A-SIT Plus GmbH

eIDAS-Personen-Matching

Dokumentation

Version 1.0

05. Juli 2022

Thomas Lenz – thomas.lenz@egiz.gv.at

Thomas Zefferer – thomas.zefferer@a-sit.at

Inhaltsverzeichnis

1. Einleitung

Die bisher im Einsatz befindliche Version des eIDAS-Knotens (bestehend aus MS-Connector und eIDAS Node AT) war nur unzureichend in der Lage, bestehende Register-Einträge von Benutzer:innen in ZMR und/oder ERnP aufzufinden. Dies führte zu Situationen, in denen fälschlicherweise neue Register-Einträge angelegt wurden und Benutzer:innen somit mit zwei elektronischen Identitäten ausgestattet wurden. Bei Service Providern führte dies in weiterer Folge zu doppelten Benutzerkonten für ein und dieselbe Person.

Ziel war es dar, die bisherige Situation zu verbessern und bestehende Benutzereinträge in Registern im Rahmen eIDAS-basierter Anmeldeprozesse zuverlässiger zu finden. Die sollte über einen zusätzlichen expliziten Matching-Schritt im Rahmen des Anmeldeprozesses erreicht werden. Dieses Dokument beschreibt diesen neu implementierten Matching-Schritt und die dahinterliegende Umsetzung.

1.1. Bisherige Lösung

Dieses Dokument beschreibt die vorgenommenen Erweiterungen des bisherigen österreichischen eIDAS-Knotens zur Erreichung der vorgesehenen Matching-Funktionalität. Abbildung 1 zeigt im Überblick die Architektur des bisherigen Systems, das zur Erreichung der gewünschten Matching-Funktionalität entsprechend erweitert wurde. Das bisherige System ermöglichte es EU-Bürgern bereits, sich an Services der österreichischen E-Government-Infrastruktur (z.B. Finanz-Online) mit ihrer ausländischen eID (z.B. deutscher elektronischer Personalausweis) anzumelden.

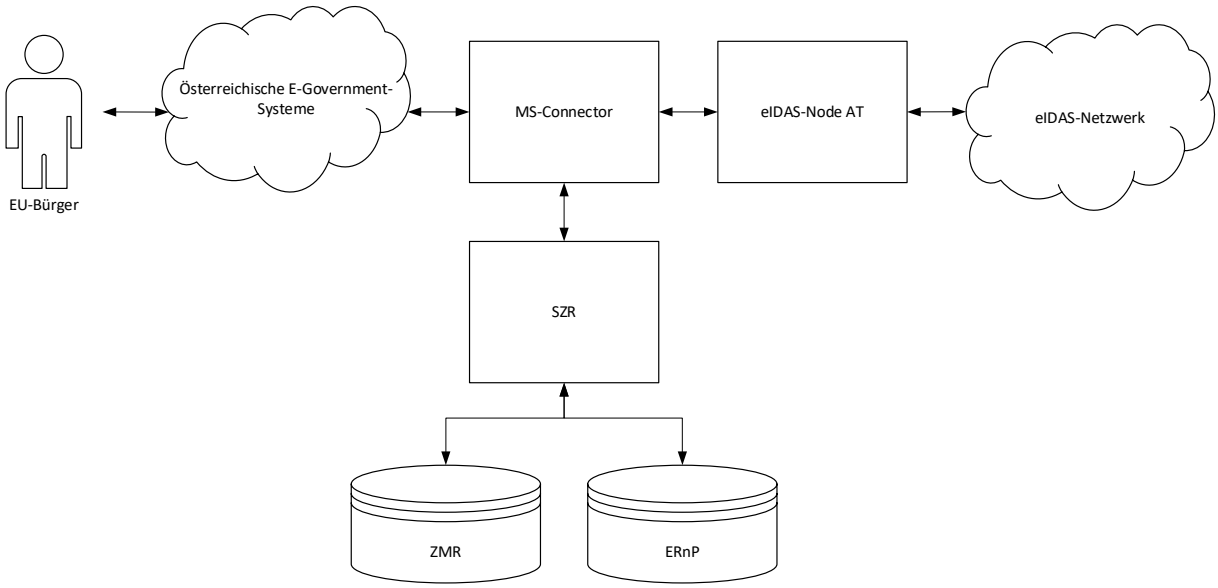

Abbildung 1. Rudimentäre Architektur des bisherigen Systems.

Der Anmeldeprozess wurde dabei bisher schon vom jeweiligen E-Government-Service an den MS-Connector und von dort weiter an die eIDAS-Node AT delegiert. Diese beiden Komponenten werden durch das BMI betrieben. Die eIDAS-Node AT veranlasste in weiterer Folge eine Authentifizierung der Benutzer:in über das eIDAS-Netzwerk. Als Resultat erhielt die eIDAS-Node AT und in weiterer Folge der MS-Connector die bestätigten Identitätsdaten (PersonIdentifier, MDS (Vorname, Familienname, Geburtsdatum) und optional weitere Attribute) der Benutzer:in. Der MS-Connector bezog bisher

über das SZR eine Personenbindung für die Benutzer:in und retournierte diese schließlich dem ursprünglich anfragenden E-Government-Service. Das Service konnte die Benutzer:in damit bisher schon identifizieren und anmelden.

Die bisherigen im Rahmen eines Anmeldeprozesses durchzuführenden Schritte sind in Abbildung 2 dargestellt. In der bisherigen Umsetzung des österreichischen eIDAS-Knotens wurden bestehende Register-Einträge der aktuellen Benutzer:in implizit im dritten Schritt, d.h. im Zuge des Bezugs der Personenbindung, gesucht.

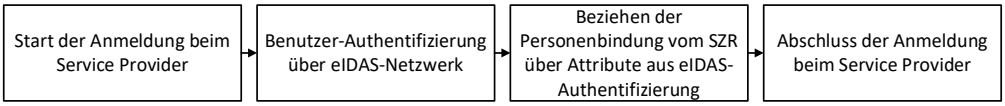

Abbildung 2. Bisherige Schritte eines Anmeldeprozesses.

1.2. Erweiterungen

Die in diesem Dokument beschriebene erweiterte Umsetzung des österreichischen eIDAS-Knotens adressiert primär jenen Prozessschritt, in dem der MS-Connector des österreichischen eIDAS-Knotens über das SZR eine Personenbindung für die Benutzer:in bezieht. In Abbildung 2 ist dies der dritte Prozessschritt. Für diesen ergaben sich folgende Herausforderungen:

- Der MS-Connector muss zuverlässig feststellen, ob die Benutzer:in bereits über einen SZR-Eintrag verfügt (d.h. entweder im ZMR oder im ERnP eingetragen ist).
- Für die Suche eines eventuell bereits vorhandenen Eintrags stehen dem MS-Connector nur jene Daten zur Verfügung, die im Zuge des laufenden Anmeldeprozesse vom eIDAS-Netzwerk bereitgestellt oder direkt über ein GUI von der Benutzer:in abgefragt wurden.
- Die vom eIDAS-Netzwerk bereitgestellten Daten sind je nach Herkunftsland der Benutzer:in unterschiedlich. So liefert zum Beispiel Deutschland potenziell ein anderes Attribut-Set aus als Spanien. Zudem sind die Eigenschaften der ausgelieferten Attribute nicht immer einheitlich (z.B. sind je nach Land ausgelieferte PersonIdentifier nicht immer persistent, sondern können sich zwischen zwei Anmeldevorgängen ein und derselben Benutzer:in auch ändern).
- Vor allem die vom eIDAS-Netzwerk bereitgestellten Daten müssen nicht zwingendermaßen mit den Daten eines bestehenden Register-Eintrags übereinstimmen, da sich sowohl Identifier als auch Benutzerattribute (z.B. Familiennamen) ändern können.
- Bestehende Einträge in ZMR und/oder ERnP können, müssen aber nicht Resultat einer vorangegangenen eIDAS-Anmeldung sein. Dadurch kann nicht davon ausgegangen werden, dass bestehende Register-Einträge Daten aus einer eIDAS-Anmeldung enthalten.

Ziel der in diesem Dokument beschriebenen Umsetzung war es, trotz dieser Herausforderungen ein möglichst zuverlässiges Auffinden bestehender Register-Einträge der involvierten Benutzer:in zu gewährleisten. Die Anzahl von false-positive Matches und false-negative Matches sollte dabei bestmöglich minimiert werden. Dazu wurde der bisherige Anmeldeprozess (siehe Abbildung 2) um einen zusätzlichen expliziten Matching-Schritt wie in Abbildung 3 rot dargestellt erweitert.

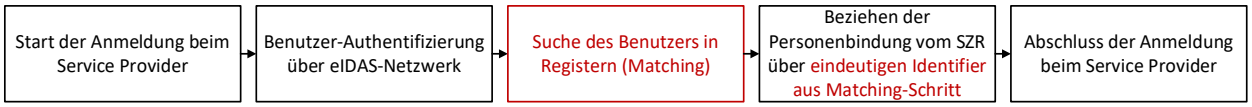

Abbildung 3. Erweiterung des Anmeldeprozesses um expliziten Matching-Schritt.

Im Rahmen dieses neuen expliziten Matching-Schritts werden noch vor Bezug der Personenbindung die bestehenden Inhalte der Register ZMR und ERnP systematisch durchsucht, um zu eruieren, ob die aktuelle Benutzer:in dort bereits eingetragen ist. Diese Suche geht über jene Matching-Mechanismen hinaus, die in der bisherigen Umsetzung des MS-Connector beim Bezug der Personenbindung implizit passierten. Wird die Benutzer:in im Zuge des neu hinzugefügten Matching-Schritts gefunden, kann im nachfolgenden Schritt (Beziehen der Personenbindung) das Ergebnis des Matching-Schritts zur eindeutigen Referenzierung der Benutzer:in (bzw. ihres Registereintrags) verwendet werden.

Abbildung 4 zeigt notwendige Erweiterungen an der bisheringen Architektur zur Umsetzung des implementierten zusätzlichen Matching-Schritts. Aus Abbildung 4 wird deutlich, dass sich die Architektur des Systems nicht grundlegend änderte. Es wurde lediglich notwendig, dass der MS-Connector direkt mit ZMR und ERnP kommuniziert, um diese Register gezielt nach Einträgen zum Benutzer durchsuchen zu können. Darüber hinaus wurde die Erweiterung des MS-Connector um ein Matching-Modul notwendig, das notwendige Matching-Funktionen im MS-Connector umsetzt.

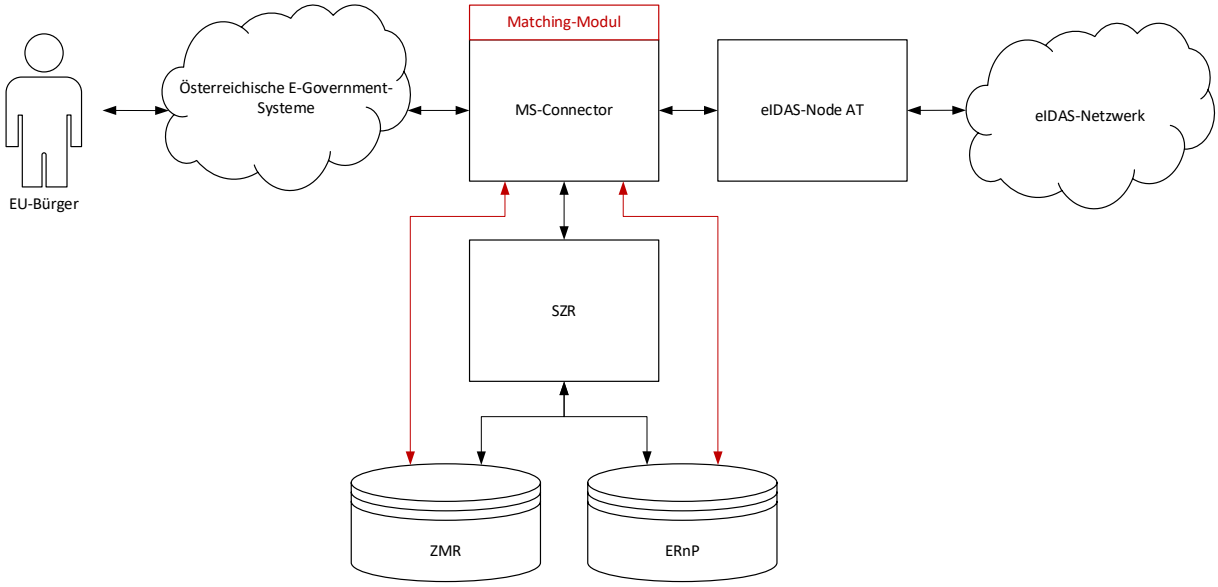

Abbildung 4. Vorgenommene Erweiterungen der Architektur.

