ID Austria

Technisches Whitepaper für Service-Owner

23. März 2023

Inhaltsverzeichnis

1. Einleitung ... 4
2. Die ID Austria im Überblick ... 6
2.1. Funktionen der ID Austria ... 6
2.2. Eigenschaften der ID Austria ... 6
2.3. Historie: Von der Bürgerkarte und Handy-Signatur zur ID Austria ... 7
2.4. Rechtliche Grundlagen ... 10
3. Überblick zur technischen Umsetzung der ID Austria ... 11
3.1. Architektur ... 11
3.2. Anmeldung an Service-Providern ... 13
3.3. Weitere Use-Cases ... 16
4. Anbindung eines Service-Providers an die ID Austria ... 17
4.1. Voraussetzungen zur Nutzung der ID Austria ... 17
4.2. Registrierung und Akkreditierung ... 18
4.2.1. Registrierung von öffentlichen Service-Providern ... 19
4.2.2. Registrierung von privaten Service-Providern ... 19
4.3. Technische Anbindung ... 21
4.3.1. Anbindung via SAML2 ... 21
4.3.2. Anbindung via OIDC ... 28
4.4. Migration von Bürgerkarte und Handy-Signatur auf die ID Austria ... 32
4.4.1. MOA E-ID Proxy ... 33
4.4.2. Aktivierung der Anbindung an die ID Austria im MOA E-ID Proxy ... 34
4.4.3. Anforderung der ID Austria an den MOA E-ID Proxy ... 35
4.4.4. Registrierung im zentralen Applikationsregister der ID Austria ... 35
4.4.5. Änderungen in Bezug auf die GUI-Integration ... 37
4.4.6. Verfügbarkeit des MOA E-ID Proxy ... 38
5. Ausgewählte Sicherheitsaspekte ... 39
5.1. Sicherstellung der Korrektheit und Aktualität ausgelieferter Attribute ... 39
5.2. Sichere Registrierungs- und Akkreditierungsprozesse ... 39
5.3. Kontrolle der vereinfachten Weiterverwendung einer vorherigen Authentifizierung ... 40
5.4. Sichere Auslieferung von Identitätsinformationen ... 41
5.4.1. Authentifizierung des Service-Providers an der ID Austria ... 41

5.4.2. Verschlüsselung der ausgelieferten Identitätsmerkmale 42
6. Vorgehensmodell für Service-Provider 43
7. Fazit und weiterführende Informationen 46

1. Einleitung

Für personalisierte Online-Anwendungen ist die sichere und zuverlässige Authentifizierung von Benutzer*innen unumgänglich. Viele Online-Anwendungen vertrauen dafür nach wie vor auf Authentifizierungsmethoden mit einem niedrigen Sicherheitsniveau. So ist die Authentifizierung über Bekanntgabe eines Benutzernamens und eines Kennworts nach wie vor stark verbreitet. Eine einfache und zugleich sichere Authentifizierung war in Österreich bisher schon durch die Verwendung der Bürgerkarte bzw. der Handy-Signatur möglich. Handy-Signatur und Bürgerkarte boten neben der sicheren und zuverlässigen Benutzerauthentifizierung Benutzer*innen auch die Möglichkeit, Dokumente elektronisch qualifiziert zu unterschreiben. Die qualifizierte elektronische Signatur, die der handschriftlichen Unterschrift gleichgestellt ist, bietet Rechtssicherheit und Schutz vor unbemerkten Änderungen. Damit gewährleistet die Verwendung der Handy-Signatur/Bürgerkarte die Authentizität von Bürger*innen, sowie die Unveränderbarkeit der signierten Daten.

Mit der Novelle zum E-Government-Gesetz[1] (2017) kommt es zu einer Weiterentwicklung der Bürgerkarte/Handy-Signatur zur sogenannten ID Austria, einem vollständigen elektronischen Identitätsnachweis. Die ID Austria ermöglicht es Bürger*innen, ihre Identität gegenüber elektronischen Anwendungen/Diensten/Verfahren (in diesem Dokument meist als Service-Provider bezeichnet), gemäß den Bestimmungen des E-Government-Gesetzes und angrenzender Rechtsmaterien (z.B. Signatur- und Vertrauensdiensteverordnung[2]), nachzuweisen. Mit dieser Weiterentwicklung soll die Verwendung der persönlichen elektronischen Identität (ID Austria) im Internet erleichtert und deren rechtliche Anerkennung in anderen europäischen Ländern ermöglicht werden.

Darüber hinaus werden die bisher schon von Handy-Signatur und Bürgerkarte bekannten Nutzungsmöglichkeiten mit der ID Austria erweitert, sodass künftig zum Beispiel auch weitere Personenmerkmale (Attribute) wie Einzelvertretungsbefugnisse, Führerschein- und Meldedaten, Staatsbürgerschaftsnachweise, etc. an dritte Stellen (z.B. elektronische Dienstanbieter) übermittelt werden können. Die Entscheidung, ob Daten an Dritte übermittelt werden dürfen, obliegt dabei stets den Betroffenen, d.h. den Bürger*innen.

Ein weiterer Vorteil der ID Austria im Vergleich zum bisherigen Handy-Signatur/Bürgerkarte-System betrifft die breite Unterstützung mobiler Anwendungsfälle. Trotz ihres mobilen Charakters war die Handy-Signatur bisher auf eine Verwendung auf klassischen Endnutzergeräten wie PCs oder Laptops beschränkt. Das mobile Gerät (Handy, Smartphone) kam dabei nur als Zweitgerät im Zuge der Benutzerauthentifizierung zum Einsatz. Die ID Austria ist hier weit flexibler und ermöglicht auch eine rein mobile Nutzung. Unter anderem können so in Zukunft auch App-basierte Service-Provider die ID Austria nutzen, um beispielsweise Bürger*innen in der App zuverlässig über die ID Austria zu authentifizieren.

Um wie bisher ein höchstes Maß an Sicherheit zu gewährleisten, verwendet die ID Austria unter anderem native Sicherheitsfunktionen der verwendeten mobilen Geräte. So werden die in modernen Smartphones verbauten sicheren Hardwarebausteine ebenso verwendet wie die von den mobilen Plattformen

[1] E-Government Gesetz:
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230
[2] Signatur- und Vetrauensdiensteverordnung:
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20009619

bereitgestellten sicheren biometrischen Authentifizierungsmethoden wie Fingerprint oder Gesichtserkennung. Dadurch wird eine gleichzeitige Verbesserung sowohl von Benutzerfreundlichkeit als auch Sicherheit erreicht.

Durch den erweiterten Funktionsumfang der ID Austria ergeben sich auch für Service-Owner[3], die die ID Austria für ihre Service-Provider nutzen möchten, einige Änderungen. Dieses Dokument bietet Service-Ownern relevante Hintergrundinformationen über die Funktionen sowie die technische Umsetzung der ID Austria. Spezielles Augenmerk wird dabei auf jene Aspekte gelegt, die für Service-Owner von besonderer Bedeutung sind. Dazu gehören die Registrierung und ggf. Akkreditierung von Service-Providern, welche nun eine zwingende Voraussetzung zur Nutzung der ID Austria sind, sowie auch die technische Anbindung von Service-Providern über die vorgesehenen Schnittstellen der ID Austria.

[3] Dieses Dokument verwendet folgende Terminologie: Der Begriff „Service-Provider (SP)“ bezeichnet ein technisches Service, das Endnutzer*innen angeboten wird. Ein Beispiel für einen Service-Provider wäre FinanzOnline. Der Begriff „Service-Owner (SO)“ bezeichnet die für den Service-Provider verantwortliche Organisation. Das kann eine Organisation des öffentlichen Sektors (z.B. ein Ministerium) oder auch ein privatwirtschaftliches Unternehmen sein. Ein Service-Owner kann für eine beliebige Anzahl an Service-Providern verantwortlich sein.

2. Die ID Austria im Überblick

Die ID Austria stellt eine Weiterentwicklung von Handy-Signatur und Bürgerkarte dar. Dementsprechend verfügt sie über ähnliche Funktionen, setzt diese jedoch teilweise anders um und weist damit punktuell andere Eigenschaften auf. Funktionen und Eigenschaften der ID Austria werden in den folgenden Unterabschnitten näher beschrieben. Nachfolgend wird ergänzend auf ausgewählte historische Aspekte und rechtliche Aspekte eingegangen, um so einen ersten Überblick zur ID Austria abzurunden.

