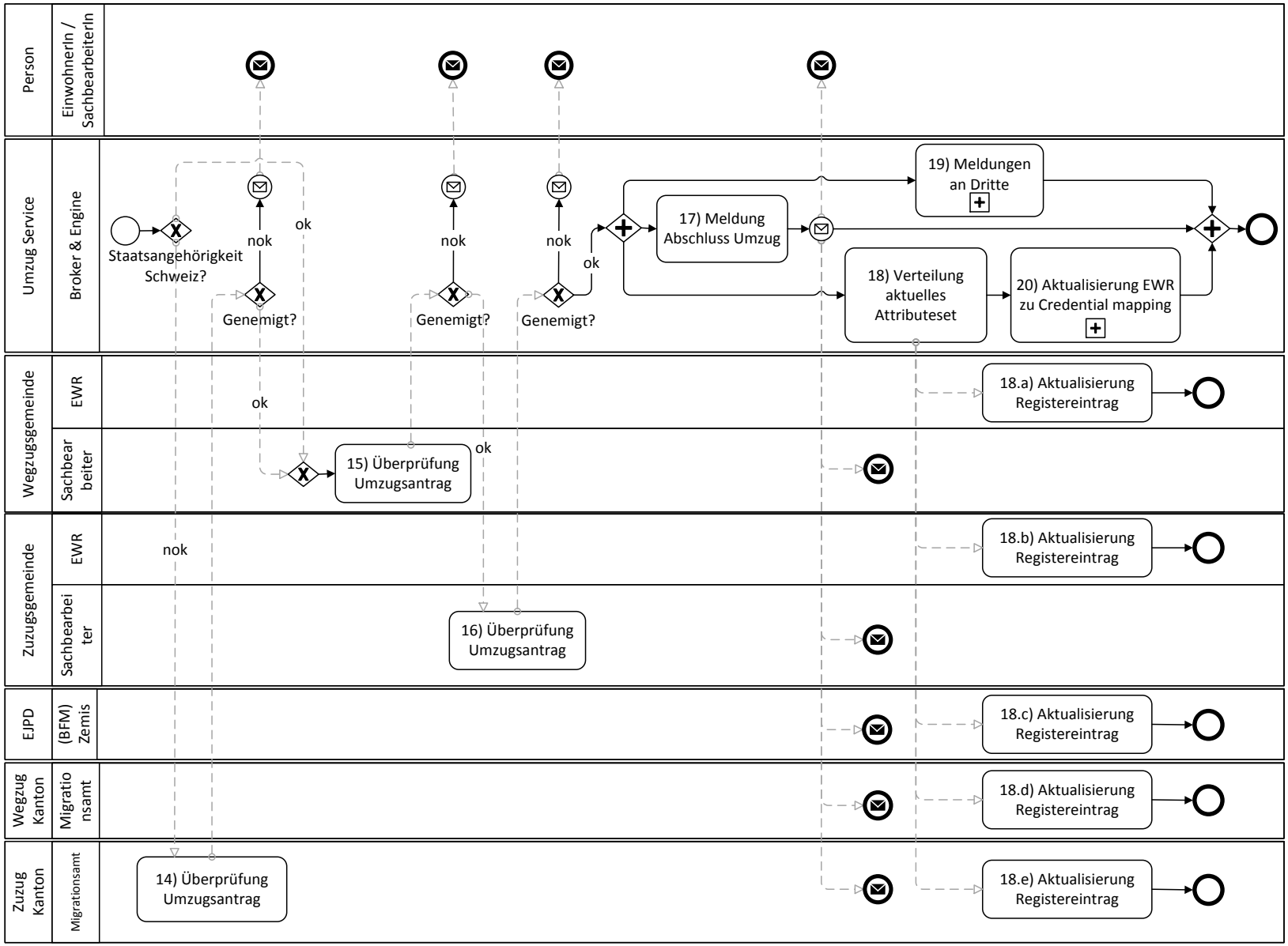


Abbildung 18 A1.12 Soll - III. Ummeldung

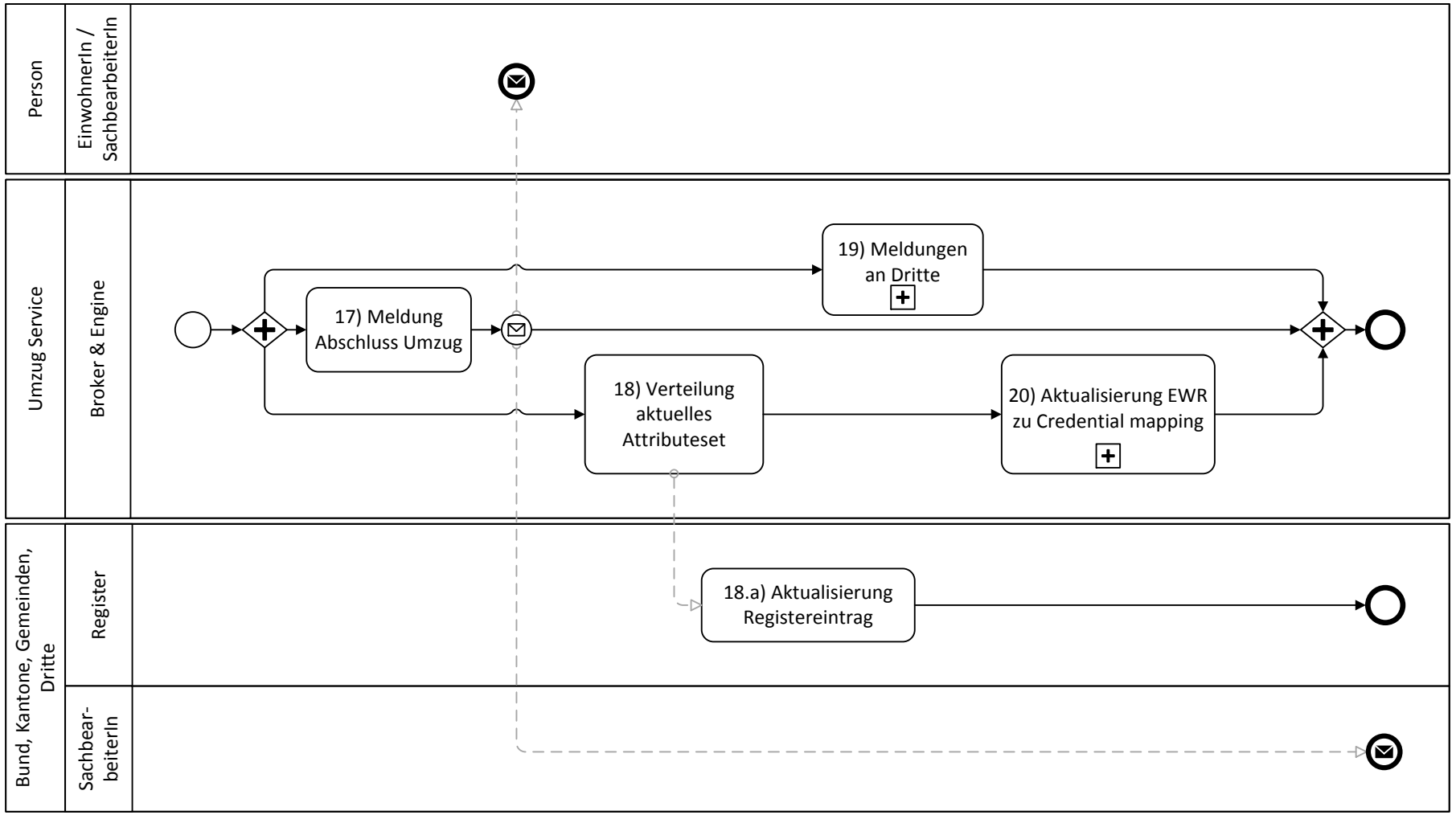


Abbildung 19 A1.12 SOLL - III. Ummeldung (Schlussteil, minimal)

6.2.2 Beschreibung zur Modellierung

1) Auswahl Umzug Service auf online Portal
Die Person wählt den UZS auf dem online Portal der Wegzugs- oder Zuzugsgemeinde, der Post oder des Bundes aus. Wo der Prozess gestartet wird ist nicht entscheidend.

2) Authentifizierung
Dieser Prozess behandelt die Authentisierung und Authentifizierung der umzugswilligen Person bzw. oder der in Stellvertretung agierenden SachbearbeiterIn.

2.a) Aufforderung zur Authentisierung
Die Person wird vom IAM B2.06 aufgefordert sich mit einem Credential zu authentisieren.

2.b) Angabe Credential
Die Person gibt das zur Authentisierung notwendige Credential an und sendet die Informationen an IAM B2.06 zurück.

2.c) Prüfung Credential
Die Person wird authentifiziert und es wird geprüft ob bereits ein EWR Attributeset bei IAM B2.06 verlinkt ist. Falls eine entsprechende Verlinkung gefunden wird, weiter mit 2.f). Falls nicht, weiter mit Schritt 2.d).
Wurde kein gültiges Credential gefunden, erfolgt über den UZS eine Meldung an die Person (Credential angeben, Credential beschaffen oder Umzug analog am Schalter durchführen).