1.3. Annahmen

Der in diesem Dokument beschriebenen Umsetzung notwendiger Matching-Operationen liegen folgende Annahmen zugrunde:

- Es wird angenommen, dass sich die Benutzer:in ehrlich verhält und korrekte Angaben macht. Macht die Benutzer:in mutwillig falsche Angaben (z.B. zu früheren Wohnsitzen), kann sie ein prinzipiell mögliches erfolgreiches Matching potenziell gezielt verhindern (falsch-negatives Matching). Dies kann je nach Anwendung von Vorteil für die Benutzer:in sein und muss daher als Angriffspfad betrachtet werden. Wichtig ist in

diesem Zusammenhang jedoch, dass die Benutzer:in durch gezielte Falschangaben in der Regel kein falsch-positives Matching erzwingen, d.h. nicht die elektronische Identität einer anderen Person übernehmen kann.

- Dem Konzept liegt die Annahme zugrunde, dass optionale Attribute, die von einem Mitgliedsstaat bereitgestellt werden, auch tatsächlich beim österreichischen eIDAS-Knoten ankommen und deren Übermittlung nicht etwa von der Benutzer:in bewusst unterbunden wird. Durch ein Unterbinden der Übermittlung optionaler Attribute kann die Benutzer:in potenziell wiederum ein erfolgreiches Matching unterbinden. Dies kann je nach Anwendung von Vorteil für die Benutzer:in sein und muss daher als Angriffspfad betrachtet werden.

1.4. Einschränkungen

Die in diesem Dokument beschriebene Umsetzung notwendiger Matching-Operationen ist folgenden Einschränkungen unterworfen:

- Die Umsetzung bietet keine Garantie, dass ein Matching in jedem Fall korrekt durchgeführt wird (d.h. ein existierender Register-Eintrag auch tatsächlich immer gefunden wird). Daher kann die Umsetzung das Entstehen von doppelten Registereinträgen für ein und dieselbe Person nicht vollkommen verhindern. Dies schon deshalb, da die Benutzer:in durch gezielte Falschangaben oder unvollständige Angaben den Matching-Prozess bewusst stören kann. Die Umsetzung stellt jedoch in jedem Fall eine Verbesserung zur aktuellen Situation dar und kann einen hohen Prozentsatz an möglichen Fällen abdecken – speziell, wenn die Benutzer:in wie vorgesehen kooperativ mit dem System interagiert.

- Die Umsetzung deckt nicht die Durchführung eventuell notwendiger manueller Kitt-Prozesse ab. Die Umsetzung sieht vor, dass der automatisierte Matching-Prozess abbricht, wenn die Notwendigkeit eines manuellen Kitt-Prozesses identifiziert wird. Solche manuellen Kitt-Prozesse können vor allem in unvorhergesehenen Situationen notwendig werden, wenn beispielsweise Suchabfragen im SZR uneindeutige Ergebnisse liefern. Die Benutzer:in wird in diesem Fall an einen entsprechenden Kontakt verwiesen.

1.5. Version

Diese Dokumentation bezieht sich auf Version 1.3 der Komponente MS-Connector. Mit dieser Version wurde die in diesem Dokument beschriebene Matching-Funktionalität integriert. Prinzipiell ist die Dokumentation auch für nachfolgende Versionen gültig, da nicht zu erwarten ist, dass sich in diesen Versionen signifikante Änderungen an der Matching-Funktionalität ergeben werden. Sollte die Matching-Funktionalität in einer späteren Version erweitert werden, wird auch eine aktualisierte Version dieser Dokumentation erstellt und ausgeliefert. Bis dahin behält diese Version der Dokumentation ihre Gültigkeit.

2. Risikoabschätzung

Das implementierte Matching-Konzept verfolgt unterschiedliche Strategien, bestehende Register-Einträge der aktuellen Benutzer:in in ZMR und ERnP aufzufinden und der Benutzer:in entsprechend zuzuordnen. Dabei ist von besonderer Bedeutung, dass keine falschen Zuordnungen vorgenommen werden. Folgende falsche Zuordnungen sind dabei prinzipiell denkbar:

- **Falsch positive Zuordnung:** Dabei wird der Benutzer:in ein falscher bestehender Register-Eintrag zugeordnet, d.h. es wird der Benutzer:in ein Registereintrag einer anderen natürlichen Person zugeordnet.
- **Falsch negative Zuordnung:** Dabei wird ein bestehender Registereintrag der jeweiligen Benutzer:in nicht gefunden und ihr daher nicht zugeordnet.

Beide Arten von falschen Zuordnungen haben negative Auswirkungen. Bei einer falsch negativen Zuordnung wird fälschlicherweise davon ausgegangen, dass für die aktuelle Benutzer:in noch kein Registereintrag besteht und daher ein neuer Eintrag angelegt. Die Benutzer:in erhält dadurch eine neue elektronische Identität (d.h. eine neue Stammzahl). Dies macht eine spätere (manuelle) Zusammenführung von Identitäten notwendig.

Gravierender sind die Auswirkungen einer falsch positiven Zuordnung. Hier wird der aktuellen Benutzer:in eine falsche bestehende elektronische Identität zugeordnet. Die Benutzer:in könnte also für eine andere natürliche Person fungieren, d.h. deren elektronische Identität übernehmen. Für diesen Fall muss speziell geprüft werden, ob eine böswillig handelnde Benutzer:in durch bewusstes Fehlverhalten (z.B. bewusste Fehleingaben) eine falsch positive Zuordnung provozieren kann.

Die meisten umgesetzten Matching-Schritte passieren weitgehend automatisiert und ohne aktives Zutun der Benutzer:in. Dementsprechend entstehen hier keine zusätzlichen Risiken. Ein beschränktes Risiko ergibt sich jedoch für jenen Matching-Schritt, in dem über die (ehemaligen) Adressdaten der Benutzer:in ein entsprechender Eintrag in den Registern gesucht wird. Hier ergibt sich für böswillig handelnde Benutzer:innen folgender möglicher Angriffspfad:

1) Die böswillige Benutzer:in macht einen Datenzwilling ausfindig, d.h. eine Person mit gleichem Vornamen, Familiennamen und Geburtsdatum.
2) Die böswillige Benutzer:in macht gültige (aktuelle oder ehemalige) Adressdaten dieses Datenzwillings ausfindig.
3) Im Zuge des Matching-Vorgangs gibt die böswillige Benutzer:in die Adressdaten ihres Datenzwillings an.
4) Da das Minimum Dataset (Vornamen, Familiennamen und Geburtsdatum) und eingegebene Adressdaten mit dem Registereintrag des Datenzwillings übereinstimmen, wird dieser Registereintrag der böswilligen Benutzer:in zugeordnet (falsch positive Zuordnung). Die Benutzer:in kann sich als der Datenzwilling ausgeben.

Die Anzahl an Datenzwillingen ist stark begrenzt, kann aber nicht ausgeschlossen werden. Zudem können Adressdaten nicht als geheim angenommen werden. Aus diesem Sachverhalt ergibt sich ein beschränktes Risiko, dass böswillige Benutzer:innen über gezielte falsche Verwendung des adressbasierten Matching-Schritts die elektronische Identität von Datenzwillingen übernehmen.

Aus diesem Grund wurde in der Umsetzung dieses Feature deaktivierbar umgesetzt. Über einen Konfigurationsparameter kann der Betreiber des österreichischen eIDAS-Knotens festlegen, ob Benutzer:innen ein Matching über Adressdaten angeboten wird. Wird dieses Feature aktiviert, müssen die damit einhergehenden oben beschriebenen Risiken bewusst sein.

3. Matching-Konzept

Dieser Abschnitt beschreibt das umgesetzte Matching-Konzept. Das Konzept wird in den folgenden Unterabschnitten über eine detaillierte Prozessbeschreibung beschrieben.

3.1. Prozessüberblick

Die einzelnen Prozessschritte des vollständigen Matching-Prozesses und deren Zusammenspiel sind in Anhang A graphisch dargestellt.

3.2. Prozessschritte

Der gesamte Matching-Prozess ist im Folgenden über dessen einzelne Prozessschritte beschrieben. Die Beschreibung korrespondiert mit der graphischen Darstellung in Anhang A. Die Nummern der Aufzählung unten korrespondieren mit den Nummern der Prozessschritte in der graphischen Darstellung in Anhang A.

1) Die Benutzer:in authentifiziert sich am eIDAS-Knoten mit ihrer ausländischen eID (z.B. deutscher elektronischer Personalausweis). Die Daten aus der Anmeldung liegen am österreichischen MS-Connector vor. Die Benutzer:in hat mit ihrem Web-Browser eine etablierte Session mit dem MS-Connector und wurde soeben vom österreichischen eIDAS-Node zum MS-Connector weitergeleitet. Dem MS-Connector sind aus der soeben erfolgten eIDAS-Anmeldung folgende Daten zur Benutzer:in bekannt:
    a) **PersonIdentifier:** Eindeutiger der Benutzer:in zugeordneter Identifikator, der die Benutzer:in im eID-System ihres Heimatlandes eindeutig identifiziert.
    b) **MDS:** Minimal Dataset bestehend aus Vornamen, Familienname und Geburtsdatum der Benutzer:in.
    c) **Zusätzliche Attribute:** Weitere Attribute, die vom eID-System des Heimatlandes der Benutzer:in optional an den österreichischen eIDAS-Knoten ausgeliefert wurden. Das Set verfügbarer zusätzlicher Attribute ist länderspezifisch. Generell kann nicht davon ausgegangen werden, dass zusätzliche Attribute im Rahmen einer Anmeldung erhalten werden, auch wenn das eID-System des involvierten Landes das prinzipiell unterstützen würde.
2) Der MS-Connector sucht in den Registern (ZMR, ERnP) nach Einträgen, die den soeben aus der eIDAS-Anmeldung erhaltenen PersonIdentifier beinhalten. Der weitere Prozessfluss hängt davon ab, wie viele Register-Einträge über die Suchabfrage gefunden werden.
    a) **1 Treffer:** Das ist der Idealfall. Unter dem aus der eIDAS-Anmeldung erhaltenen PersonIdentifier wurde genau ein Register-Eintrag gefunden. Da der PersonIdentifier unique ist und genau einer Person zugeordnet werden kann, kann davon ausgegangen werden, dass die Person in den Registern eindeutig gefunden wurde. Das Matching der aus der eIDAS-Anmeldung erhaltenen Daten auf die vorhandenen Register-Daten war also erfolgreich. Der Prozess setzt fort in Schritt 3).

b) **0 Treffer:** Der aus der eIDAS-Anmeldung erhaltene PersonIdentifier ist in den Registern bisher nicht bekannt. Das kann zwei Gründe haben: (1) Entweder ist dies der erste Kontakt mit dieser Person, sodass diese in den Registern noch unbekannt ist. (2) Oder die Person ist in den Registern bereits vorhanden, allerdings ist dem entsprechenden Registereintrag der aktuelle PersonIndentifier noch nicht zugewiesen (z.B., weil die Person einen neuen eID mit geänderten PersonIdentifier erhalten hat). In jedem Fall müssen hier zusätzliche Schritte unternommen werden, um einen eventuell bereits vorhandenen Registereintrag zur Person mit anderen Mitteln zu finden. Der Prozess setzt fort in Schritt 5).

c) **Mehr als 1 Treffer:** Dieser Fall sollte nicht eintreten, da der PersonIdentifier unique ist. Retournieren die Register als Ergebnis auf die Suchabfrage trotzdem mehr als einen Eintrag, ist davon auszugehen, dass bereits in den Registern mehrere Einträge zur Person bestehen. Hier ist daher ein manueller Kitt-Prozess notwendig. Der Prozess bricht an dieser Stelle mit einem Fehler ab.

3) Der MS-Connector vergleicht die von den Registern (ZMR, ERnP) erhaltenen Daten mit jenen Daten, die er im Zuge der soeben durchgeführten eIDAS-Anmeldung erhalten hat. Verglichen wird hier in jedem Fall das MDS. Wenn möglich findet auch ein Vergleich zusätzlicher Attribute statt. Aus dem durchgeführten Datenabgleich ergeben sich folgende zwei Möglichkeiten:

   a) **Update nicht erforderlich:** Alle aus der eIDAS-Anmeldung erhaltenen Daten (Person-Identifier, MDS, zusätzliche Attribute (optional)) sind im Register bereits bekannt, d.h. wurden vom Register als Antwort auf die Suchanfrage retourniert. In diesem Fall endet der Prozess an dieser Stelle. Die Benutzer:in ist erfolgreich identifiziert und der MS-Connector kann wie gewohnt mit der Anforderung einer Personenbindung über das SZR fortsetzen.

   b) **Update erforderlich:** Aus der eIDAS-Anmeldung wurden Daten erhalten, die im Register noch unbekannt sind, d.h. im Zuge der Suchabfrage nicht vom Register retourniert wurden. Es ergibt sich also die Notwendigkeit, die Daten im Register zu aktualisieren. Der Prozess setzt dementsprechend in Schritt 4) fort.

4) Der MS-Connector aktualisiert die Daten im jeweiligen Register (ZMR und/oder ERnP). In jedem Fall werden erhaltene eIDAS-Attribute in ZMR und ERnP aktualisiert. MDS und andere Merkmale (Attribute) werden in ZMR und ERnP eingetragen, sofern diese im Registereintrag noch nicht vorhanden sind. Der MDS-Datensatz wird ausschließlich im ERnP aktualisiert, im ZMR findet keine Aktualisierung statt, auch wenn via eIDAS-Anmeldung andere (neuere) MDS-Attribute erhalten wurden. Nach Durchführung dieses Schritts endet der Prozess an dieser Stelle (unabhängig davon, ob die Daten im Register aktualisiert wurden). Die Benutzer:in ist erfolgreich identifiziert und der MS-Connector kann wie gewohnt mit der Aufbereitung und Auslieferung der Identitätsdaten der Benutzer:in an den anfragenden SP fortsetzen.