2.1. Funktionen der ID Austria

Die ID Austria ermöglicht es behördlichen und privaten Service-Providern (Web-Applikationen, Apps, etc.), die Funktionalität des Logins bzw. der Anmeldung von Benutzer*innen über deren persönliche ID zu integrieren. Grundsätzlich stellt das ID-Austria-System dabei die folgenden Authentifizierungsmöglichkeiten zur Verfügung:

- **Authentifizierung an einem Vertrauensdiensteanbieter (VDA)**: Anmeldung mittels Erstellung einer qualifizierten Signatur bei einem VDA. Die erstellte Signatur dient als Identifikationsmittel gegenüber dem Identity-Provider (IDP) des ID-Austria-Systems.
- **Vereinfachte Weiterverwendung einer Authentifizierung am ID-Austria-System:** Anmeldung am ID-Austria-System mittels eines kryptographischen Bindungszertifikats, das nach der Registrierung der ID Austria zwischen Benutzer*innen, deren mobile Geräte und dem IDP erstellt werden kann. Die vereinfachte Weiterverwendung der ID Austria[4] ist gemäß E-Government-Gesetz (EGovG) umgesetzt.
- **Authentifizierung über eIDAS:** Anmeldung via grenzübergreifenden eIDAS-Framework für Benutzer*innen mit ausländischen elektronischen Identitäten (eID).

Neben der sicheren Authentifizierung von Benutzer*innen bietet die ID Austria auch die Möglichkeit, qualifizierte – und damit rechtsgültige – elektronische Signaturen zu erstellen. Auch diese Funktion kann von Service-Providern integriert werden, um etwa Formulare oder Verträge durch Endanwender*innen signieren zu lassen.

2.2. Grundlegende Eigenschaften der ID Austria

Als Nachfolger der Bürgerkarte bzw. Handy-Signatur erbt die ID Austria alle positiven Eigenschaften, die schon die bestehenden Lösungen Bürgerkarte und Handy-Signatur ausgezeichnet haben. Durch gezielte Weiterentwicklungen wurden diese Eigenschaften noch um weitere Aspekte erweitert. Im Folgenden sind die Kerneigenschaften der ID Austria zusammengefasst.

- **Mehrfaktorauthentifizierung.** Sichere Authentifizierung von Benutzer*innen in Online-Verfahren über Mehrfaktorauthentifizierung.

- **Staatliche Register als Basis.** Zuverlässige Identifizierung von Benutzer*innen über eindeutigen (jedoch sektorspezifischen) Identifikator (verknüpft mit österreichischen

[4] Vereinfachte Weiterverwendung: https://www.parlament.gv.at/PAKT/VHG/XXVII/ME/ME_00056/index.shtml

staatlichen Registern) und Minimal Dataset (bestehend aus Vornamen, Familiennamen und Geburtsdatum).

- **Unterstützung ausländischer nationaler eID-Systeme.** Unterstützung der Authentifizierung von Benutzer*innen mit ausländischem eID über Anbindung der ID Austria an das europäische eIDAS-Framework.
- **Behördlicher Ausstellungsprozess.** Registrierungs- und Ausstellungsprozess einer ID Austria für Bürger*innen in behördlicher Qualität.
- **Grenzüberschreitende Verwendbarkeit.** Tauglichkeit für den grenzüberschreitenden Einsatz der ID Austria zum Beispiel zur Anmeldung an Service-Providern anderer EU-Mitgliedsstaaten.
- **Mobile-Ready.** Unterstützung von mobilen Nutzungsszenarien wie zum Beispiel App-basierte Service-Provider.
- **Erweitertes Attribut-Set.** Auslieferung von weiteren persönlichen Attributen an Service-Provider. Zusätzliche Attribute werden aus zugänglichen Datenquellen (z.B. Verwaltungsregister) bezogen und ausschließlich nach Zustimmung der Benutzer*in ausgeliefert.
- **Nachhaltigkeit.** Nachhaltige und anpassungsfähige technische Architektur, die sich durch einen modularen Aufbau, eine einfache Anbindung von Service-Providern über Standard-Identitätsprotokolle sowie die Anbindung an den österreichischen Register- und Systemverbund auszeichnet.
- **Qualifizierte Signatur als Zusatzfeature.** Unterstützung der Erstellung von rechtsgültigen, qualifizierten elektronischen Signaturen (z.B. PDF-Signaturen)

Die Summe dieser Eigenschaften bringt nicht nur für Benutzer*innen zahlreiche Vorteile, sondern macht die ID Austria auch für Service-Provider zu einer attraktiven Identitätsmanagementlösung.

2.3. Historie: Von der Bürgerkarte und Handy-Signatur zur ID Austria

Nationale Identitätsmanagementsysteme sind wie alle technischen Systeme dem Wandel der Zeit unterworfen und müssen stets den aktuellen Anforderungen angepasst werden. Als Weiterentwicklung der Bürgerkarte und Handy-Signatur stellt die ID Austria den bislang letzten Entwicklungsschritt im Rahmen des laufenden Weiterentwicklungsprozesses des österreichischen nationalen elektronischen Identitätsmanagementsystems dar. Im Sinne der Vollständigkeit und der besseren Nachvollziehbarkeit diverser Designentscheidungen hinter der ID Austria sei an dieser Stelle ein kurzer historischer Rückblick auf die Entwicklungen der letzten Jahrzehnte gegeben.

Betrachtet man den gesamten Entwicklungsprozess des österreichischen nationalen elektronischen Identitätsmanagementsystems, so kann die Bürgerkarte als erster wesentlicher Schritt und Grundstein aller nachfolgenden Weiterentwicklungen ausgemacht werden. Grundidee der Bürgerkarte war es, Bürger*innen ein Werkzeug in die Hand zu geben, mit dem sie sich sicher und zuverlässig an Online-Services (Service-Providern) der österreichischen E-Government-Infrastruktur authentifizieren konnten. In Anbetracht der technischen Möglichkeiten und Rahmenbedingungen der damaligen Zeit scheint auch

heute noch die Wahl von Chipkarten als zugrundeliegende Technologie nachvollziehbar. Bürger*innen konnten unterschiedliche Chipkarten (so z.B. auch die e-card) als Bürgerkarte aktivieren. Im Zuge der Aktivierung wurde die Stammzahl als eindeutiger Identifikator zusammen mit dem Minimal Dataset (MDS) sicher auf die Chipkarte aufgebracht. Die Stammzahl wurde dabei im Zuge des Registrierungsprozesses aus der ZMR-Zahl der Bürger*in berechnet, die ZMR-Zahl dazu aus dem ZMR abgefragt[5]. Stammzahl und MDS wurden in eine signierte Datenstruktur, die sogenannte Personenbindung, eingebettet und in der Chipkarte sicher gespeichert. Im Zuge des Aktivierungsprozesses wurde ebenfalls ein qualifiziertes Signaturzertifikat für die Bürger*in ausgestellt und auf ihre Chipkarte aufgebracht. Der gesamte Aktivierungsprozess wurde dementsprechend vom Zertifizierungsdienstanbieter (ZDA), der die entsprechenden qualifizierten Signaturzertifikate ausstellen konnte, durchgeführt.

Die Verwendung der Bürgerkarte im Zuge von Anmeldeprozessen an Service-Providern erforderte die Installation einer Software (die sogenannte Bürgerkartenumgebung) auf dem Endnutzergerät der Bürger*in. Nach Eingabe der entsprechenden Karten-PIN(s) im Zuge des Anmeldeprozesses wurden von der Chipkarte zunächst die erforderlichen Attribute (Identifikator, MDS) in Form der Personenbindung ausgelesen. Über die Erstellung einer qualifizierten Signatur stimmte die Bürger*in schließlich der Übermittlung der Attribute an den Service-Provider zur erfolgreichen Anmeldung zu. Die Erstellung einer qualifizierten Signatur war dementsprechend immer schon ein integraler Bestandteil bürgerkartenbasierter Anmeldeprozesse.