2.d) Anfrage weiterer Identifikationsinformationen
Ist kein Link zu einem EWR vorhanden, so wird die Person angefragt, weitere Identifikationsinformationen anzugeben.

2.e) Eingabe weiterer Identifikationsinformationen
Wenn im IAM B2.06 noch kein EWR Attributeset mit der Identität der Person verlinkt ist, wird letztere zur Angabe weiterer Identifikationsattribute aufgefordert. Diese umfassen z.B. den amtlichen Namen, Vornamen, Geburtsdatum, Geburtsort und die Wegzug Gemeinde.

2.f) Abfrage EWR Attributeset
Beim EWR der verlinkten (2.c) bzw. angegebenen (2.e) Gemeinde (Wegzug) wird das entsprechende Attributeset der Person abgefragt. Das Attributeset bzw. die Fehlermeldung („kein passendes Attributeset gefunden“) wird an IAM B2.06 übermittelt.
Wurde kein passendes Attributeset gefunden, erfolgt über den UZS eine Meldung an die Person (zu definieren: soll der eUZ abgebrochen und die Person zur analogen Durchführung aufgefordert werden (entspricht vorliegender Modellierung) oder soll ein Loop eingebaut werden, bei dem die Person zur Überprüfung der angegebenen Informationen (primär Wegzug Gemeinde) aufgefordert wird?). an den UZS.

2.g) Authentifizierungsantwort bilden
Wurde (mindestens) ein passendes EWR Attributeset geliefert, bildet IAM B2.06 mit diesem und der Bestätigung der Gültigkeit des Credentials die Authentifizierungsantwort und übermittelt diese an den UZS.

3) Präsentation minimaler Attributwerte aus dem EWR Attributeset
Die Person bekommt nun Name, Vorname und Adresse aus dem EWR Attributeset angezeigt.
Wurden mehr als ein passendes Attributeset beim EWR der Wegzug Gemeinde gefunden (keine eindeutige Zuweisung möglich), so werden aus den gefundenen Attributesets jeweils Name, Vorname und Adresse angezeigt.

4) Bestätigung minimales EWR Attributeset

Mit dem Wählen eines Attributesets bestätigt die Person die Zugehörigkeit von ersterem zu sich bzw. zu der am Schalter befindlichen EinwohnerIn.
Wird die Auswahl von der Person als inkorrekt angeben bzw. keines der angezeigten Auswahlmöglichkeiten als zu ihr zugehörig bestätigt, so erfolgt eine Aufforderung, den Prozess analog am Schalter der Gemeinde durchzuführen. Dies führt zur Beendigung des Online Umzugs.

5) Angabe Attribute ausserhalb EWR

Die Person muss die Zuzugsadresse (Strasse, Ort und PLZ) sowie das Umzugsdatum angeben. Allenfalls können hier zusätzliche Attribute angegeben werden, die nicht im minimalen Attributeset vom EWR enthalten sind (z.B. Angaben zur KVG Police, EWID Nummer etc.).

6) EWID Nummer erfassen

In diesem Prozess wird die EWID von der Person angeben, vom Umzug Service überprüft und erfasst.

7) Prüfung KVG Police

In diesem Prozess wird die KVG Police von der Person angeben, vom Umzug Service überprüft und erfasst.
Im Falle von einer fehlenden Police wird dies im Attributeset vermerkt, welches am Ende des Prozesses an die Zuzugsgemeinde geschickt wird.

8) Prüfung und Erfassung Ausländer Status

8.a) Überprüfung Status (KMA)

Der Ausländerstatus wird beim KMA des Wegzugskantons überprüft. Dies ist ein maschineller Prozess; die manuelle Überprüfung wird im Prozessschritt 14) vom KMA des Zuzugskantons durchgeführt.
Bei Einigung der KMAs kann man diesen Schritt löschen und die Statusüberprüfung direkt via ZEMIS klären und bestätigen lassen.

8.b) Abfrage Attribute

Attribute der Person, mit entsprechendem Ausländer EWR Attribut, werden in ZEMIS abgefragt.

9) Abfrage Attribute (Infostar)

Attribute der Person werden in Infostar abgerufen.

10) Eintrag Attribute in Attributeset

Die zusammengetragenen Attribute aus den Prozessen 6), 7) und 9) werden ins aktuelle Attributeset geschrieben.