5) Dieser Prozessschritt wird durchgeführt, wenn die Register-Suche in Schritt 2) in keinem Treffer resultierte. In diesem Fall wird eruiert, ob mit Hilfe der aus der eIDAS-Anmeldung erhaltenen Daten (v.a. der zusätzlichen Attribute) und dem Wissen um das Heimatland der Benutzer:in eine länderspezifische Detailsuche in den Registern möglich ist. Im Fall

einer deutschen Benutzer:in kann z.B. die ursprüngliche Suche in Schritt 2 fehlschlagen, da die Benutzer:in in der Zwischenzeit einen neuen elektronischen Personalausweis und damit auch einen neuen PersonIdentifier erhalten hat. Hier kann dann im Rahmen einer länderspezifischen Detailsuche über das MDS und die zusätzlichen Attribute „Geburtsort“ und „Geburtsname“ eine Detailsuche (ohne PersonIdentifier) durchgeführt werden. Im aktuellen Schritt 5 überprüft also der MS-Connector anhand der verfügbaren Informationen, ob eine länderspezifische Detailsuche möglich ist. Die folgenden beiden Resultate können Ergebnis dieser Überprüfung sein:

a) **Länderspezifische Suche möglich:** Mit den verfügbaren Daten (zusätzliche Attribute, etc.) ist eine länderspezifische Suche möglich. In diesem Fall setzt der Prozess in Schritt 6) fort.

b) **Länderspezifische Suche nicht möglich:** Mit den verfügbaren Daten (zusätzliche Attribute, etc.) ist keine länderspezifische Suche möglich. In diesem Fall wird die länderspezifische Suche übersprungen und der Prozess setzt direkt in Schritt 8) fort.

6) In diesem Schritt wird eine länderspezifische Detailsuche in den Registern durchgeführt. Für deutsche Benutzer:innen kann beispielsweise eine Suche unter Verwendung von MDS und den zusätzlichen Attributen „Geburtsort“ und „Geburtsname“ erfolgen, was laut Angaben aus Deutschland eindeutige Suchergebnisse liefert. In Bezug auf das Resultat der durchgeführten länderspezifischen Register-Suche können drei Fälle unterschieden werden:

   a) **1 Treffer:** Dies ist der Idealfall. Unter Verwendung der verfügbaren Informationen und Daten konnte in den Registern ein einzelner Eintrag gefunden werden. Es kann davon ausgegangen werden, dass dieser Eintrag der aktuellen Benutzer:in zugeordnet werden kann (erfolgreiches Matching). Um bei künftigen Anmeldungen ein erfolgreiches Matching direkt über den PersonIdentifier der Benutzer:in zu erreichen, wird ein automatischer Kitt-Prozess initiiert, in dem die Daten aus der aktuellen eIDAS-Anmeldung der Benutzer:in in den gefundenen Register-Eintrag integriert werden. Der Prozess setzt fort in Schritt 7)a).

   b) **0 Treffer:** Die länderspezifische Register-Suche war nicht erfolgreich und es konnte kein passender Eintrag gefunden werden. Es müssen daher weitere Möglichkeiten versucht werden, ein erfolgreiches Matching auf einen bereits existierenden Eintrag zu erreichen. Der Prozess setzt fort in Schritt 8).

   c) **Mehr als ein Treffer:** Dieser Fall sollte nicht eintreten, da die länderspezifische Suche so umgesetzt sein muss, dass diese Suche eindeutige Ergebnisse liefert, sofern in den Registern zu einer Person keine doppelten Einträge existieren. Retournieren die Register als Ergebnis auf die länderspezifische Suchabfrage trotzdem mehr als einen Eintrag, ist davon auszugehen, dass bereits in den Registern mehrere Einträge zur Person bestehen. Hier ist daher ein manueller Kitt-Prozess notwendig. Der Prozess bricht an dieser Stelle mit einem Fehler ab.

7) In diesem Schritt wird ein Kitt-Prozess durchgeführt. Im Rahmen dieses Kitt-Prozesses werden automatisiert Daten eines bestehenden Register-Eintrags mit zusätzlichen Daten aus der aktuellen Benutzer-Session zusammengeführt. Voraussetzung für die

Durchführung dieses Schritts ist, dass die inhaltliche Ergänzung der Registerdaten rechtlich zulässig ist. Dieser Kitt-Prozess kann an verschiedenen Stellen innerhalb des gesamten Matching-Prozesses notwendig werden. Dementsprechend müssen die unten angeführten Ausprägungen/Varianten des Kitt-Prozesses unterschieden werden. Unabhängig von der konkreten Ausprägung/Variante des Kitt-Prozesses endet der Matching-Prozess nach erfolgreicher Durchführung des Kitt-Prozesses. Die Benutzer:in ist erfolgreich identifiziert und der MS-Connector kann wie gewohnt mit der Aufbereitung und Auslieferung der Identitätsdaten der Benutzer:in an den anfragenden SP fortsetzen.

a) **Variante a):** In dieser Variante werden die aus der eIDAS-Anmeldung erhaltenen Daten der Benutzer:in (PersonIdentifier, MDS, zusätzliche Attribute) mit einem bestehenden Registern-Eintrag, der über verschiedene Suchabfragen gefunden wurde, zusammengeführt.

b) **Variante b):** In dieser Variante werden die aus der ursprünglichen eIDAS-Anmeldung erhaltenen Daten der Benutzer:in (PersonIdentifier, MDS, zusätzliche Attribute) und auch die aus einer weiteren eIDAS-Anmeldung erhaltenen Daten der Benutzer:in (PersonIdentifier, MDS, zusätzliche Attribute) mit einem bestehenden Register-Eintrag, der über verschiedene Suchabfragen gefunden wurde, zusammengeführt. Im Vergleich zu Variante a) müssen in dieser Variante also Daten aus zwei verschiedenen eIDAS-Anmeldungen (ein und derselben Person) mit einem bestehenden Register-Eintrag zusammengeführt werden.

8) Dieser Schritt wird durchgeführt, wenn die Suche über den PersonIdentifier aus der eIDAS-Anmeldung kein Matching mit existierenden Register-Einträgen brachte und zudem auch die nachfolgende länderspezifische Suche entweder gar nicht möglich war, oder ebenfalls keinen Treffer (Matching) mit existierenden Register-Einträgen brachte. In diesem Fall wird in diesem Schritt eine Register-Suche mit dem MDS (Vorname, Familienname, Geburtsdatum) der Benutzer:in durchgeführt. Folgende zwei mögliche Ergebnisse dieser Suche können unterschieden werden:

   a) **0 Treffer:** Das ist das „erwünschte“ Resultat. Wenn sogar die Suche über MDS ohne Miteinbeziehung weiterer Identifikatoren (PersonIdentifier, etc.) keinen Treffer ergibt, kann davon ausgegangen werden, dass die aktuelle Benutzer:in tatsächlich noch nicht in den Registern eingetragen ist. In diesem Fall setzt der Prozess in Schritt 9) fort, in dem die Benutzer:in unter Verwendung der aktuellen Daten aus der durchgeführten eIDAS-Anmeldung im ERnP eingetragen wird.

   b) **Zumindest 1 Treffer:** Retournieren die Register als Antwort auf die Suchanfrage via MDS zumindest einen Treffer, müssen in jedem Fall weitere Schritte für ein eindeutiges Matching durchgeführt werden. Dabei ist es unerheblich, ob genau ein Treffer oder sogar mehrere Treffer retourniert werden. Werden von den Registern mehrere Treffer retourniert, müssen weitere Schritte unternommen werden, um aus den retournierten Treffern den tatsächlich korrekten Register-Eintrag herauszufiltern. Auch wenn nur ein Treffer retourniert wird, kann nicht automatisch von einem korrekten Matching ausgegangen werden, da der Suchanfrage nur das MDS der Benutzer:in zugrunde lag und daher auch der Eintrag eines MDS-Datenzwillings retourniert worden sein könnte. Wird also auf

die Suchanfrage unter Verwendung des MDS zumindest ein Treffer retourniert, setzt der Prozess immer in Schritt 10) fort.

9) In diesem Schritt wird die aktuelle Benutzer:in unter Verwendung ihrer Daten (PersonIdentifier, MDS, zusätzliche Attribute) im ERnP neu angelegt. Über die diesem Schritt vorausgehenden Prozessschritte wurde festgestellt, dass die Benutzer:in bisher nicht in den Registern eingetragen ist. Nach der in diesem Schritt erfolgten Eintragung im ERnP endet der Prozess an dieser Stelle. Die Benutzer:in ist erfolgreich identifiziert und der MS-Connector kann wie gewohnt mit der Aufbereitung und Auslieferung der Identitätsdaten der Benutzer:in an den anfragenden SP fortsetzen.

10) Die bisher skizzierten Prozessschritte verliefen – mit Ausnahme der initialen eIDAS-Anmeldung – gänzlich ohne Benutzerinteraktion, sondern ausschließlich durch gezielte Register-Abfragen. Alle bisherigen Prozessschritte sind für Benutzer:innen also vollkommen transparent und wirken sich nicht negativ auf die User-Experience aus. Ab dem hier beschriebenen Schritt 10) sind jedoch komplexere Matching-Methoden notwendig, die unter anderem auch eine Interaktion mit der Benutzer:in bedingen. Bis zu diesem Schritt 10) wurde über gezielte Registerabfragen bereits festgestellt, dass (1) mit dem PersonIdentifier kein Register-Eintrag zu finden ist, (2) eine länderspezifische Suche nicht möglich ist oder diese keinen Treffer in den Registern liefert und (3) die Suche nur mit dem MDS der Benutzer:in zumindest einen Treffer liefert. In diesem aktuellen Schritt 10) wird die Benutzer:in nun vom MS-Connector über ein GUI gefragt, ob sie als Ergänzung zur schon durchgeführten eIDAS-Anmeldung noch eine weitere eIDAS-Anmeldung durchführen kann, um den MS-Connector mit zusätzlichen Daten (Attributen) zu ihrer Person zu versorgen. Denkbar sind hier (a) eine erneute Anmeldung mit derselben eID, die bereits zu Beginn für die ursprüngliche eIDAS-Anmeldung verwendet wurde, im Rahmen derer nun aber weitere zusätzliche Attribute angefordert und bereitgestellt werden; und (b) eine erneute Anmeldung mit einer anderen eID. Die Benutzer:in gibt die Möglichkeit der Durchführung einer weiteren (alternativen) eIDAS-Anmeldung über das GUI bekannt. Basierend auf dem Input der Benutzer:in ergeben sich zwei Möglichkeiten zum weiteren Vorgehen:

    a) **Weitere eIDAS-Anmeldung möglich:** Die Benutzer:in kann eine weitere (alternative) eIDAS-Anmeldung durchführen. In diesem Fall setzt der Prozess in Schritt 11) mit der Durchführung dieser weiteren eIDAS-Anmeldung fort.

    b) **Weitere eIDAS-Anmeldung nicht möglich:** Die Benutzer:in sieht keine Möglichkeit der Durchführung einer weiteren eIDAS-Anmeldung. In diesem Fall setzt der Prozess in Schritt 14) fort, in dem über das GUI weitere Möglichkeiten der Konkretisierung von Suchabfragen an Register eruiert werden.

11) Hat die Benutzer:in im Schritt 10) über das GUI angegeben, dass sie eine weitere eIDAS-Anmeldung durchführen kann, wird diese in diesem Prozessschritt durchgeführt. Der MS-Connector initiiert dazu einen weiteren Anmeldeprozess über die Komponenten „eIDAS-Node AT“ des österreichischen eIDAS-Knotens. Nach erfolgreicher Durchführung der erneuten eIDAS-Anmeldung erhält der MS-Connector schließlich die Anmeldedaten der Benutzer:in (PersonIdentifier, MDS, zusätzliche Attribute) aus dieser Anmeldung. Achtung: Die erhaltenen Daten sollten sich idealerweise von denen aus der ursprünglichen eIDAS-Anmeldung unterscheiden, ansonsten ist kein verbessertes

Matching erwartbar. Mit dem soeben aus der weiteren eIDAS-Anmeldung erhaltenen (alternativen) PersonIdentifier führt der MS-Connector eine erneute Register-Suche durch. In Bezug auf das Ergebnis dieser Suche können drei Fälle unterschieden werden:

a) **1 Treffer:** Dies ist der Idealfall. Über den PersonIdentifier aus der weiteren eIDAS-Anmeldung konnte genau ein Register-Eintrag gefunden werden. Da der PersonIdentifier unique ist, kann davon ausgegangen werden, dass dieser Eintrag tatsächlich zur aktuellen Benutzer:in gehört. Der Prozess setzt in Schritt 7)b) fort, indem über einen automatisierten Kitt-Prozess die Daten aus dem gefundenen Register-Eintrag mit den Daten aus der ursprünglichen eIDAS-Anmeldung und aus der eben durchgeführten weiteren eIDAS-Anmeldung zusammengeführt werden.

b) **0 Treffer:** Auch der aus der weiteren eIDAS-Anmeldung erhaltene PersonIdentifier ist in den Registern bisher nicht bekannt. Das kann zwei Gründe haben: (1) Entweder ist dies tatsächlich der erste Kontakt mit dieser Person, sodass diese in den Registern noch unbekannt ist. (2) Oder die Person ist in den Registern bereits vorhanden, allerdings ist dem entsprechenden Registereintrag der PersonIndentifier aus der weiteren eIDAS-Anmeldung auch noch nicht zugewiesen. In jedem Fall müssen hier noch zusätzliche Schritte unternommen werden, um einen eventuell bereits vorhandenen Registereintrag zur Person mit anderen Mitteln zu finden. Der Prozess setzt fort in Schritt 12).

c) **Mehr als 1 Treffer:** Dieser Fall sollte nicht eintreten, da der PersonIdentifier unique ist. Retournieren die Register als Ergebnis auf die Suchabfrage trotzdem mehr als einen Eintrag, ist davon auszugehen, dass bereits in den Registern mehrere Einträge zur Person bestehen. Hier ist daher ein manueller Kitt-Prozess notwendig. Der Matching-Prozess bricht an dieser Stelle mit einem Fehler ab.