Auf Seiten des Service-Providers war zur Unterstützung bürgerkartenbasierter Anmeldeprozesse die Installation und der Betrieb der Software MOA-ID (Module für Online-Applikationen – Identifikation) notwendig. Diese kapselte den gesamten bürgerkartenbasierten Anmeldeprozess (Interaktion mit der Bürgerkartenumgebung, etc.) und fungierte aus Sicht des Service-Providers sozusagen als dezentraler Identity-Provider (IDP).

Nachteile dieses ursprünglichen Konzepts, d.h. der Umsetzung der Funktion „Bürgerkarte“ über Chipkarten, zeigten sich in der Praxis vor allem in Bezug auf die Benutzerfreundlichkeit. So stellte die notwendige lokale Installation und der Betrieb eines Kartenlesegeräts und der Software „Bürgerkartenumgebung“ viele Bürger*innen vor Herausforderungen. Die Notwendigkeit einer lokalen Softwareinstallation wurde zwischenzeitig durch eine Java-Applet-basierte Alternative aufgehoben, trotzdem konnten chipkartenbasierte Ansätze insgesamt kein hohes Akzeptanzniveau erreichen.

Um hier entgegenzuwirken, wurde die Handy-Signatur entwickelt. Grundlegende Idee war es, Benutzer*innen eine Alternative zur chipkartenbasierten Bürgerkarte zu bieten, die ohne lokale Hardware- und Softwareinstallationen auskommt, gleichzeitig aber denselben Funktionsumfang (sichere Anmeldung an Service-Providern, Erstellung qualifizierter elektronischer Signaturen) bietet. Um diese Anforderungen zu erfüllen, basiert die Handy-Signatur auf einem zentralen Hardware Security Module (HSM). Dieses hat vergleichbare Sicherheitseigenschaften wie eine Chipkarte, ist jedoch weit performanter. Das zentrale HSM ersetzt bei der Handy-Signatur die Funktionen der Chipkarte, d.h. es wird zur sicheren Speicherung und Verwendung der im Rahmen der Aktivierung erstellten Personenbindungen und Signaturzertifikate (und Schlüssel) der Bürger*innen verwendet. Die Verwendung von Chipkarten wird damit obsolet. Gleichzeit müssen die sicherheitskritischen Daten auch nicht am Mobiltelefon der Bürger*in gespeichert

[5] Alternativ konnten die entsprechenden Daten auch dem Ergänzungsregister für natürliche Personen (ERnP) bezogen werden, dieser Vorgang war für die Bürger*in ohnehin weitgehend transparent.

werden. Das Mobiltelefon dient ausschließlich als zweiter Authentifizierungsfaktor (neben einem Passwort), über den sichergestellt wird, dass nur die legitime Person Zugriff auf ihre zentral im HSM gespeicherten Daten erhält.

Durch den Wegfall der Chipkarte weist die Handy-Signatur eine wesentlich höhere Benutzerfreundlichkeit im Vergleich zur klassischen Bürgerkarte auf. Diese zeigte sich in den letzten Jahren auch deutlich an den Nutzerzahlen. Aus Sicht der Service-Owner und Service-Provider ergab sich durch Einführung der Handy-Signatur wenig Adaptierungsbedarf. Tatsächlich war der gesamte Anmeldeprozess nach wie vor in MOA-ID gekapselt. In der Regel war es für den Service-Provider irrelevant, ob „hinter" MOA-ID eine Benutzerauthentifizierung über Bürgerkarte oder Handy-Signatur stattfand. Die Schnittstelle zu MOA-ID und die von MOA-ID erhaltenen Daten der Benutzer*in (Personenbindung, etc.) waren stets gleich. Dies bedeutete auch, dass der Betrieb einer MOA-ID Instanz nach wie vor eine zwingende Voraussetzung für Service-Provider war, die die Handy-Signatur zur Anmeldung von Benutzer*innen nutzen wollten.

Obwohl die Handy-Signatur vor allem in Bezug auf die Benutzerfreundlichkeit ein bedeutender Schritt in die richtige Richtung war, zeigten sich auch hier im Laufe der Zeit einige Limitierungen. So ist die Handy-Signatur nicht für sogenannten Mobile-Only-Lösungen geeignet, in denen das mobile Endnutzergerät (z.B. Smartphone) die einzige Benutzerschnittstelle zum Service-Provider darstellt. Die Handy-Signatur bedingt aus Sicherheitsgründen immer die Verwendung zweier unabhängiger Endnutzergeräte (in der Regel PC/Laptop und Mobiltelefon). Ein rein App-basierter Service-Provider kann so die Handy-Signatur nicht nutzen. Auch die Tatsache, dass die Personenbindung mit den Attributen der Bürger*in einmalig zum Zeitpunkt der Aktivierung der persönlichen Handy-Signatur erstellt wird, weist in der Praxis einige Nachteile auf. Zu guter Letzt ist auch die nach wie vor bestehende Notwendigkeit des Betriebs von MOA-ID durch Service-Owner nicht ideal.

Ziel der ID Austria ist es, diese nach wie vor bestehenden Nachteile auszumerzen und das österreichische nationale elektronische Identitätsmanagementsystems bereit für eine rein mobile Nutzung zu machen. Durch diverse grundlegende architektonische Änderungen wird bei der ID Austria beispielsweise der Betrieb einer MOA-ID-Instanz für Service-Owner obsolet. Zusätzlich wird die Personenbindung nun im Rahmen jedes Anmeldeprozesses dynamisch neu erstellt und kann neben eindeutigem Identifikator und dem MDS nun auch noch weitere Informationen zur Bürger*in (Attribute) enthalten, wobei die Bürger*in stets die Kontrolle über die Auslieferung ihrer Attribute behält. Der wohl wichtigste Vorteil für Bürger*innen ist aber wohl, dass die ID Austria auch geeignet für Mobile-Only-Lösungen ist, die Notwendigkeit der Verwendung zweier separater Endnutzergeräte also nicht mehr gegeben ist.

Wie schon im ursprünglichen Bürgerkarten-Konzept vorgesehen, unterstützt auch die ID Austria nach wie vor die sichere Anmeldung an Service-Providern und die Erstellung qualifizierter elektronischer Signaturen. Während diese Kernfunktionen über alle Entwicklungsschritte der letzten Jahrzehnte beibehalten wurden, wurden die zugrundliegenden technischen Konzepte und konkreten Implementierungen stets den aktuellen Anforderungen und Rahmenbedingungen angepasst. Die ID Austria stellt den aktuell letzten Schritt dieser laufenden Weiterentwicklung dar.

2.4. Rechtliche Grundlagen

Die rechtlichen Grundlagen für die ID Austria sind unter anderem durch das E-Government-Gesetz (EGovG)[6] und dessen letzte Novelle[7], sowie durch die Verordnung der Europäischen Union über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS Verordnung[8]) gegeben. Daneben existieren noch weitere Rechtsgrundlagen auf nationaler und EU-Ebene, die ebenfalls einen Einfluss auf Konzept und Umsetzung der ID Austria haben. Exemplarisch sei an dieser Stelle die Datenschutzgrundverordnung (DSGVO[9]) in Verbindung mit dem Datenschutzgesetz (DSG) genannt, die natürlich auch im Kontext der ID Austria zu berücksichtigen ist.

Ein vollständiger Überblick aller rechtlichen Grundlagen würde den Rahmen dieses Dokuments bei weitem sprengen. Zusammenfassend kann jedoch festgehalten werden, dass die ID Austria als österreichisches nationales elektronisches Identitätsmanagementsystem einerseits auf gesetzlichen Vorgaben beruht und andererseits konform zu allen geltenden Gesetzen und Verordnungen ist.

[6] E-Government-Gesetz: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230
[7] Novelle zum E-Government-Gesetz: https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2020_I_169/BGBLA_2020_I_169.html
[8] IDAKS Verordnung: https://eur-lex.europa.eu/eli/reg/2014/910/oj?locale=de
[9] DSGVO: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32016R0679

3. Überblick zur technischen Umsetzung der ID Austria

Dieses Kapitel bietet eine Übersicht der technischen Umsetzung der ID Austria. Dazu wird zunächst die technische Architektur im Überblick beschrieben. Basierend darauf wird dann auf den aus Sicht eines Service-Providers relevantesten Anwendungsfall „Anmeldung an einem Service-Provider“ näher eingegangen. Weitere Anwendungsfälle werden im Überblick kurz skizziert.