11) Ergänzung um Attribute für kantonale Spezialanforderungen

In diesem Schritt kann der Einwohner zusätzliche Attribute angeben, die vom Zuzugskanton oder der Zugzugsgemeinde gefordert werden und nicht dem Minimalset nach Art. 6 RHG (vgl. 6.3) entsprechen. Hier können z.B. Drittstaatsangehörige Auszüge aus dem Betreibungsregister hochladen bzw. bestellen.

12) Erfassen gewünschter Meldungen an Dritte

In diesem Prozess kann die Person Dritte angeben, die über den Umzug informiert werden sollen. Beispiele sind Post, Bank, etc.

13) E-Payment

In diesem Prozess autorisiert die Person den Umzug Service ihr bei einem erfolgreichen Abschluss des Prozesses (Aktivität 17) den zu bezahlenden Betrag zu belasten.
Nach erfolgter Autorisierung wird eine briefliche Mitteilung an die Wegzugsadresse der umzugswilligen Person gesendet (Inhalt: Prozess gestartet, Prozess ID, Kontaktinformationen). Dies dient dem Nachweis für die Person und der Verhinderung missbräuchlicher Ummeldungen durch Dritte.

14) Überprüfung Umzugsantrag durch Sachbearbeiter KMA Zuzugskanton

Der Umzugsantrag wird dem KMA des Zuzugskantons gesendet. Dem KMA ist es überlassen, wie es den Antrag prüfen möchte (z.B. EU-Staatsangehörige maschinell und Drittstaatsangehörige manuell). Relevant ist hier, dass mit den KMAs definiert wird, welche Attribute genau für die Überprüfung des Umzugsantrags erforderlich sind und – unabhängig von maschinell oder manuell – dass es am Ende des Schritts vom KMA ein OK/nicht OK bekommt.
Falls der Antrag nicht genehmigt wird, so erhält die Person eine Mitteilung, dass der Prozess nicht abgeschlossen werden konnte und sie sich am Schalter der Wegzugsgemeinde melden muss.
Damit eine medienbruchfreie Kommunikation ermöglicht werden kann, muss es dem Sachbearbeiter möglich sein, den Antrag elektronisch zu überprüfen.

16) Überprüfung Umzugsantrag durch Sachbearbeiter Zuzugsgemeinde

Der Umzugsantrag wird einem Sachbearbeiter der Zuzugsgemeinde gesendet und von diesem manuell überprüft. Falls der Antrag nicht genehmigt wird, so erhält die Person eine Mitteilung, dass der Prozess nicht abgeschlossen werden konnte und sie sich auf am Schalter der Wegzugsgemeinde melden muss.
Damit eine medienbruchfreie Kommunikation ermöglicht werden kann, muss es dem Sachbearbeiter möglich sein den Antrag elektronisch zu überprüfen (OK Button).

17) Meldung Abschluss Umzugsprozess

Der Umzug Service meldet der Person, den Sachbearbeitern der Migrationsämter von Wegzugs- und Zuzugskantonen, den Sachbearbeitern der Wegzugs- und Zuzugsgemeinde und ZEMIS, dass der Umzugsprozess erfolgreich war. In der Meldung an die Person ist zudem eine Quittung von der ausgelösten Zahlung (vgl. Prozess 13)) enthalten.

18) Verteilung aktuelles Attributeset

Das aktuelle Attributeset wird dem EWR der Wegzugs- und Zuzugsgemeinde, den Migrationsämtern des Wegzugs- und Zugzugskanton, sowie ZEMIS elektronische gesendet.
Es muss mit Datenabweichungen zwischen Infostart, ZEMIS und EWR gerechnet werden. Annahmen:
- Die Wohnortsdaten sind IMMER im EWR aktueller.
- Die Zivilstandsdaten sind IMMER in Infostar aktueller.

18.a) Aktualisierung Registereintrag in EWR Wegzugsgemeinde

18.b) Aktualisierung Registereintrag in EWR Zuzugsgemeinde

18.c) Aktualisierung Registereintrag in ZEMIS

18.d) Aktualisierung Registereintrag Migrationsamt Wegzugskanton

18.e) Aktualisierung Registereintrag Migrationsamt Zuzugskanton

19) Meldungen an Dritte

Wurden im Prozess 12) Dritte angegeben, so werden diese in diesem Prozess entsprechend informiert.

20) Aktualisierung EWR zu Credential mapping IAM B2.06

Damit beim nächsten Umzug das richtige EWR vom IAM B2.06 vermittelt werden kann, muss die Verlinkung von Credential zu EWR Eintrag (alt: Wegzugsgemeinde, aktuell: Zuzugsgemeinde) aktualisiert werden.