12) Dieser Prozessschritt wird durchgeführt, wenn die Register-Suche in Schritt 11) in keinem Treffer resultierte. In diesem Fall wird eruiert, ob mit Hilfe der aus der weiteren eIDAS-Anmeldung erhaltenen Daten (v.a. der zusätzlichen Attribute) und dem Wissen um das Heimatland der Benutzer:in eine länderspezifische Detailsuche in den Registern möglich ist. Dieser Prozessschritt ähnelt also Schritt 5), nur dass dieser aktuelle Schritt 12) auf den Daten aus der erneuten (und nicht der ursprünglichen) eIDAS-Anmeldung operiert. Im aktuellen Schritt 12) überprüft also der MS-Connector anhand der verfügbaren Informationen, ob eine länderspezifische Detailsuche möglich ist. Die folgenden beiden Resultate können Ergebnis dieser Überprüfung sein:

a) **Länderspezifische Suche möglich:** Mit den verfügbaren Daten (zusätzliche Attribute, etc.) ist eine länderspezifische Suche möglich. In diesem Fall setzt der Prozess in Schritt 13) fort.

b) **Länderspezifische Suche nicht möglich:** Mit den verfügbaren Daten (zusätzliche Attribute, etc.) ist keine länderspezifische Suche möglich. Das versuchte Matching über eine weitere alternative eIDAS-Anmeldung war also nicht erfolgreich. Der Prozess setzt daher im schon bekannten Schritt 10) fort, in dem die Benutzer:in erneut gefragt wird, ob eine weitere eIDAS-Anmeldung möglich ist. Hier ergibt sich also eine Schleife, die erst durchbrochen wird, wenn die

Benutzer:in in Schritt 10) angibt, dass keine weitere Möglichkeit einer alterativen eIDAS-Anmeldung besteht.

13) In diesem Schritt wird eine länderspezifische Detailsuche mit den erhaltenen Daten aus der weiteren eIDAS-Anmeldung durchgeführt. Dieser Prozessschritt ähnelt also Schritt 6), nur dass dieser aktuelle Schritt 13) auf den Daten aus der erneuten (und nicht der ursprünglichen) eIDAS-Anmeldung operiert. In Bezug auf das Resultat der durchgeführten länderspezifischen Register-Suche können drei Fälle unterschieden werden:

    a) **1 Treffer:** Dies ist der Idealfall. Unter Verwendung der verfügbaren Informationen und Daten aus der erneuten eIDAS-Anmeldung konnte in den Registern ein einzelner Eintrag gefunden werden. Es kann davon ausgegangen werden, dass dieser Eintrag der aktuellen Benutzer:in zugeordnet werden kann (erfolgreiches Matching). Um bei künftigen Anmeldungen ein erfolgreiches Matching direkt über den PersonIdentifier der Benutzer:in zu erreichen, wird ein automatischer Kitt-Prozess initiiert, in dem die Daten aus der aktuellen eIDAS-Anmeldung und die Daten aus der ursprünglichen eIDAS-Anmeldung der Benutzer:in in den gefundenen Register-Eintrag integriert werden. Der Prozess setzt fort in Schritt 7)b).

    b) **0 Treffer:** Die länderspezifische Register-Suche war nicht erfolgreich und es konnte kein passender Eintrag gefunden werden. Das versuchte Matching über eine weitere alternative eIDAS-Anmeldung war also nicht erfolgreich. Der Prozess setzt daher im schon bekannten Schritt 10) fort, in dem die Benutzer:in erneut gefragt wird, ob eine weitere eIDAS-Anmeldung möglich ist. Hier ergibt sich also eine Schleife, die erst durchbrochen wird, wenn die Benutzer:in in Schritt 10) angibt, dass keine weitere Möglichkeit einer alterativen eIDAS-Anmeldung besteht.

    c) **Mehr als ein Treffer:** Dieser Fall sollte nicht eintreten, da die länderspezifische Suche so umgesetzt sein muss, dass diese Suche eindeutige Ergebnisse liefert, sofern in den Registern zu einer Person keine doppelten Einträge existieren. Retournieren die Register als Ergebnis auf die länderspezifische Suchabfrage trotzdem mehr als einen Eintrag, ist davon auszugehen, dass bereits in den Registern mehrere Einträge zur Person bestehen. Hier ist daher ein manueller Kitt-Prozess notwendig. Der Matching-Prozess bricht an dieser Stelle mit einem Fehler ab.

14) Dieser Schritt wird durchgeführt, wenn die Benutzer:in in Schritt 10) über das GUI des MS-Connector angibt, dass sie nicht in der Lage ist, eine weitere eIDAS-Anmeldung (mit anderer eID oder anderem Attribut-Set) durchzuführen. In diesem Fall wird die Benutzer:in in diesem Schritt 14 über das GUI gefragt, ob sie über eine Handy-Signatur verfügt und mit dieser einen Anmeldeprozess durchführen kann. Basierend auf dem Input der Benutzer:in ergeben sich zwei Möglichkeiten zum weiteren Vorgehen:

    a) **Anmeldung mit Handy-Signatur möglich:** Die Benutzer:in kann eine Anmeldung via Handy-Signatur durchführen. In diesem Fall setzt der Prozess in Schritt 15) mit der Durchführung einer Handy-Signatur-Anmeldung fort.

b) **Anmeldung mit Handy-Signatur nicht möglich:** Die Benutzer:in sieht keine Möglichkeit der Durchführung einer Handy-Signatur-Anmeldung. In diesem Fall setzt der Prozess in Schritt 16) fort, in dem über das GUI weitere Möglichkeiten der Konkretisierung von Suchabfragen in Registern eruiert werden.

15) In diesem Schritt initiiert der MS-Connector eine Handy-Signatur-Anmeldung der Benutzer:in. Über die Handy-Signatur-Anmeldung bezieht der MS-Connector das bPK-ZP der Benutzer:in. Der MS-Connector fragt mit dem bPK-ZP der Benutzer:in die Register nach einem Eintrag der Benutzer:in ab. In Bezug auf das Resultat der durchgeführten Register-Suche können drei Fälle unterschieden werden:

   a) **0 Treffer:** Mit dem bPK-ZP der Benutzer:in wurde kein Register-Eintrag gefunden. Das Matching über eine Handy-Signatur-Anmeldung schlug fehl. Es müssen daher weitere Möglichkeiten des Matchings versucht werden. Der Matching-Prozess setzt dazu in Schritt 16) fort. *Hinweis: Dieser Fall sollte nicht eintreten, da die Benutzer:in nur dann eine Handy-Signatur haben kann, wenn sie auch eine Stammzahl und damit einen entsprechenden Registereintrag hat. Der Fall wird hier trotzdem der Vollständigkeit halber betrachtet, bzw. deckt auch Fehlerfälle ab, in denen die Handy-Signatur-Anmeldung nicht erfolgreich durchgeführt werden kann (z.B., weil die Benutzer:in ihr Signaturpasswort vergessen hat).*

   b) **1 Treffer:** Mit dem bPK-ZP der Benutzer:in wurde genau ein Register-Eintrag gefunden. Da das bPK-ZP unique ist, kann davon ausgegangen werden, dass dieser Eintrag der Benutzer:in zuzuordnen ist. Um bei künftigen Anmeldungen ein erfolgreiches Matching direkt über den PersonIdentifier der Benutzer:in zu erreichen, wird ein automatischer Kitt-Prozess initiiert, in dem die Daten aus der aktuellen eIDAS-Anmeldung der Benutzer:in in den gefundenen Register-Eintrag integriert werden (sofern rechtlich möglich). Der Prozess setzt fort in Schritt 7)a).

   c) **Mehr als 1 Treffer:** Dieser Fall sollte nicht eintreten, da das bPK-ZP unique ist, sodass die Suche über das bPK-ZP eindeutige Ergebnisse liefern muss, sofern in den Registern zu einer Person keine doppelten Einträge existieren. Retournieren die Register als Ergebnis auf die Suchabfrage mit dem bPK-ZP trotzdem mehr als einen Eintrag, ist davon auszugehen, dass bereits in den Registern fälschlicherweise mehrere Einträge zur Person bestehen. Hier ist daher ein manueller Kitt-Prozess notwendig. Der Matching-Prozess bricht an dieser Stelle mit einem Fehler ab.

16) Dieser Schritt wird aufgerufen, wenn weder über eine weitere (alternative) eIDAS-Anmeldung noch über eine Handy-Signatur-Anmeldung ein erfolgreiches Matching erreicht werden konnte. In diesem Fall wird in diesem Schritt die Benutzer:in gefragt, ob sie über einen aktuellen oder ehemaligen Wohnsitz in Österreich verfügt. Ist dies der Fall, kann davon ausgegangen werden, dass ein entsprechender Register-Eintrag besteht. In diesem Schritt kann die Benutzer:in über das GUI des MS-Connector angeben, ob ein solcher Wohnsitz existiert. Basierend auf dem Input der Benutzer:in ergeben sich zwei Möglichkeiten zum weiteren Vorgehen:

a) **Wohnsitz vorhanden:** Die Benutzer:in verfügt über einen aktuellen oder ehemaligen Wohnsitz in Österreich. In diesem Fall setzt der Prozess in Schritt 17) fort, in dem die Benutzer:in Details zu ihrem Wohnsitz über das GUI angibt.

b) **Wohnsitz nicht vorhanden:** Die Benutzer:in verfügt über keinen aktuellen oder ehemaligen Wohnsitz in Österreich. Ein Matching über einen Wohnsitz ist damit nicht möglich. Es wurden damit alle Möglichkeiten ein Matching zu finden ausgeschöpft. Es kann daher davon ausgegangen werden, dass die Benutzer:in in den Registern noch nicht vorhanden ist. Der Prozess setzt daher in Schritt 9) fort, in dem basierend auf den Daten aus der ursprünglichen eIDAS-Anmeldung ein neuer Eintrag im ERnP erstellt wird.

17) Dieser Schritt wird durchgeführt, wenn die Benutzer:in zuvor in Schritt 16) angegeben hat, über einen aktuellen oder ehemaligen Wohnsitz in Österreich zu verfügen. In diesem Fall werden in diesem Schritt über das GUI weitere Informationen (Meldedaten) zu diesem Wohnsitz von der Benutzer:in abgefragt[1,2]. Der Matching-Prozess setzt fort in Schritt 18).

18) In diesem Schritt werden die in Schritt 17 von der Benutzer:in abgefragten Meldedaten für eine Register-Suche verwendet. In Bezug auf das Resultat der durchgeführten Register-Suche können drei Fälle unterschieden werden:

a) **0 Treffer:** Mit den angegebenen Meldedaten konnte kein Register-Eintrag gefunden werden. Das Matching über Meldedaten der Benutzer:in schlug fehl. Es wurden damit alle Möglichkeiten ein Matching zu finden ausgeschöpft. Es kann daher davon ausgegangen werden, dass der Benutzer in den Registern noch nicht vorhanden ist. Der Prozess setzt daher in Schritt 9) fort, in dem basierend auf den Daten aus der ursprünglichen eIDAS-Anmeldung ein neuer Eintrag im ERnP erstellt wird.

b) **1 Treffer:** Mit den Meldedaten der Benutzer:in wurde genau ein Register-Eintrag gefunden. Um zu verifizieren, dass der gefundene Eintrag tatsächlich der aktuellen Benutzer:in zuzuordnen ist, muss ein Abgleich der erhaltenen Daten aus dem Register-Eintrag mit den Daten aus der eIDAS-Anmeldung erfolgen. Der Prozess setzt daher in Schritt 19) fort.

c) **Mehr als 1 Treffer:** Werden auf die Suchanfrage mit den angegebenen Meldedaten mehr als ein Treffer retourniert, liegt in den Registern potenziell ein mehrfacher Eintrag der Benutzer:in vor. In diesem Fall ist ein manueller Kitt-Prozess notwendig. Möglich ist auch, dass mehrere Treffer aufgrund von Datenzwillingen in den Registern retourniert werden, da die Suchabfrage keine

[1] Laut Abstimmung mit dem BM.I am 27.05.2021 reicht die Abfrage von Gemeinde, Straße und Hausnummer. Stimmen diese Daten (und das MDS der Benutzer:in) überein, kann von einem erfolgreichen Matching ausgegangen werden.