3.1. Architektur

Bei der ID Austria handelt es sich um ein komplexes Gesamtsystem, das sich aus diversen Einzelkomponenten zusammensetzt. Die Einzelkomponenten werden dabei von verschiedenen Organisationen entwickelt und betrieben. Für Service-Owner und ihre Service-Provider bleibt die interne Struktur des Gesamtsystems weitgehend transparent. Service-Provider interagieren mit dem System „ID Austria“ stets über wohldefinierte Schnittstellen. In diesem Abschnitt wird im Sinne eines guten Gesamtverständnisses trotzdem ein rudimentärer Blick auf die interne Struktur des Gesamtsystems geworfen.

Die Gesamtarchitektur der ID Austria setzt sich aus mehreren Domains zusammen. Jede Domain enthält eine oder mehrere Komponenten des Gesamtsystems. Der Begriff Domain bezeichnet hier einen Teil des Gesamtsystems, dessen Komponenten von einer Organisation (BRZ, BMI, etc.) betrieben werden und der einen bestimmten Teil der Funktionalität der ID Austria kapselt. Eine Sonderstellung nimmt hier die User-Domain ein, die den Bereich der Endnutzer*in, sowie deren verwendeten Endnutzergeräte umfasst.

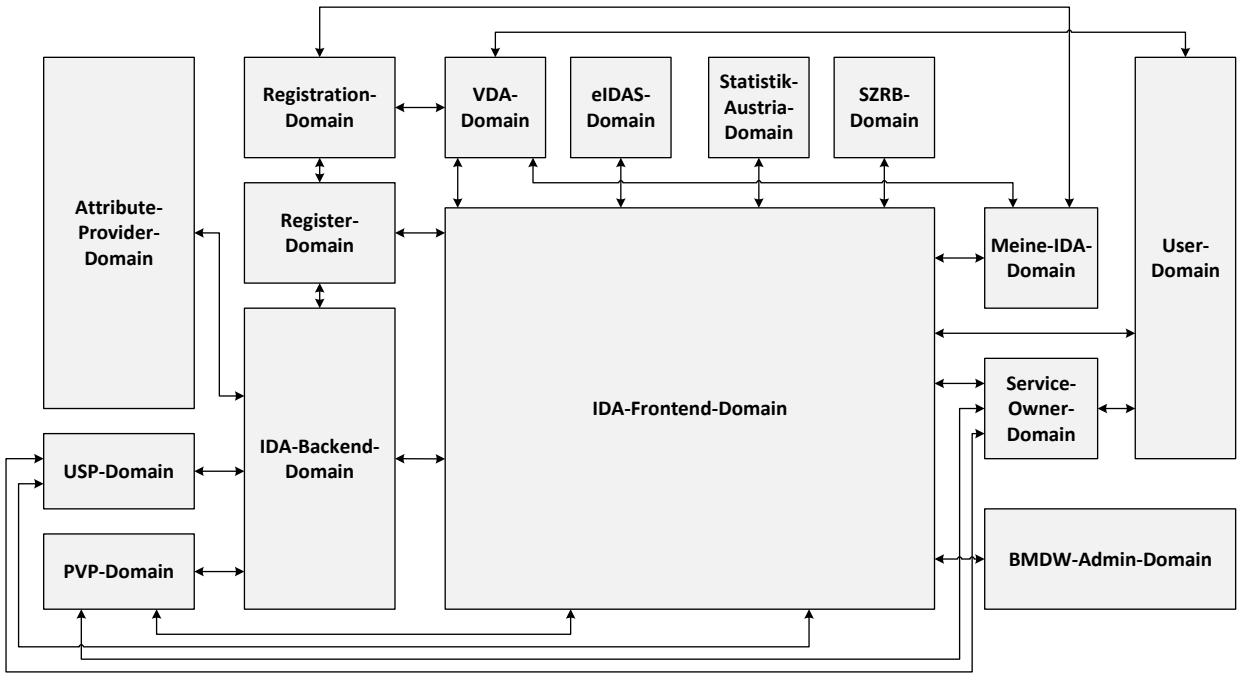

Abbildung 1. Gesamtarchitektur der ID Austria - Domain Ebene.

Im Sinne einer übersichtlichen Darstellung zeigt Abbildung 1 die relevanten Domains der ID Austria, ohne auf deren Komponenten im Detail einzugehen. In dieser Darstellung werden neben den einzelnen Domains selbst auch relevante Schnittstellen zwischen diesen Domains sichtbar.

Aus der Darstellung auf Domainebene kann bereits eine erste grobe Beschreibung der verschiedenen Anwendungsszenarien, die die ID Austria unterstützt, gegeben werden. Diese sind im Folgenden zusammengefasst.

Vor einer Verwendung der ID Austria muss die Benutzer*in ihre persönliche ID Austria registrieren. Dies erfolgt über definierte, organisatorische Prozesse und technische Komponenten, die in der Registration-Domain angesiedelt sind. Die Registration-Domain und ihre Komponenten werden vom Bundesministerium für Inneres (BM.I) bereitgestellt. Die Registration-Domain verfügt über eine Schnittstelle zur User-Domain, da die Benutzer*in mit ihren Endgeräten mit Komponenten der Registration-Domain interagieren muss. Die Registration-Domain verfügt über weitere Schnittstellen zur Backend-Domain und zur VDA-Domain. Erstere ist ebenfalls im Bereich des BM.I angesiedelt und beinhaltet unter anderem das für die Registrierung einer persönlichen ID Austria notwendige Stammzahlenregister (SZR). Die VDA-Domain repräsentiert hingegen den Bereich des Vertrauensdienstanbieters (VDA), der im Zuge der Registrierung einer ID Austria ein qualifiziertes Signaturzertifikat für die Benutzer*in ausstellt.

Nach erfolgter Registrierung kann die Benutzer*in ihre persönliche ID Austria zur Anmeldung an Service-Providern verwenden. Service-Provider (und auch die entsprechenden Service-Owner) sind in der Service-Provider-Domain angesiedelt. Die Service-Provider-Domain verfügt über eine Schnittstelle zur User-Domain, über welche die Benutzer*in bereitgestellte Dienste des Service-Providers in Anspruch nehmen kann. Der Service-Provider nutzt die ID Austria zur Authentifizierung der Benutzer*in. Dementsprechend verfügt die Service-Provider-Domain auch über eine Schnittstelle zur Frontend-Domain. Diese wird durch das BRZ betrieben und stellt unter anderem jene Schnittstellen bereit, über die Service-Provider Anmeldeprozesse initiieren können. Um Dienste der ID Austria nutzen zu können, muss der Service-Provider zunächst selbst bei der ID Austria registriert und akkreditiert werden. Dies erfolgt unter anderem über Komponenten in der USP/PVP-Domain. Dementsprechend existiert auch eine Schnittstelle zwischen der Service-Provider-Domain und der USP/PVP-Domain.