[2] Bei der Umsetzung des GUI wurde darauf geachtet, dass die Möglichkeiten für versehentliche Fehleingaben durch die Benutzer:in (z.B. untersch. Schreibweise des Straßennamens) minimiert werden. Dazu wurde auf eine bestehende Lösung des BM.I zurückgegriffen, über die Benutzer:innen über das GUI basierend auf den bisherigen Eingaben (z.B. Gemeinde) eine Vorauswahl weiterer möglicher Eingaben präsentiert bekommen. Die dafür nötigen Schnittstelle wurde vom BM.I bereitgestellt.

eindeutige ID beinhaltet. Bei Retournierung von mehr als einem Treffer bricht der Matching-Prozess in jedem Fall an dieser Stelle mit einem Fehler ab.

19) In diesem Schritt wird der erhaltene Treffer aus der Register-Suche über eingegebene Meldedaten mit den bereits vorhandenen Daten aus der eIDAS-Anmeldung verglichen. Für ein erfolgreiches Matching müssen diese Daten übereinstimmen. Als Resultat des durchgeführten Vergleichs ergeben sich folgende beide Varianten:

    a) **Datenvergleich erfolgreich:** Im Erfolgsfall wird – um bei künftigen Anmeldungen ein erfolgreiches Matching direkt über den PersonIdentifier der Benutzer:in zu erreichen – ein automatischer Kitt-Prozess initiiert werden, in dem die Daten aus der aktuellen eIDAS-Anmeldung der Benutzer:in in den gefundenen Register-Eintrag integriert werden (sofern rechtlich möglich). Der Prozess setzt fort in Schritt 7)a).

    b) **Datenvergleich nicht erfolgreich:** Stimmen die Daten aus dem gefundenen Register-Eintrag und der eIDAS-Anmeldung nicht überein, kann nicht von einem erfolgreichen Matching ausgegangen werden. Der Matching-Versuch schlug fehl. Es wurden damit alle Möglichkeiten ein Matching zu finden ausgeschöpft. Es kann daher davon ausgegangen werden, dass der Benutzer in den Registern noch nicht vorhanden ist. Der Prozess setzt daher in Schritt 9) fort, in dem basierend auf den Daten aus der ursprünglichen eIDAS-Anmeldung ein neuer Eintrag im ERnP erstellt wird.

3.3. Abdeckung relevanter Use-Cases

Das umgesetzte und in diesem Dokument beschriebene Matching-Konzept muss mit einer Vielzahl an Use-Cases umgehen können. Zum Beispiel muss es in der Lage sein, eine neue Benutzer:in (die noch keinen Register-Eintrag hat) als solche zu identifizieren oder auch eine schon in den Registern eingetragene Benutzer:in wiederzufinden, obwohl sich Teile des MDS der Benutzer:in geändert haben.

Die unterschiedlichen zu berücksichtigenden Use-Cases ergeben sich aus der Kombination der folgenden Parameter:

1) **PersonIdentifier (PI) aus aktueller eIDAS-Anmeldung:** Im Idealfall ist der PI aus der eIDAS-Anmeldung persistent, d.h., aus jeder eIDAS-Anmeldung der Benutzer:in resultiert derselbe PI. Es kann aber auch der Fall eintreten, dass sich der PI im Vergleich zur letzten eIDAS-Anmeldung geändert hat und der PI aus der aktuellen eIDAS-Anmeldung damit nicht dem PI entspricht, der im Register-Eintrag der Benutzer:in hinterlegt ist.

2) **MDS aus aktueller eIDAS-Anmeldung:** Im Idealfall ist das MDS aus der eIDAS-Anmeldung persistent, d.h., aus jeder eIDAS-Anmeldung der Benutzer:in resultiert dasselbe MDS. Es kann aber auch der Fall eintreten, dass sich das MDS im Vergleich zur letzten eIDAS-Anmeldung geändert hat (z.B. Namensänderung durch Eheschließung) und das MDS aus der aktuellen eIDAS-Anmeldung damit nicht dem MDS entspricht, welches im Register-Eintrag der Benutzer:in hinterlegt ist.

3) **Register-Eintrag für Benutzer:in:** Die Benutzer:in kann in den Registern entweder bereits eingetragen sein (aufgrund einer vorherigen eIDAS-Anmeldung, aufgrund eines

Wohnsitzes in Österreich, etc.), oder aber in den Registern noch unbekannt sein. Hinweis: Auch wenn ein Register-Eintrag für die Benutzer:in bereits vorhanden ist, müssen nicht zwangsweise die Daten des Eintrags mit den Daten aus der aktuellen eIDAS-Anmeldung übereinstimmen.

4) **Bestehender SZR-Eintrag im Register über PI auffindbar:** Aufgrund der Tatsache, dass der PI nicht notwendigerweise persistent ist, kann sich der PI im bestehenden Register-Eintrag der Benutzer:in von jenem aus der aktuellen eIDAS-Anmeldung unterscheiden. In dem Fall ist der Register-Eintrag über den PI nicht auffindbar. Eine Register-Suche über den PI ist natürlich auch dann nicht erfolgreich, wenn für die Benutzer:in noch kein Register-Eintrag existiert.

5) **MDS der Benutzer:in im Register auffindbar:** Das aus der eIDAS-Anmeldung erhaltene MDS der Benutzer:in ist nicht notwendigerweise in den Registern auffindbar, unabhängig davon, ob ein Register-Eintrag der Benutzer:in existiert. Das MDS ist beispielsweise potenziell nicht auffindbar, wenn kein Register-Eintrag der Benutzer:in existiert, oder sich das MDS der Benutzer:in in der Zwischenzeit geändert hat. Hingegen kann das MDS auffindbar sein, wenn sich das MDS einer in den Registern bereits eingetragenen Benutzer:in nicht geändert hat, oder aber ein Register-Eintrag einer anderen Benutzer:in das gleiche MDS aufweist (MDS ist nicht notwendigerweise unique).

Durch Kombination all dieser Faktoren können alle prinzipiell denkbaren Use-Cases systematisch identifiziert und betrachtet werden. Dies ist in folgender Tabelle dargestellt. Durch Variation der fünf Parameter, von denen jeder zwei Werte (Ja, Nein) annehmen kann, ergeben sich insgesamt $2^5 = 32$ mögliche Use-Cases. Nicht alle theoretisch möglichen Kombinationen machen in der Realität auch Sinn. In der Tabelle sind daher über eine grüne Hintergrundfarbe jene Use-Cases markiert, die in der Praxis tatsächlich betrachtet werden müssen. Für alle anderen Use-Cases ist kurz angeführt, warum diese in der Praxis keine Rolle spielen. Für relevante Use-Cases ist auch deren vorgesehener Prozessfluss angegeben. Die Zahlen beziehen sich auf die Prozessschritte, die in Abschnitt 2.2 beschrieben sind.

	1	**2**	**3**	**4**	**5**		
Use-Case	**eIDAS-Anmeldung mit geändertem PI**	**eIDAS-Anmeldung mit geändertem MDS**	**Person hat bereits einen Register-Eintrag (ZMR oder ERnP)**	**Register-Eintrag via PI aus aktueller eIDAS-Anmeldung auffindbar**	**MDS aus aktueller eIDAS-Anmeldung im Register vorhanden**	**Beschreibung**	**Prozessfluss**
1	N	N	N	N	N	Erstanmeldung des Benutzers mit eID (und auch nicht aus Wohnsitz bekannt), kein MDS-Zwilling in Registern vorhanden	1-2-5-(6)-8-9
2	N	N	N	N	J	Erstanmeldung des Benutzers mit eID (und auch nicht aus Wohnsitz bekannt), allerdings MDS-Zwilling bereits in Registern vorhanden	1-2-5-(6)-8-10-14-16-9 (Annahme: Kein GUI-Matching möglich)
3	N	N	N	J	N	Fall darf nicht vorkommen unter der Annahme, dass PI	

						unique ist. Wenn PI auffindbar (4), muss zuvor schon eID-Anmeldung passiert sein. Dann muss aber auch Person in Registern eingetragen sein (3)	
4	N	N	N	J	J	Fall darf nicht vorkommen unter der Annahme, dass PI unique ist. Wenn PI auffindbar (4), muss zuvor schon eID-Anmeldung passiert sein. Dann muss aber auch Person in Registern eingetragen sein (3)	
5	N	N	J	N	N	Fall darf nicht vorkommen: Wenn Person im Register (3) ist und keine Anmeldung mit neuem MDS erfolgt (2), muss Person mit MDS im Register auffindbar sein (5)	
6	N	N	J	N	J	Erstanmeldung des Benutzers mit eID (sonst wäre PI via Register auffindbar (4), da ja keine Anmeldung mit geändertem PI (1)). Register-Eintrag aber (z.B. wegen Wohnsitz) vorhanden (3). Dadurch Eintrag auch via MDS auffindbar (5), da keine Anmeldung mit geändertem MDS (2)	1-2-5-(6)-8-10-14-16-17-18-19-7a (Annahme: GUI-Matching via Meldedaten möglich und erfolgreich; Alternative wäre auch GUI-Matching via HS)
7	N	N	J	J	N	Fall darf nicht vorkommen: Wenn Person im Register (3) ist und keine Anmeldung mit neuem MDS erfolgt (2), muss Person mit MDS im Register auffindbar sein (5)	
8	N	N	J	J	J	Wiederanmeldung mit bereits bekannter (und im Register eingetragener) eID	1-2-3
9	N	J	N	N	N	Fall macht so keinen Sinn: Offensichtlich erste Anmeldung, da User im Register nicht bekannt (3), dann kann aber keine Anmeldung mit geändertem MDS (2) erfolgen (geändert in Bezug auf was?)	
10	N	J	N	N	J	Fall macht so keinen Sinn: Offensichtlich erste Anmeldung, da User im Register nicht bekannt (3), dann kann aber keine Anmeldung mit geändertem MDS (2) erfolgen (geändert in Bezug auf was?)	
11	N	J	N	J	N	Fall macht so keinen Sinn: Offensichtlich erste	

						Anmeldung, da User im Register nicht bekannt (3), dann kann aber PI nicht auffindbar sein im Register (4), wenn PI unique ist. Außerdem kann dann keine Anmeldung mit geändertem MDS (2) erfolgen.	
12	N	J	N	J	J	Fall macht so keinen Sinn: Offensichtlich erste Anmeldung, da User im Register nicht bekannt (3), dann kann aber keine Anmeldung mit geändertem MDS (2) erfolgen (geändert in Bezug auf was?)	
13	N	J	J	N	N	Person im Register (z.B. wegen Wohnsitz) aber nicht wegen vorheriger eID-Anmeldung. Sonst würde PI im Register gefunden werden (hat sich ja nicht geändert (1)). Anmeldung aber mit geändertem MDS (2), daher MDS auch nicht auffindbar (gibt also auch keinen MDS-Zwilling mit neuem MDS).	1-2-5-(6)-8-9 ACHTUNG!! Das aktuelle Konzept geht hier fälschlicherweise von einem neuen Benutzer aus und findet den bestehenden Eintrag nicht!
14	N	J	J	N	J	Person im Register (z.B. wegen Wohnsitz) aber nicht wegen vorheriger eID-Anmeldung. Sonst würde PI im Register gefunden werden (hat sich ja nicht geändert (1)). Anmeldung aber mit geändertem MDS (2), trotzdem MDS aber auffindbar (gibt also einen MDS-Zwilling mit „neuem“ MDS).	1-2-5-(6)-8-10-14-16-17-18-19-7a (Annahme: GUI-Matching via Meldedaten möglich und erfolgreich; Alternative wäre auch GUI-Matching via HS) Hinweis: Prozess funktioniert nur zufällig wegen MDS-Zwillings
15	N	J	J	J	N	Person im Register wegen früherer eID-Anmeldung (PI auffindbar (4)), User kommt aber mit neuem MDS, daher MDS auch nicht in Register auffindbar (es existiert auch kein MDS-Zwilling).	1-2-3-4
16	N	J	J	J	J	Person im Register wegen früherer eID-Anmeldung (PI auffindbar (4)), User kommt mit neuem MDS, MDS aber trotzdem in Register auffindbar (es existiert also offensichtlich ein MDS-Zwilling).	1-2-3-4
17	J	N	N	N	N	Fall macht keinen Sinn: Wenn Person nicht im Register ist (3), kann sie	

						auch nicht mit geändertem PI kommen (1).	
18	J	N	N	N	J	Fall macht keinen Sinn: Wenn Person nicht im Register ist (3), kann sie auch nicht mit geändertem PI kommen (1).	
19	J	N	N	J	N	Fall macht keinen Sinn: Wenn Person nicht im Register ist (3), kann sie auch nicht mit geändertem PI kommen (1).	
20	J	N	N	J	J	Fall macht keinen Sinn: Wenn Person nicht im Register ist (3), kann sie auch nicht mit geändertem PI kommen (1).	
21	J	N	J	N	N	Fall so nicht möglich: Benutzer ist bekannt im Register entweder wegen ehem. Wohnsitz oder wegen vorheriger eID-Anmeldung (PI zwar nicht auffindbar (4), ist aber auch geändert (1)). Allerdings kommt Benutzer mit unverändertem MDS (2) und ist trotzdem nicht auffindbar via MDS (5) (Widerspruch).	
22	J	N	J	N	J	Benutzer ist bekannt im Register entweder wegen ehem. Wohnsitz oder wegen vorheriger eID-Anmeldung (PI zwar nicht auffindbar (4), ist aber auch geändert (1)). Benutzer kommt mit unverändertem MDS (2) und MDS wird auch gefunden im Register (5).	1-2-5-(6)-8 -> GUI-Matching Hinweis: Klassischer Fall für länderspez. Matching über Attribute
23	J	N	J	J	N	Fall nicht möglich. Wenn PI geändert ist (1), darf PI nicht im Register auffindbar sein (4), sofern PI unique ist.	
24	J	N	J	J	J	Fall nicht möglich. Wenn PI geändert ist (1), darf PI nicht im Register auffindbar sein (4), sofern PI unique ist.	
25	J	J	N	N	N	Fall macht so keinen Sinn. Wenn Benutzer noch nicht im Register angelegt ist (3), kann er auch nicht mit geändertem PI kommen (1).	
26	J	J	N	N	J	Fall macht so keinen Sinn. Wenn Benutzer noch nicht im Register angelegt ist, kann er auch nicht mit geändertem PI kommen.	
27	J	J	N	J	N	Fall nicht möglich. Wenn PI	

						geändert ist (1), darf PI nicht im Register auffindbar sein (4), sofern PI unique ist.	
28	J	J	N	J	J	Fall nicht möglich. Wenn PI geändert ist (1), darf PI nicht im Register auffindbar sein (4), sofern PI unique ist.	
29	J	J	J	N	N	Benutzer ist im Register angelegt (3), kommt aber mit neuem PI (1) und neuem MDS (2) und ist daher weder über PI (4) noch über MDS (5) auffindbar.	1-2-5-(6)-8-9 Hinweis: Matching nicht erfolgreich -> Muss über länderspez. Suche abgefangen werden. Diese ist aber nur erfolgreich, wenn zusätzliche Attribute (ohne des PI/MDS) Eindeutigkeit garantieren (z.B. Steuernummer bei IT-User)
30	J	J	J	N	J	Benutzer ist im Register angelegt (3), kommt aber mit neuem PI (1) und neuem MDS (2) und ist daher weder über PI (4) noch über MDS (5) auffindbar. Allerdings existiert offensichtlich ein MDS-Zwilling, dessen MDS im Register gefunden wird.	1-2-5-(6)-8 -> GUI-Matching Hinweis: Klassischer Fall für länderspez. Matching über Attribute; man kommt nur wegen Datenzwilling ins GUI-Matching
31	J	J	J	J	N	Fall nicht möglich. Wenn PI geändert ist (1), darf PI nicht im Register auffindbar sein (4), sofern PI unique ist.	
32	J	J	J	J	J	Fall nicht möglich. Wenn PI geändert ist (1), darf PI nicht im Register auffindbar sein (4), sofern PI unique ist.	

Aus obenstehender Tabelle ist ersichtlich, dass sich insgesamt 11 relevante Use-Cases ergeben, die vom hier beschriebenen Matching-Konzept und der darauf basierenden Implementierung abgedeckt werden müssen.

Der Umstand, ob ein gegebener Use-Case vom Matching-Konzept ausreichend abgedeckt ist (d.h., ob ein erfolgreiches Matching für diesen Use-Case möglich ist) hängt in einigen Fällen auch davon ab, ob eine länderspezifische Suche in den Registern durchgeführt werden kann. Dies wiederum hängt vom Heimatland der Benutzer:in und den von diesem Land zur Verfügung gestellten Attributen (bzw. auch vom Verhalten der Benutzer:in, die die Auslieferung von Attributen unterdrücken kann) ab.

Für eine vollständige Betrachtung werden in folgender Tabelle nochmal die 11 relevanten Use-Cases dargestellt. Für jeden Use-Case werden jedoch zwei unterschiedliche Varianten betrachtet. So wird jeder Use-Case einmal mit und einmal ohne die Möglichkeit einer länderspezifischen Suche betrachtet.

	1	2	3	4	5	6		
Use-Case	**eIDAS-Anmeldung mit geändertem PI**	**eIDAS-Anmeldung mit geändertem MDS**	**Person hat bereits einen Register-Eintrag (ZMR oder ERnP)**	**Register-Eintrag via PI aus aktueller eIDAS-Anmeldung auffindbar**	**MDS aus aktueller eIDAS-Anmeldung im Register vorhanden**	**Länder-spezifische Suche für gegebenes Land möglich**	**Beschreibung**	**Prozessfluss**
1-1	N	N	N	N	N	**N**	Erstanmeldung des Benutzers mit eID (und auch nicht aus Wohnsitz bekannt), kein MDS-Zwilling in Register vorhanden	1-2-5-8-9
1-2	N	N	N	N	N	**J**	Erstanmeldung des Benutzers mit eID (und auch nicht aus Wohnsitz bekannt), kein MDS-Zwilling in Register vorhanden	1-2-5-6-8-9
2-1	N	N	N	N	J	**N**	Erstanmeldung des Benutzers mit eID (und auch nicht aus Wohnsitz bekannt), allerdings MDS-Zwilling bereits in Register vorhanden	1-2-5-8-10-14-16-9 (Annahme: User macht keine GUI-Matching-Schritte – erfolgreiches Matching wäre sowieso nicht möglich)
2-2	N	N	N	N	J	**J**	Erstanmeldung des Benutzers mit eID (und auch nicht aus Wohnsitz bekannt), allerdings MDS-Zwilling bereits in Register vorhanden	1-2-5-6-8-10-14-16-9 (Annahme: User macht kein GUI-Matching-Schritte – erfolgreiches Matching wäre sowieso nicht möglich)
6-1	N	N	J	N	J	**N**	Erstanmeldung des Benutzers mit eID (sonst wäre PI via Register auffindbar (4), da ja keine Anmeldung mit geändertem PI (1)). Dadurch wäre auch kein Matching über länderspez. Suche möglich (in diesem Use-Case ohnehin nicht möglich). Register -Eintrag	1-2-5-8-10-14-16-17-18-19-7a (Annahme: GUI-Matching via Meldedaten möglich und erfolgreich; Alternative wäre auch GUI-Matching via HS)

							aber (z.B. wegen Wohnsitz) vorhanden (3). Dadurch Eintrag auch via MDS auffindbar (5), da keine Anmeldung mit geändertem MDS (2)	
6-2	N	N	J	N	J	**J**	Erstanmeldung des Benutzers mit eID (sonst wäre PI via Register auffindbar (4), da ja keine Anmeldung mit geändertem PI (1)). Dadurch auch kein Matching über länderspez. Suche möglich. Register -Eintrag aber (z.B. wegen Wohnsitz) vorhanden (3). Dadurch Eintrag auch via MDS auffindbar (5), da keine Anmeldung mit geändertem MDS (2)	1-2-5-6-8-10-14-16-17-18-19-7a (Annahme: GUI-Matching via Meldedaten möglich und erfolgreich; Alternative wäre auch GUI-Matching via HS)
8-1	N	N	J	J	J	**N**	Wiederanmeldung mit bereits bekannter (und im Register eingetragener) eID	1-2-3
8-2	N	N	J	J	J	**J**	Wiederanmeldung mit bereits bekannter (und im Register eingetragener) eID	1-2-3
13-1	N	J	J	N	N	**N**	Person im Register (z.B. wegen Wohnsitz) aber nicht wegen vorheriger eID-Anmeldung. Sonst würde PI im Register gefunden werden (hat sich ja nicht geändert (1)). Anmeldung aber mit geändertem MDS im Vergleich zu Register -Eintrag (2), daher MDS auch nicht auffindbar (gibt also auch keinen MDS-Zwilling mit neuem MDS).	1-2-5-8-9 Hinweis: Das aktuelle Konzept geht hier fälschlicherweise von einem neuen Benutzer aus und findet den bestehenden Eintrag nicht!
13-2	N	J	J	N	N	**J**	Person im Register (z.B. wegen Wohnsitz) aber nicht wegen vorheriger eID-	1-2-5-6-8-9 Hinweis: Das aktuelle Konzept geht hier

							Anmeldung. Sonst würde PI im Register gefunden werden (hat sich ja nicht geändert (1)). Anmeldung aber mit geändertem MDS (2), daher MDS auch nicht auffindbar (gibt also auch keinen MDS-Zwilling mit neuem MDS). Länderspezifische Suche wird zwar durchgeführt, führt wegen geändertem MDS aber auch nicht zum Erfolg.	fälschlicherweise von einem neuen Benutzer aus und findet den bestehenden Eintrag nicht!
14-1	N	J	J	N	J	**N**	Person im Register (z.B. wegen Wohnsitz) aber nicht wegen vorheriger eID-Anmeldung. Sonst würde PI im Register gefunden werden (hat sich ja nicht geändert (1)). Anmeldung aber mit geändertem MDS (2), trotzdem MDS aber auffindbar (gibt also einen MDS-Zwilling mit „neuem“ MDS).	1-2-5-8-10-14-16-17-18-19-7a (Annahme: GUI-Matching via Meldedaten möglich und erfolgreich; Alternative wäre auch GUI-Matching via HS) Hinweis: Prozess funktioniert nur zufällig wegen zufälligem MDS-Zwilling (wäre sonst gleiches Resultat wie Use-Case 13-1)
14-2	N	J	J	N	J	**J**	Person im Register (z.B. wegen Wohnsitz) aber nicht wegen vorheriger eID-Anmeldung. Sonst würde PI im Register gefunden werden (hat sich ja nicht geändert (1)). Anmeldung aber mit geändertem MDS (2), trotzdem MDS aber auffindbar (gibt also einen MDS-Zwilling mit „neuem“ MDS). Länderspezifische Suche funktioniert nicht wegen geändertem MDS.	1-2-5-6-8-10-14-16-17-18-19-7a (Annahme: GUI-Matching via Meldedaten möglich und erfolgreich; Alternative wäre auch GUI-Matching via HS) Hinweis: Prozess funktioniert nur zufällig wegen zufälligem MDS-Zwilling (wäre sonst gleiches Resultat wie Use-Case 13-2)
15-1	N	J	J	J	N	**N**	Person im Register wegen früherer eID-Anmeldung (PI auffindbar (4)), User kommt aber	1-2-3-4

							mit neuem MDS, daher MDS auch nicht in Register auffindbar (es existiert auch kein MDS-Zwilling).	
15-2	N	J	J	J	N	**J**	Person im Register wegen früherer eID-Anmeldung (PI auffindbar (4)), User kommt aber mit neuem MDS, daher MDS auch nicht in Register auffindbar (es existiert auch kein MDS-Zwilling).	1-2-3-4
16-1	N	J	J	J	J	**N**	Person im Register wegen früherer eID-Anmeldung (PI auffindbar (4)), User kommt mit neuem MDS, MDS aber trotzdem in Register auffindbar (es existiert also offensichtlich ein MDS-Zwilling).	1-2-3-4
16-2	N	J	J	J	J	**J**	Person im Register wegen früherer eID-Anmeldung (PI auffindbar (4)), User kommt mit neuem MDS, MDS aber trotzdem in Register auffindbar (es existiert also offensichtlich ein MDS-Zwilling).	1-2-3-4
22-1	J	N	J	N	J	**N**	Benutzer ist bekannt im Register entweder wegen ehem. Wohnsitz oder wegen vorheriger eID-Anmeldung (PI zwar nicht auffindbar (4), ist aber auch geändert (1)). Benutzer kommt mit unverändertem MDS (2) und MDS wird auch gefunden im Register (5).	1-2-5-8 -> GUI-Matching (falls möglich), da länderspezifische Suche nicht möglich
22-2	J	N	J	N	J	**J**	Benutzer ist bekannt im Register entweder wegen ehem. Wohnsitz oder wegen vorheriger eID-Anmeldung (PI zwar nicht	1-2-5-6-7

							auffindbar (4), ist aber auch geändert (1)). Benutzer kommt mit unverändertem MDS (2) und MDS wird auch gefunden im Register (5).	
29-1	J	J	J	N	N	**N**	Benutzer ist im Register angelegt (3), kommt aber mit neuem PI (1) und neuem MDS (2) und ist daher weder über PI (4) noch über MDS (5) auffindbar.	1-2-5-8-9 Achtung: Matching nicht erfolgreich – Benutzer wird neu angelegt.
29-2	J	J	J	N	N	**J**	Benutzer ist im Register angelegt (3), kommt aber mit neuem PI (1) und neuem MDS (2) und ist daher weder über PI (4) noch über MDS (5) auffindbar.	1-2-5-6-7 Annahme: Länderspezifisches Matching erfolgreich trotz neuem MDS und PI – nur möglich, wenn zusätzliche Attribute (ohne PI/MDS) Eindeutigkeit garantieren (z.B. Steuernummer). Achtung: Wenn länderspezifisches Matching nicht erfolgreich: Neuer Benutzer wird angelegt (weil MDS nicht gefunden wird).
30-1	J	J	J	N	J	**N**	Benutzer ist im Register angelegt (3), kommt aber mit neuem PI (1) und neuem MDS (2) und ist daher weder über PI (4) noch über MDS (5) auffindbar. Allerdings existiert offensichtlich ein MDS-Zwilling, dessen MDS im Register gefunden wird.	1-2-5-8 -> GUI-Matching Hinweis: Benutzer kommt nur wegen zufälligem Datenzwilling ins GUI-Matching
30-2	J	J	J	N	J	**J**	Benutzer ist im Register angelegt (3), kommt aber mit neuem PI (1) und neuem MDS (2) und ist daher weder über PI (4) noch über MDS (5) auffindbar. Allerdings existiert	1-2-5-6-7 Annahme: Länderspezifisches Matching erfolgreich trotz neuem MDS und PI – – nur möglich, wenn zusätzliche

							offensichtlich ein MDS-Zwilling, dessen MDS im Register gefunden wird.	Attribute (ohne PI/MDS) Eindeutigkeit garantieren (z.B. Steuernummer). Achtung: Wenn länderspezifisches Matching nicht erfolgreich: GUI-Matching. (Ins GUI-Matching kommt man nur wegen zufälligem Datenzwilling)