Kernaufgabe der Frontend-Domain ist die Authentifizierung von Benutzer*innen. Die Authentifizierung erfolgt im Falle der Verwendung einer registrierten, persönlichen ID Austria über den Vertrauensdienstanbieter (VDA), der in der VDA-Domain angesiedelt ist. Dementsprechend verfügt die Frontend-Domain über eine Schnittstelle zur VDA-Domain. Für Bürger*innen anderer EU-Mitgliedsstaaten kann eine Authentifizierung über das eIDAS-Framework erfolgen. Komponenten des eIDAS-Frameworks sind der eIDAS-Domain zugeordnet, die sich ebenfalls im Hoheitsgebiet des BM.I befindet, und welche ebenfalls über eine Schnittstelle zur Frontend-Domain verfügt. Sowohl VDA-Domain als auch eIDAS-Domain haben eine Schnittstelle zur User-Domain, über die die Benutzer*in authentifiziert wird. Auch die Frontend-Domain selbst verfügt über eine Schnittstelle zur User-Domain, da auch hier eine Interaktion mit der Benutzer*in im Zuge der Benutzerauthentifizierung notwendig ist. Da sich eine Benutzer*in auch mittels einer Vollmacht in Vertretung für eine andere Person anmelden kann, benötigt die Frontend-Domain auch eine Anbindung an Komponenten, die relevante Vollmachten-Informationen bereitstellen. Solche Komponenten sind in der Statistik-Austria-Domain, der SZRB-Domain und der USP/PVP-Domain

angesiedelt. Die Frontend-Domain verfügt demzufolge auch über Schnittstellen zu diesen drei Domains. Zur Bereitstellung von datenschutzrechtlich relevanten Informationen verfügt die Frontend-Domain auch über eine Schnittstelle zur BMDW-Admin-Domain. Über diese Schnittstelle können gezielt datenschutzbezogene Abfragen an die ID Austria gestellt werden. Schließlich verfügt die Frontend-Domain auch noch über eine Schnittstelle zur Meine-ID-Austria-Domain, sodass Benutzer*innen über ein persönliche Dashboard[10] Abfragen und Wartungstätigkeiten (Widerruf, etc.) selbstständig durchführen können.

Während die Frontend-Domain primär für die Authentifizierung von Benutzer*innen verantwortlich ist, liegt es im Verantwortungsbereich der Backend-Domain, die im Zuge des Anmeldeprozesses vom Service-Provider angeforderten Attribute bereitzustellen. Die Frontend-Domain fragt benötigte Attribute dementsprechend über eine Schnittstelle zur Backend-Domain ab. Die Backend-Domain hält einige der unterstützten Attribute selbst. Andere Attribute werden hingegen von der Attribute-Provider-Domain bezogen. Dazu verfügt die Backend-Domain über eine Schnittstelle zur Attribute-Provider-Domain. Neben der bereits oben erwähnten Schnittstelle zur Registration-Domain verfügt die Backend-Domain auch noch über eine Schnittstelle zur USP/PVP-Domain, welche im Zuge der Registrierung von Service-Providern benötigt wird.

Zusammengefasst ermöglichen das Gesamtsystem der ID Austria und seine Domains, dass sich Benutzer*innen ihre persönliche ID Austria registrieren und sich in weiterer Folge mit ihren registrierten ID Austria an Service-Providern anmelden (authentifizieren) können. Die notwendige Funktionalität wird durch technische Komponenten, die in den verschiedenen Domains angesiedelt sind, bereitgestellt.

3.2. Anmeldung an Service-Providern

Die Anmeldung an Service-Providern stellt aus Sicht der Benutzer*innen den wohl wichtigsten Anwendungsfall der ID Austria dar. Nach erfolgter Registrierung der persönlichen ID Austria kann eine Anmeldung an Service-Providern beliebig oft wiederholt werden, solange die persönliche ID Austria der Benutzer*in gültig ist.

Die ID Austria unterstützt verschiedene Varianten von Anmeldeprozessen. Die unterschiedlichen Varianten ergeben sich dabei primär aufgrund der Variation folgender Faktoren:

- **Art der Benutzerauthentifizierung.** Im Zuge der Anmeldung an einem Service-Provider fungiert das ID-Austria-System als Identity-Provider (IDP). Die Benutzer*in muss sich dementsprechend gegen das ID-Austria-System authentifizieren. Dafür stehen unterschiedliche Optionen zur Verfügung.
    - **VDA.** Authentifizierung via VDA unter Verwendung der persönlichen ID Austria.
    - **Vereinfachte Weiterverwendung.** Authentifizierung via vereinfachte Weiterverwendung einer vorherigen erfolgreichen Authentifizierung[11].

[10] Das Dashboard ist derzeit noch in Entwicklung. Der Begriff „Dashboard“ ist ein Arbeitstitel, der endgültige Name dieser Anwendung, die der Benutzer*in die Verwaltung ihrer ID Austria ermöglicht, steht noch nicht fest.
[11] Das Konzept der vereinfachten Weiterverwendung wurde mit der ID Austria neu eingeführt. Nach einer erfolgreichen Authentifizierung unter Verwendung der persönlichen ID Austria können Benutzer*innen ihr mobiles

    - **EU-Login.** Authentifizierung via eIDAS-konformer ausländischer elektronischer Identitäten.

- **Verwendete Client-Komponente.** Die Anmeldung an einem Service-Provider kann von Benutzer*innen mit verschiedenen Client-Komponenten initiiert werden. Welche Client-Komponente zum Einsatz kommt, hängt vom Service-Provider und der Art des angebotenen Service ab. Allgemein gesprochen stehen in Bezug auf die Verwendung von Client-Komponenten die Optionen Digitales-Amt-App, Third-Party-App[12] und Web-Browser zur Verfügung, wobei für die letzten beiden noch unterschieden werden muss, ob sich diese am selben Gerät wie die Digitales-Amt-App befinden oder auf einem Zweitgerät verwendet werden.

Durch Variation dieser Faktoren (Art der Benutzerauthentifizierung bzw. verwendete Client-Komponente) ergeben sich unterschiedliche Varianten von Anmeldeprozessen. Die wichtigsten Varianten sind im Folgenden überblicksmäßig beschrieben.

- **Anmeldung in Digitales-Amt-App.** Die Benutzer*in befindet sich in der Digitales-Amt-App. Die App greift auf eine geschützte Ressource eines serverseitigen SP zu. Der SP erstellt daraufhin einen Authentifizierungs-Request, der über die ID-Austria-Komponente der Digitales-Amt-App an den Identity-Provider (IDP) übermittelt wird. Die Benutzerauthentifizierung am IDP erfolgt über die ID-Austria-Komponente der Digitales-Amt-App. Nach erfolgter Benutzerauthentifizierung erstellt der IDP einen Identitätsnachweis und übermittelt diesen an den SP. Die Benutzer*in wird aus der ID-Austria-Komponente zurück in die Digitales-Amt-App weitergeleitet.

- **Anmeldung in Third-Party-App.** Die Benutzer*in befindet sich in einer Third-Party-App (TPA), die sich am gleichen Gerät wie die Digitales-Amt-App mit ID-Austria-Komponente befindet. Die TPA greift auf eine geschützte Ressource eines serverseitigen SP zu. Der SP erstellt daraufhin einen Authentifizierungs-Request, der zunächst über die TPA an die ID-Austria-Komponente der Digitales-Amt-App und von dort an den IDP übermittelt wird. Die Benutzerauthentifizierung am IDP erfolgt über die ID-Austria-Komponente der Digitales-Amt-App. Nach erfolgter Benutzerauthentifizierung erstellt der IDP einen Identitätsnachweis und übermittelt diesen an den SP. Die Benutzer*in wird aus der ID Austria-Komponente zurück in die TPA weitergeleitet.

- **Anmeldung in Third-Party-App ausgehend von Digitales-Amt-App.** Ziel ist auch in dieser Variante, dass eine authentifizierte Session zwischen einer Third-Party-App, die sich am gleichen Gerät wie die Digitales-Amt-App mit ID-Austria-Komponente befindet, und einem serverseitigen SP hergestellt wird. Allerdings befindet sich die Benutzer*in beim Start des

---

Gerät unter Verwendung der Digitales-Amt-App an das ID-Austria-System kryptographisch binden. Dabei wird ein Token ausgestellt und am mobilen Gerät sicher gespeichert. Das Token kann dann für nachfolgende Authentifizierungsprozesse gegen die ID Austria verwendet werden. Die Benutzer*in erspart sich so die Eingabe des Passworts, eine Authentifizierung erfolgt über ein biometrisches Merkmal und das erwähnte Token.

[12] Dabei handelt es sich um eine spezifische App, die vom Service-Owner zusammen mit dem Service-Provider bereitgestellt wird. Die Third-Party-App kann entweder als Frontend eines serverseitigen Service-Providers (z.B. ein Web-Service) dienen, oder auch als Stand-alone-Komponente fungieren.