Über die in obiger Tabelle durchgeführte detaillierte Betrachtung der relevanten Use-Cases inkl. Berücksichtigung einer eventuell möglichen länderspezifischen Suche in Registern über zusätzliche Attribute können folgende Limitierungen des hier beschriebenen Matching-Konzepts identifiziert werden:

- Das Matching schlägt fehl und es wird fälschlicherweise ein neuer Register-Eintrag angelegt, wenn:
  - Die Benutzer:in z.B. aufgrund eines Wohnsitzes in Österreich bereits in einem Register eingetragen ist; und
  - Der Register-Eintrag nicht über den PI aus der aktuellen eIDAS-Anmeldung auffindbar ist (z.B., weil eben Eintrag aufgrund von Wohnsitz und nicht wegen früherer eID-Anmeldung angelegt wurde); und
  - MDS aus aktueller eIDAS-Anmeldung nicht mit dem MDS im bestehenden SZR-Eintrag übereinstimmt (z.B. wegen Eheschließung).
- Das Matching schlägt fehl und es wird fälschlicherweise ein neuer Register-Eintrag angelegt, wenn:
  - Die Benutzer:in bereits in einem Register eingetragen ist; und
  - Der PI und das MDS aus der aktuellen eIDAS-Anmeldung sich von den Daten im bestehenden Register-Eintrag unterscheiden; und
  - Auch kein anderer Register-Eintrag mit dem MDS aus der aktuellen eIDAS-Anmeldung existiert (d.h. kein MDS-Zwilling im Register)[3].

Die durch das Matching-Konzept nicht ausreichend abgedeckten Use-Cases dürften in der Praxis eher selten auftreten. Trotzdem muss das Bewusstsein vorhanden sein, dass durch das Matching-Konzept und seine Umsetzung keine vollständige Abdeckung aller möglichen Szenarien und Use-Cases möglich ist.

Der Vollständigkeit halber sei hier auch noch der Umstand erwähnt, dass das Konzept nicht in der Lage ist, zuverlässig bereits existierende doppelte Register-Einträge zu erkennen. Existiert zum Beispiel bereits ein Eintrag zur Benutzer:in sowohl im ZMR als auch im ERnP, wird über das Konzept

[3] Ist ein MDS-Zwilling vorhanden, würde das weitere Matching-Versuche über die GUI verursachen, die möglicherweise zum Erfolg führen können.

im Zuge der Anmeldung eventuell trotzdem nur ein Eintrag gefunden (z.B. dann, wenn genau ein Eintrag über den PersonIdentifier aus der aktuellen Anmeldung auffindbar ist). Ziel des hier beschriebenen Matching-Konzepts ist es, die Entstehung neuer doppelter Einträge zu verhindern, es ist jedoch nicht in der Lage, bereits bestehende doppelte Einträge zuverlässig zu finden[4].

Die aktuelle Umsetzung des Matching-Konzepts wurde gegen die in obiger Tabelle angeführten relevanten Use-Cases getestet.

[4] Es wäre technisch sehr wohl möglich, das Konzept so anzupassen, dass auch bereits bestehende doppelte Einträge zuverlässig gefunden werden. Dies würde allerdings die Komplexität einer eIDAS-Anmeldung für alle Benutzer beträchtlich erhöhen. So müsste sichergestellt sein, dass alle Benutzer alle möglichen Matching-Varianten (Handy-Signatur-Anmeldung, Eingabe Meldedaten, etc.) vollständig durchlaufen, auch wenn zuvor bereits ein Eintrag zur Benutzer:in gefunden wurde. Nur so könnte ausgeschlossen werden, dass neben dem bereits gefundenen Eintrag nicht auch noch ein zweiter Eintrag existiert.

4. Register-Zugriffe

Das in diesem Dokument beschriebene Matching-Konzept sieht eine direkte Interaktion zwischen dem österreichischen eIDAS-Knoten (konkret dessen Komponente MS-Connector) und den Registern ZMR und ERnP im Zuge einer eIDAS-Anmeldung (z.B. Benutzer:in mit deutschem elektronischen Prsonalausweis meldet sich an FinanzOnline an) vor. Diese Interaktion mit den Registern muss aus den folgenden Gründen erfolgen:

- **Suchen von Einträgen:** Bestehende Register-Einträge der aktuellen Benutzer:in müssen in ZMR und ERnP gesucht werden, um zu verhindern, dass ein zusätzlicher (doppelter) Eintrag angelegt wird (Matching).
- **Erweitern bestehender Einträge:** Bestehende Register-Einträge müssen mit zusätzlichen Daten (Attribute) aus der aktuellen eIDAS-Anmeldung ergänzt werden, damit bei nachfolgenden Anmeldevorgängen eine erfolgreiche Suche auch über diese Daten möglich ist. Das ist notwendig, da nicht davon ausgegangen werden kann, dass eine erfolgreiche Suche immer über den PersonIdentifier aus der eIDAS-Anmeldung möglich ist.
- **Anlegen neuer Einträge:** Wird die aktuelle Benutzer:in in den Registern nicht gefunden, muss ein neuer Eintrag für die Benutzer:in unter Verwendung der Daten (Attribute) im ERnP angelegt werden.

4.1. Mapping von eIDAS-Attributen auf Datenfelder in Registern

Aus den oben skizzierten Interaktionsschritten (Suchen, Erweitern, Anlegen) stellte sich unmittelbar die zentrale Frage, wie eIDAS-Attribute in ZMR und/oder ERnP gespeichert werden sollen. Eine Herausforderung ergab sich dadurch, dass die bestehenden Register bisher keine expliziten Datenfelder für eIDAS-Attribute vorsahen.

Aus der eIDAS-Anmeldung stehen folgende Attribute zur Verfügung, die in irgendeiner Form in ZMR und/oder ERnP gespeichert werden müssen, sodass später danach gesucht werden kann:

- **PersonIdentifier:** Eindeutige ID der Benutzer:in mit einer maximalen Länge von 255 Zeichen. *Achtung: Der PersonIdentifier ist nicht notwendigerweise persistent, d.h. es kann nicht davon ausgegangen werden, dass bei wiederholten Anmeldungen derselben Benutzer:in immer derselbe PersonIdentifier geliefert wird. Es ist auch nicht auszuschließen, dass eine Benutzer:in mehrere eID-Token und damit mehrere PersonIdentifier hat.*
- **MDS:** Vorname, Familienname, Geburtsdatum der Benutzer:in. *Achtung: Es darf nicht davon ausgegangen werden, dass Vorname und Familienname über die Lebensdauer der Benutzer:in (und die ihres Registereintrags) unverändert bleiben.*
- **Optional: Zusätzliche länderspezifische Attribute:** Je nach Herkunftsland können aus der eIDAS-Anmeldung zusätzliche Attribute verfügbar sein (z.B. Geburtsname und Geburtsort bei deutschen Benutzer:innen). *Achtung: Es kann nicht davon ausgegangen werden, dass diese Attribute in jedem Anmeldevorgang zur Verfügung stehen, da die Benutzer:in die Auslieferung dieser Attribute unterbinden kann (gilt nicht für PersonIdentifier und MDS).*

Für die Speicherung dieser Daten (eIDAS-Attribute) gab es prinzipiell zwei Möglichkeiten:

- **Variante A: Speicherung in existierenden Datenfeldern:** Dies hätte den Vorteil gehabt, dass die Struktur der Register nicht angepasst hätte werden müssen. Wenn umsetzbar, wäre daher diese Variante zu präferieren gewesen.
- **Variante B: Erweiterung der Registerstruktur um explizite Felder für eIDAS-Attribute:** Dies ist generell die technisch sauberere Variante, ist aber mit mehr Aufwand auf Seiten der Register verbunden.

Eine im Rahmen der Konzepterstellung durchgeführte Machbarkeitsanalyse ergab, dass eine Speicherung beliebiger eIDAS-Attribute als Dokumente zu einer Person gemäß Variante A nicht durchführbar war. Die zugrundeliegende Datenstruktur unterstütze dieses Vorhaben nicht. Damit blieb nur Variante B, d.h. die Erweiterung der bestehenden Registerstruktur um explizite Felder zur Speicherung von Attributen aus eIDAS-Anmeldungen.

Im ZMR und ERnP wurde die Struktur eines Personeneintrags dementsprechend so erweitert, dass folgende Operationen möglich wurden:

- Speicherung einer beliebigen Anzahl an zusätzlichen eIDAS-Attributen in der Form *<Länder-Code, Attribut-Name, Attribut-Wert>* zu einem Register-Eintrag
- Suche nach Register-Einträgen über eine beliebige Anzahl von *<Länder-Code, Attribut-Name, Attribut-Wert>*

4.2. Notwendige Register-Zugriffe laut Matching-Konzept

Im Folgenden sind jene Prozessschritte des Matching-Konzepts gelistet, die eine Interaktion mit ERnP und ZMR vorsehen. Für jeden Prozessschritt sind Inhalte der Registeranfragen und erwartete Antworten skizziert.

4.2.1. Prozessschritt 2)

In diesem Prozessschritt wird der eindeutige Identifier der Benutzer:in (PersonIdentifier) aus der eben erfolgten Authentifizierung am eIDAS-Knoten für eine Suchanfrage im Zentralen Melderegister (ZMR) und im Ergänzungsregister (ERnP) verwendet. Im Rahmen dieses Prozessschritts erfolgt also eine Datenabfrage am ZMR/ERnP.

Inhalte der Anfrage an ZMR/ERnP:

- „PersonIdentifier“ der Benutzer:in aus Authentifizierung am eIDAS-Knoten
- LänderCode zum „PersonIdentifier“

Erwartete Inhalte der Antwort von ZMR/ERnP:

- Registereintrag mit übereinstimmendem „PersonIdentifier“ oder leere Liste

4.2.2. Prozessschritt 4)

In diesem Prozessschritt werden die Daten im ZMR/ERnP entsprechend den Daten aus der zuvor erfolgten Authentifizierung am eIDAS-Knoten ergänzt. Im Rahmen dieses Prozessschritts erfolgt also eine Aktualisierung von Daten im ZMR/ERnP.

Inhalte der Anfrage an ZMR/ERnP:

- In Prozessschritt 2) erhaltene Daten des bestehenden Registereintrags
- Zusätzliche/geänderte Attribute aus eIDAS-Anmeldung

Erwartete Inhalte der Antwort von ZMR/ERnP:

- OK

4.2.3. Prozessschritt 6)

In diesem Prozessschritt wird unter Verwendung der eIDAS-Attribute aus der zuvor erfolgten Authentifizierung am eIDAS-Knoten eine länderspezifische Detailsuche in ZMR/ERnP durchgeführt. Im Rahmen dieses Prozessschritts erfolgt also eine Datenabfrage am ZMR/ERnP.

Inhalte der Anfrage an ZMR/ERnP:

- Länderabhängige Liste an Attributen und zugehöriger Attributwerte aus Authentifizierung an eIDAS-Knoten

Erwartete Inhalte der Antwort von ZMR/ERnP:

- Liste an Registereinträgen mit übereinstimmenden Attributwerten

4.2.4. Prozessschritt 7a)

In diesem Prozessschritt wird ein bestehender Register-Eintrag mit den Daten aus der aktuellen eIDAS-Anmeldung zusammengeführt. Im Rahmen dieses Prozessschritts erfolgt also eine Aktualisierung von Daten im ZMR bzw. ERnP. Welche Daten des bestehenden Eintrags genau aktualisiert werden müssen/können, hängt vom aktuellen Datenbestand im Register und den verfügbaren Daten aus der eIDAS-Anmeldung ab.