Anmeldeprozesses nicht in der Third-Party-App, sondern in der Digitales-Amt-App. Dementsprechend greift die Digitales-Amt-App auf eine geschützte Ressource eines serverseitigen SP zu. Der SP erstellt daraufhin einen Authentifizierungs-Request, der über die Digitales-Amt-App und ihre ID-Austria-Komponente an den IDP übermittelt wird. Die Benutzerauthentifizierung am IDP erfolgt über die ID-Austria-Komponente der Digitales-Amt-App. Nach erfolgter Benutzerauthentifizierung erstellt der IDP einen Identitätsnachweis und übermittelt diesen an den SP. Die Benutzer*in wird aus der ID-Austria-Komponente in die TPA weitergeleitet. Dabei wird auch die notwendige Information an die TPA übergeben, über die schlussendlich die authentifizierte Session zwischen der TPA und dem SP etabliert werden kann.

- **Anmeldung in mobilem Browser ausgehend von Digitales-Amt-App.** Ziel dieser Variante ist es, eine authentifizierte Session zwischen einem Web-Browser, der sich am gleichen Gerät wie die Digitales-Amt-App mit ID-Austria-Komponente befindet, und einem serverseitigen SP herzustellen. Die Benutzer*in befindet sich beim Start des Anmeldeprozesses nicht in diesem Browser, sondern in der Digitales-Amt-App. Dementsprechend greift die Digitales-Amt-App auf eine geschützte Ressource eines serverseitigen SP zu. Der SP erstellt daraufhin einen Authentifizierungs-Request, der über die Digitales-Amt-App und ihre ID-Austria-Komponente an den IDP übermittelt wird. Die Benutzerauthentifizierung am IDP erfolgt über die ID-Austria-Komponente der Digitales-Amt-App. Nach erfolgter Benutzerauthentifizierung erstellt der IDP einen Identitätsnachweis und übermittelt diesen an den SP. Die Benutzer*in wird aus der ID-Austria-Komponente in den Browser weitergeleitet. Dabei wird auch die notwendige Information an den Browser übergeben, über die die authentifizierte Session zwischen dem Browser und dem SP etabliert werden kann.
- **Anmeldung in Browser auf Zweitgerät.** Die Benutzer*in befindet sich in einem Web-Browser, der sich jedoch auf einem anderen Gerät als die Digitales-Amt-App mit ID-Austria-Komponente befindet. Der Browser greift auf eine geschützte Ressource eines serverseitigen SP zu. Der SP erstellt daraufhin einen Authentifizierungs-Request, der an den Browser retourniert und von dort an den IDP übermittelt wird. Die Benutzerauthentifizierung erfolgt im Web-Browser. Nach erfolgter Benutzerauthentifizierung erstellt der IDP einen Identitätsnachweis und übermittelt diesen an den SP. Die Benutzer*in verbleibt während des gesamten Prozesses im Web-Browser.

Die oben gelisteten Varianten ergeben sich ausschließlich durch eine systematische Variation der prinzipiell zur Verfügung stehenden Klassen von Client-Komponenten. Eine weitere Dimension möglicher Varianten wird durch die Verwendung unterschiedlicher Methoden der Authentifizierung gegen den IDP (als Teil der ID Austria) aufgespannt. Konkret kann eine Authentifizierung gegen den IDP über ein, nach Erstellung einer kryptographischen Bindung ausgestelltes Binding-Zertifikat, über den VDA oder über eine eIDAS-konforme europäische elektronische Identität erfolgen.

Die tatsächlich zur Anwendung kommende Art der Benutzerauthentifizierung gegen den IDP ist für Service-Provider jedoch weitgehend[13] transparent. Auf eine weitere Detaillierung und Differenzierung der oben gelisteten Varianten wird an dieser Stelle daher verzichtet.

Abschließend sei darauf hingewiesen, dass die oben beschriebenen Beispiele nur einen Auszug aller theoretisch möglichen Varianten abdecken. Die Beispiele wurden so gewählt, dass die häufigsten und damit relevantesten Varianten abgedeckt sind. Eine Unterstützung für weitere Anmeldevarianten wird im ID-Austria-System laufend ergänzt.

3.3. Weitere Use-Cases

Neben den in den vorigen Abschnitten näher beschriebenen Anmeldeprozessen unterstützt die ID Austria noch eine Reihe weiterer Use-Cases für Benutzer*innen und anderen involvierte Parteien. So können Service-Provider Benutzer*innen auch zur Erstellung einer qualifizierten Signatur auffordern. Diese wird dann über den VDA, der als Teil des ID-Austria-Systems gesehen werden kann, durchgeführt. Auch in Bezug auf die Erstellung qualifizierter elektronischer Signaturen ergeben sich unterschiedliche Varianten abhängig von der verwendeten Client-Komponente und der konkreten Ausformung des Service-Providers. Insgesamt sind Signaturerstellungsprozesse jedoch weniger komplex, da Signaturerstellungs-Requests vom Service-Provider direkt an den VDA gesendet werden können und daher weite Teile des ID-Austria-Systems nicht involviert sind. Aus diesem Grund wird auf Signaturerstellungsprozesse in diesem Whitepaper nicht im Detail eingegangen.

Neben Signaturerstellungsprozessen stehen Benutzer*innen noch eine Reihe weiterer Use-Cases zur Verfügung. Beispielsweise wird Benutzer*innen auch ein Dashboard geboten, über das sie ihre persönliche ID Austria verwalten können. Service-Owner und Service-Provider tangieren diese Prozesse jedoch nur am Rande. Aus diesem Grund werden auch diese Prozesse hier im Rahmen dieses grundlegenden Überblicks über die ID Austria nicht im Detail beschrieben.

[13] Die ID Austria ermöglicht es Service-Providern, die Verwendung des Features zur vereinfachten Weiterverwendung einer zuvor durchgeführten Benutzerauthentifizierung zu limitieren und so eine komplette Authentifizierung über den VDA immer zu erzwingen.

4. Anbindung eines Service-Providers an die ID Austria

Um die ID Austria zur Anmeldung von Benutzer*innen nutzen zu können, müssen Service-Provider in der Lage sein, mit der ID Austria technisch zu interagieren. Die ID Austria stellt dafür definierte technische Schnittstellen basierend auf etablierten Protokollen bereit. Dieses Kapitel beschreibt die notwendigen Schritte zur Anbindung eines Service-Providers an die ID Austria über die vorgesehenen Schnittstellen.

4.1. Voraussetzungen zur Nutzung der ID Austria

Behördliche und private Service-Owner (SO) können die Funktionalität des Logins bzw. der Anmeldung von Benutzer*innen in ihre Service-Provider (SP) wie Web-Applikationen, Apps, etc. an die ID Austria auslagern. Die ID Austria fungiert dementsprechend als Identity-Provider und stellt SP dabei die folgenden Authentifizierungsmöglichkeiten zur Verfügung:

- **Authentifizierung an einem Vertrauensdiensteanbieter (VDA)**: Anmeldung mittels Erstellung einer qualifizierten Signatur bei einem VDA. Die erstellte Signatur dient als Identifikationsmittel gegenüber dem Identity-Provider (IDP) des ID-Austria-Systems.
- **Vereinfachte Weiterverwendung einer Authentifizierung am ID-Austria-System:** Anmeldung am ID-Austria-System mittels eines kryptographischen Bindungszertifikats, das nach der Registrierung der ID Austria zwischen Benutzer*innen, deren mobile Geräte und dem IDP erstellt werden kann. Die vereinfachte Weiterverwendung der ID Austria[14] ist gemäß E-Government-Gesetz (EGovG) umgesetzt.
- **Authentifizierung über eIDAS:** Anmeldung via grenzübergreifenden eIDAS-Framework für Benutzer*innen mit ausländischen elektronischen Identitäten (eID). Nur registrierte und akkreditierte Service-Provider können die ID Austria zur Anmeldung von Benutzer*innen verwenden. Hier ergibt sich somit ein eklatanter Unterschied zum bisherigen System basierend auf Bürgerkarte und Handy-Signatur.