Inhalte der Anfrage an ZMR/ERnP:

- Zuvor gefundener bestehender Register-Eintrag der Benutzer:in
- Zusätzliche bzw. neuere Daten/Attribute aus der eben durchgeführten eIDAS-Anmeldung

Erwartete Inhalte der Antwort von ZMR/ERnP:

- OK

4.2.5. Prozessschritt 7b)

In diesem Prozessschritt werden mehrere zu ein und derselben Person gehörende elektronische Identitäten (d.h. Einträge in ZMR oder ERnP) zusammengeführt. Konkret muss ein bestehender Register-Eintrag mit den Daten aus der ursprünglichen eIDAS-Anmeldung und auch mit den Daten aus der alternativen eIDAS-Anmeldung zusammengeführt werden. Im Rahmen dieses Prozessschritts erfolgt also eine Aktualisierung von Daten im ZMR/ERnP. Die konkrete Art und Weise der Zusammenführung hängt von diversen Rahmenbedingungen ab.

Inhalte der Anfrage an ZMR/ERnP:

- Zuvor gefundener bestehender Register-Eintrag der Benutzer:in

- Zusätzliche bzw. neuere Daten/Attribute aus der ursprünglich durchgeführten eIDAS-Anmeldung
- Zusätzliche bzw. neuere Daten/Attribute aus der eben durchgeführten eIDAS-Anmeldung

Erwartete Inhalte der Antwort von ZMR/ERnP:

- OK

4.2.6. Prozessschritt 8)

Im Rahmen dieses Prozessschritts wird eine Suche in ZMR und ERnP mit dem MDS der Benutzer:in (Familienname, Vorname, Geburtsdatum), das aus der zuvor erfolgten Authentifizierung am eIDAS-Knoten erhalten wurde, durchgeführt. Im Rahmen dieses Prozessschritts erfolgt also eine Datenabfrage am ZMR/ERnP.

Inhalte der Anfrage an ZMR/ERnP:

- MDS der Benutzer:in aus der eben durchgeführten eIDAS-Anmeldung

Erwartete Inhalte der Antwort von ZMR/ERnP:

- Liste an Registereinträgen mit übereinstimmendem MDS

4.2.7. Prozessschritt 9)

In diesem Prozessschritt wird ein neuer Eintrag im ERnP mit den Daten der Benutzer:in vorgenommen. Im Rahmen dieses Prozessschritts erfolgt also eine Neueintragung von Daten im ERnP.

Inhalte der Anfrage an ERnP:

- Daten der Benutzer:in aus der eben durchgeführten eIDAS-Anmeldung (PersonIdentifier, MDS, optional zusätzliche Attribute)

Erwartete Inhalte der Antwort von ERnP:

- OK

4.2.8. Prozessschritt 11)

Im Rahmen dieses Prozessschritts wird eine Suchanfrage in ZMR und ERnP mit dem neuen, aus der alternativen eIDAS-Authentifizierung resultierenden PersonIdentifier durchgeführt. Im Rahmen dieses Prozessschritts erfolgt also eine Datenabfrage am ZMR/ERnP.

Inhalte der Anfrage an ZMR/ERnP:

- PersonIdentifier der Benutzer:in aus der alternativen eIDAS-Anmeldung

Erwartete Inhalte der Antwort von ZMR/ERnP:

- Registereintrag mit übereinstimmendem „PersonIdentifier“ oder leere Liste

4.2.9. Prozessschritt 13)

In diesem Prozessschritt wird unter Verwendung der Attribute aus der erfolgten alternativen eIDAS-Anmeldung eine länderspezifische Detailsuche in ZMR/ERnP durchgeführt. Der Prozessschritt ist identisch zu jenem in Abschnitt 5.2.3, erfolgt jedoch mit Daten aus der gewählten alternativen Anmeldung. Im Rahmen dieses Prozessschritts erfolgt also eine Datenabfrage am ZMR/ERnP.

Inhalte der Anfrage an ZMR/ERnP:

- Länderabhängige Liste an Attributen und zugehöriger Attributwerte aus alternativer eIDAS-Authentifizierung

Erwartete Inhalte der Antwort von ZMR/ERnP:

- Liste an Registereinträgen mit übereinstimmenden Attributwerten

4.2.10. Prozessschritt 15)

Im Rahmen dieses Prozessschritts wird eine Suchanfrage in ZMR und ERnP mit dem bPK-ZP, das aus der Authentifizierung über Handy-Signatur erhalten wurde, durchgeführt. Im Rahmen dieses Prozessschritts erfolgt also eine Datenabfrage am ZMR/ERnP.

Inhalte der Anfrage an ZMR/ERnP:

- bPK-ZP der Benutzer:in

Erwartete Inhalte der Antwort von ZMR/ERnP:

- Registereintrag mit übereinstimmendem bPK-ZP oder leere Liste

4.2.11. Prozessschritt 18)

In diesem Prozessschritt wird im Register nach der Benutzer:in unter Verwendung der von der Benutzer:in eingegebenen Meldedaten gesucht. Im Rahmen dieses Prozessschritts erfolgt also eine Datenabfrage am ZMR/ERnP.

Inhalte der Anfrage an ZMR/ERnP:

- MDS der Benutzer:in
- Eingegebene Meldedaten der Benutzer:in

Erwartete Inhalte der Antwort von ZMR/ERnP:

- Liste an Registereinträgen mit übereinstimmenden MDS und Meldedaten oder leere Liste

5. Deployment und Konfiguration

Abbildung 5 zeigt nochmal die grundlegende Architektur des österreichischen eIDAS-Knotens und illustriert, dass zur Umsetzung des in diesem Dokument beschriebenen Matching-Konzepts ausschließlich Änderungen an der Komponente MS-Connector vorgenommen wurden. Andere Komponenten des österreichischen eIDAS-Knotens blieben davon unberührt.

Um die umgesetzte Matching-Funktionalität zur Anwendung zu bringen, ist daher lediglich das Deployment einer neuen Release der Komponente MS-Connector notwendig. Diese wird dem BM.I als Betreiber des österreichischen eIDAS-Knotens als Web Application Archive (WAR) Datei zur Verfügung gestellt und kann in einem entsprechend konfigurierten Application Server (Apache Tomcat) ausgeführt werden.

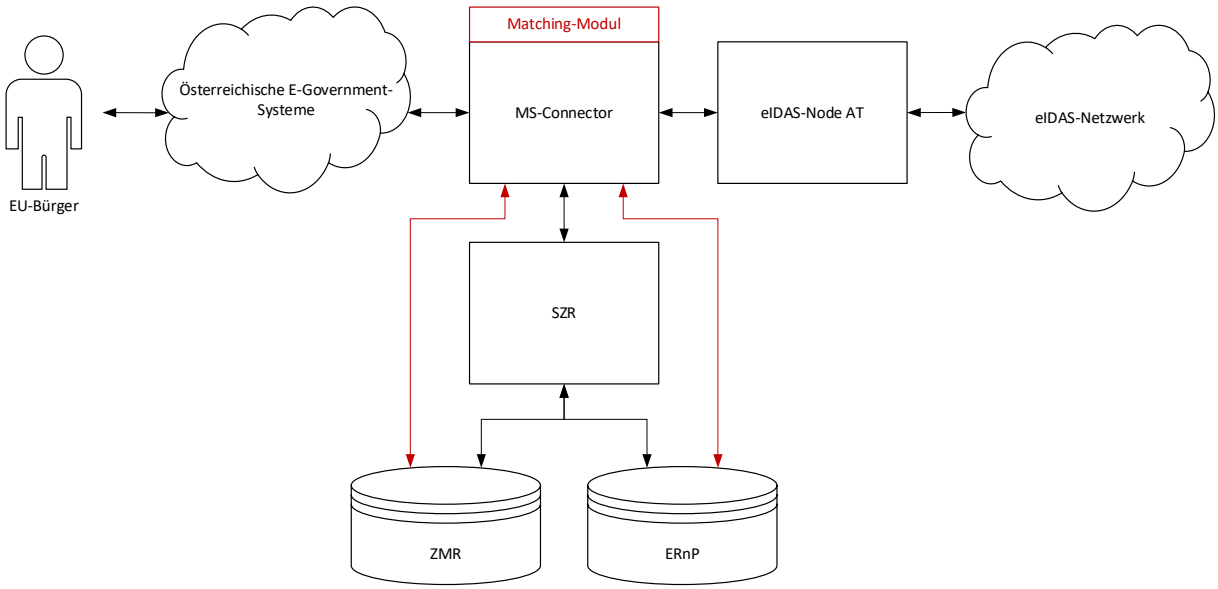

Abbildung 5. Komponenten des österreichischen eIDAS-Knotens.

Die WAR-Datei wird stets zusammen mit Release-Notes in Form einer Readme-Datei ausgeliefert. Diese Release-Notes beinhalten eine Übersicht zu den in der jeweiligen Version vorgenommenen Änderungen und relevante Informationen bezüglich der Durchführung eines Updates auf die aktuelle Version.

Zudem wird mit jeder Release ein Handbuch mitgeliefert. Dieses beschreibt notwendige Parameter zur Konfiguration der Applikation.

Anhang A: Vollständige Umsetzung: Annotiertes Prozessflussdiagramm

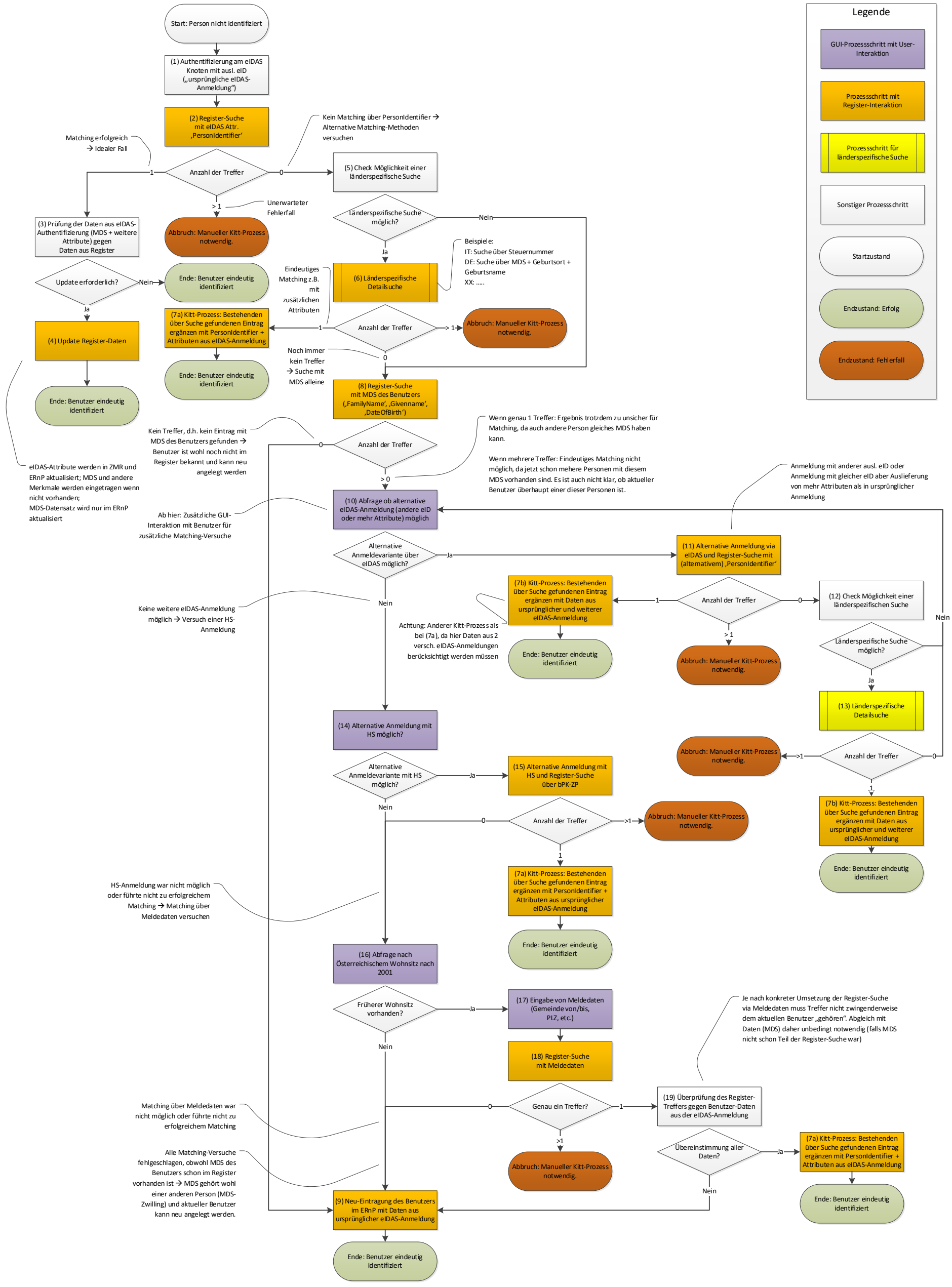

Abbildung 6. Annotierter Prozessfluss des gesamten Matching-Prozesses.