Über die Registrierung erhält die ID Austria alle notwendigen Informationen zur Kommunikation mit dem SP. Basierend auf diesen Informationen kann die ID Austria für den SP und seine Applikation diverse Policies definieren, wie bspw. die Befugnis zur Abfrage von unverschlüsselten bzw. verschlüsselten bereichsspezifischen Personenkennzeichen (bPK) diverser Bereiche oder bestimmter Attribute aus behördlichen oder privaten Registern. Im Zuge des Registrierungsprozesses eines SP wird so festgelegt, welche Attribute die ID Austria dem Service-Owner (bzw. dessen Service-Providern) bereitstellt. Über den minimalen Datensatz ((v)bPKs, Name, Geburtsdatum) hinausgehende Attribute werden dabei auch von anderen Attribute-Providern (z.B. behördliche oder private Register) bezogen.

Zusammenfassend kann somit festgehalten werden, dass die ID Austria prinzipiell allen Service-Ownern und Service-Providern offensteht. Dies gilt sowohl für Service-Owner des öffentlichen als auch des privaten Sektors. Eine Verwendung der ID Austria bedingt jedoch eine vorhergehende Registrierung und Akkreditierung des Service-Providers und auch der für den Service-Provider verantwortlichen Service-

[14] Vereinfachte Weiterverwendung: https://www.parlament.gv.at/PAKT/VHG/XXVII/ME/ME_00056/index.shtml

Owner. Nachfolgend wird die Registrierung für öffentliche- und private Service-Provider näher beschrieben.

4.2. Registrierung und Akkreditierung

Die Notwendigkeit einer Registrierung (und Akkreditierung) von Service-Ownern und Service-Providern ist einer jener Aspekte, in denen sich die ID Austria signifikant vom bisherigen Bürgerkarte-/Handy-Signatur-System unterscheidet. Die vorgeschriebene Registrierung und Akkreditierung aller Service-Provider (und ihrer Service-Owner), welche die ID Austria nutzen möchten hat zum Ziel, die Vertrauenswürdigkeit in das System insgesamt zu erhöhen. Durch den vorgesehenen Registrierungs-/Akkreditierungsprozess können Service-Provider mit unlauteren Agenden vom System ausgeschlossen werden. Gleichzeitig kann zum Beispiel auch kontrolliert werden, dass Service-Provider tatsächlich nur jene Daten (Attribute) zu Benutzer*innen erhalten, die sie für das angebotene Service tatsächlich benötigen. Die Notwendigkeit einer Registrierung und Akkreditierung trägt somit insgesamt zur Sicherheit der ID Austria und zum Schutz der Daten der Benutzer*innen bei.

Wie erwähnt gliedert sich der Registrierungsprozess eines Service-Providers in die folgenden zwei Teile:

- **Registrierung des Service-Providers.** Im Zuge dieses Prozesses gibt der Service-Owner technische und organisatorische Daten zum Service-Provider an, der an die ID Austria angebunden werden soll. Dies inkludiert unter anderem auch die technischen Metadaten zur Anbindung des Service-Providers über die Protokolle SAML2 oder OIDC.
- **Akkreditierung des Service-Providers.** Wurden alle notwendigen Daten zum Service-Provider vollständig angegeben, folgt die Akkreditierung. Diese wird vom BM.I durchgeführt. Im Zuge der Akkreditierung werden die Daten des Service-Providers auf Korrektheit und Plausibilität geprüft. Sind alle Daten in Ordnung, wir der Service-Provider akkreditiert, d.h. für die Verwendung der ID Austria freigeschalten.

Damit ein Service-Owner eigene Service-Provider registrieren kann (und diese in weiterer Folge durch das BM.I akkreditiert werden können), muss sich der Service-Owner zunächst selbst registrieren. Nur registrierte – und damit im System bekannte – Service-Owner können ihrerseits Service-Provider registrieren.

Prinzipiell kann zwischen privatwirtschaftlichen und öffentlichen Service-Providern unterschieden werden. Während alle Service-Provider beider Kategorien immer zunächst registriert werden müssen, ergibt sich in Bezug auf die Akkreditierung ein Unterschied zwischen den beiden Kategorien. Konkret muss die Akkreditierung in der oben beschriebenen Form nur von privatwirtschaftlichen Service-Providern durchlaufen werden. Für Service-Provider des öffentlichen Sektors erfolgt eine automatische Akkreditierung nach erfolgreicher Registrierung. Für Service-Provider des öffentlichen Sektors werden angegebene Registrierungsdaten jedoch im Nachhinein stichprobenartig geprüft.

Die technische Umsetzung der notwendigen Registrierungs- und Akkreditierungsprozesse basiert auf existierender Infrastruktur. So können privatwirtschaftliche Service-Owner notwendige Registrierungsprozesse über das Unternehmensserviceportal (USP) vornehmen. Für Service-Owner des öffentlichen Sektors steht eine PVP-basierte Lösung zur Verfügung.

Aktuelle Informationen bezüglich der relevanten Registrierungs- und Akkreditierungsprozesse können unter anderem der Website https://eid.egiz.gv.at entnommen werden. Nachfolgend wird die Registrierung für öffentliche- und private Service-Provider näher beschrieben.

4.2.1. Registrierung von öffentlichen Service-Providern

Die Registrierung und Verwaltung von öffentlichen Service-Providern durch oder im Auftrag des Service-Owners, erfolgt über das ID Austria SP Registrierungssystem (IDA-SPR) des ID-Austria-Systems. Hierfür bietet das IDA-SPR einen Zugang als behördenübergreifende Webanwendung entsprechend den Vorgaben des Portalverbunds[15] der österreichischen Behörden. Das IDA-SPR wurde bereits in der Portalverbund-AnwendungsInformation[16] (PAI) veröffentlicht und steht somit den Portalverbundteilnehmer*innen zur Verfügung. Das IDA-SPR steht sowohl für das Produktivsystem als auch für das Testsystem der ID Austria zur Verfügung. Behördliche Organisationen (Service-Owner) können das IDA-SPR an ihrem bestehenden Stammportal (STP) registrieren und erhalten somit direkten Zugriff auf das IDA-SPR um ihre Anwendungen am ID-Austria-System zu verwalten.

Der Zugriff auf das IDA-SPR erfolgt unter Verwendung des Portalverbundprotokolls (PVP), wobei alle für die Integration notwendigen Informationen sowie das Betriebshandbuch über die PAI verfügbar sind. Nach einer erfolgreichen Anmeldung am IDA-SPR werden die aktuell registrierten Service-Provider des jeweiligen Service-Owners, sofern vorhanden, dargestellt. Danach können sowohl bestehende Service-Provider verwaltet bzw. geändert als auch neue Service-Provider angelegt werden. Bereits registrierte Service-Provider können über das IDA-SPR verwaltet werden. Diese Verwaltung umfasst sowohl die Aktivierung bzw. Deaktivierung der Anwendung als auch die Konfiguration und Änderung von Anwendungsparametern. Hierfür können unterschiedliche Versionen eines Service-Providers erstellt werden, wobei jedoch immer nur exakt eine Version einer Anwendung aktiv sein kann.

Aktuelle Informationen zum Registrierungsprozess von öffentlichen bzw. behördlichen Service-Providern können der ID-Austria-Website unter folgendem Link entnommen werden:

https://eid.egiz.gv.at/anbindung/registrierung/registrierung-von-behoerdlichen-service-providern/

4.2.2. Registrierung von privaten Service-Providern

Private Unternehmen können ihre Service-Provider über das Unternehmensserviceportal (USP) verwalten. Hierfür bietet das USP einen Zugriff auf das IDA-SPR des ID-Austria-Systems. Die Neuregistrierung von privaten Service-Providern am produktiven ID-Austria-System erfordert einen Akkreditierungsprozess. Im Zuge dieser Akkreditierung werden sowohl technische als auch organisatorische Parameter validiert. Die Aktivierung der Anwendung kann nur nach einer positiven Akkreditierung durchgeführt werden.

Zur Verwaltung von Service-Providern stellt das USP den Zugriff auf die Verwaltungsapplikation (IDA-SPR) bereit. Um Zugriff auf das IDA-SPR zu erhalten, muss einem Mitarbeiter des Service-Owners der Zugriff auf das IDA-SPR zugeordnet werden. Zu beachten ist, dass auch eine Anpassung eines bestehenden Service-

[15] Portalverbund: https://neu.ref.wien.gv.at/at.gv.wien.ref-live/web/reference-server/ag-iz-portalverbund
[16] Portalverbund-AnwendungsInformationen: https://portal.lfrz.at/at.gv.lfrz.pai-p//application_summary

Providers eine Neuakkreditierung erfordern kann, sofern die Änderungen zuvor akkreditierte Daten betreffen.

Aktuelle Informationen zum Registrierungsprozess von privaten Service-Providern können der ID-Austria-Website unter folgendem Link entnommen werden:

https://eid.egiz.gv.at/anbindung/registrierung/registrierung-von-privaten-service-providern/

4.2.3. Erstellung und Aktivierung eines Service-Providers

Im Zuge der Registrierung eines Service Providers am IDA-SPR, erhält das ID-Austria-System alle für die Anbindung erforderlichen Informationen. Hierbei handelt es sich sowohl um technische Kommunikationsparameter zwischen dem Service-Provider und dem Identity-Provider des ID-Austria-Systems, als auch organisatorische Festlegungen wie bspw. die gewünschten Attribute, die vom ID-Austria-System für den jeweiligen Service-Provider (bzw. dessen Applikation) bereitgestellt werden sollen.

Als erstes müssen die notwendigen Service-Provider-Daten in der Konfigurationsoberfläche des Registrierungssystems als Entwurf angegeben werden. Dieser Entwurf kann vom Service-Owner gespeichert und dadurch von der Konfigurationsoberfläche automatisch technisch geprüft werden. Öffentliche Service-Provider wechseln hiernach automatisch in den akkreditierten Zustand. Service-Owner eines privatwirtschaftlichen Service-Providers können die Akkreditierung per Button-Klick manuell veranlassen. Nach einer erfolgreichen Akkreditierung kann der Service-Provider schließlich aktiviert werden und steht nach der Aktivierung für Benutzer*innen mit ID-Austria-Login zur Verfügung.

Für allfällige Änderungen der Service-Provider-Daten besteht die Möglichkeit, den Service-Provider zu duplizieren und die erforderlichen Daten in einem neuen Entwurf zu ändern. Hierbei ist zu beachten, dass eine Änderung von bereits akkreditierten Service-Provider-Daten eine neue Akkreditierung und einen erneuten Durchlauf des Aktivierungsprozesses erfordert. Eine Darstellung der möglichen Zustände eines Service-Providers und der möglichen Aktionen eines Service-Owners im IDA-SPR wird in Abbildung 2 geboten.

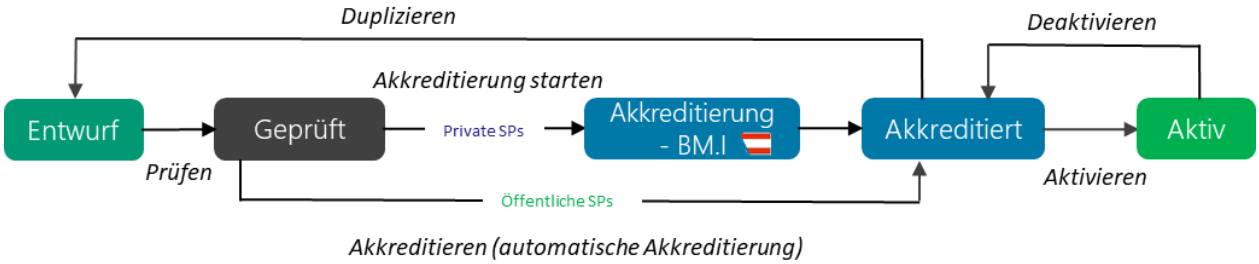

Abbildung 2. Erstellung und Aktivierung eines Service-Providers im IDA-SPR

4.3. Technische Anbindung

Aus Sicht der Service-Provider stellt die ID Austria einen Identity-Provider dar. Die sich dahinter verbergenden Komplexität mag aufgrund der Eigenheiten des österreichischen nationalen Identitätsmanagementsystems beträchtlich sein, die Funktion der ID Austria entspricht für Service-Provider jedoch im Prinzip jener eines herkömmlichen Identity-Provider. Dementsprechend besteht die Interaktion mit der ID Austria im Zuge von Anmeldeprozessen für Service-Provider aus den folgenden Schritten:

- **Initiierung der Benutzerauthentifizierung.** Der Service-Provider übermittelt an die ID Austria einen Authentifizierungs-Request. Im Zuge der Übermittlung dieses Request wird die Benutzer*in an die ID Austria weitergeleitet.
- **Durchführung der Benutzerauthentifizierung.** Die ID Austria authentifiziert die Benutzer*in und ermittelt alle vom Service-Provider über den Authentifizierungs-Request angeforderten Attribute.
- **Anmeldung der Benutzer*in.** Die ID Austria übermittelt die angeforderten Attribute dem Service-Provider über eine signierte Authentifizierungs-Response. Der Service-Provider kann diese Response und die darin enthaltenen Attribute verwenden, um die Benutzer*in anzumelden.

Trotz der Komplexität des Gesamtsystems der ID Austria ist die Interaktion mit Service-Providern relativ einfach. Zur Kommunikation mit Service-Providern, d.h. zur Entgegennahme von Authentifizierungs-Requests und zur Retournierung von Authentifizierungs-Responses, vertraut die ID Austria auf die bewährten Identitätsmanagementprotokolle SAML2 und Open ID Connect (OIDC). Service-Provider können also eines dieser beiden Protokolle wählen, um mit der ID Austria als Identity-Provider zu interagieren. Die nachfolgenden Unterabschnitte gehen auf relevante Details zur technischen Anbindung von Service-Providern an die ID Austria über diese beiden Protokolle näher ein.

Wichtig ist in diesem Zusammenhang, dass die ID Austria das veraltete Protokoll SAML1 nicht mehr unterstützt. Service-Provider, die noch auf dem SAML1-Identitätsprotokoll basieren, können für die beschränkte Dauer einer Übergangsphase eine neu bereitgestellte Proxy-Funktion von MOA-ID nutzen, um Anmeldeprozesse über die ID Austria zu integrieren. Der Service-Provider kann wie bisher SAML1-basierte Authentifizierungs-Requests an die MOA-ID-Instanz des Service-Owners absetzen. MOA-ID wandelt diese in einen entsprechenden SAML2-Request um und sendet diesen an die ID Austria. Die von der ID Austria erhaltene SAML2-Response wird wiederum von MOA-ID entgegengenommen, in eine SAML1-Response umgewandelt und dem Service-Provider retourniert. Voraussetzung zur Nutzung dieser Proxy-Funktion von MOA-ID ist ein Upgrade auf die aktuelle Version, wodurch aus MOA-ID der sogenannte MOA E-ID Proxy wird.

4.3.1. Anbindung via SAML2

Eine Anbindung via SAML2 ist primär für webbasierte Service-Provider (z.B. Web-Applikationen) vorgesehen, auf die von Benutzer*innen über einen Web-Browser zugegriffen wird. Im Kontext webbasierter Lösungen hat sich der Einsatz von SAML2 bewährt. Ein Einsatz von SAML2 ist prinzipiell auch

für Service-Provider basierend auf mobilen Apps denkbar. Im Kontext mobiler Applikationen hat sich in den letzten Jahren jedoch OIDC zum de-facto Standard entwickelt. Eine Verwendung von SAML2 scheint hier daher aufgrund des Mangels einschlägiger Bibliotheken weniger zielführend.

Für eine erfolgreiche Interaktion zwischen ID Austria und Service-Provider müssen die Voraussetzungen zur Nutzung, wie in Abschnitt 4.1 beschrieben, erfüllt sein. Eine Grundvoraussetzung ist, dass der Service-Provider (und auch der verantwortliche Service-Owner) bei der ID Austria registriert und akkreditiert sind. Nur nach erfolgreicher Registrierung sind der ID Austria alle technischen Informationen (SAML2-Metadaten, etc.) bekannt, um mit dem Service-Provider interagieren zu können.

4.3.1.1. SAML2-basierter Authentifizierungsprozess

Die SAML2-Spezifikation legt im Wesentlichen fest, wie Service-Provider die Benutzerauthentifizierung durch Absetzen eines entsprechenden Authentifizierungs-Request an einen Identity-Provider delegieren können und wie der Identity-Provider nach durchgeführter Benutzerauthentifizierung die Attribute der Benutzer*in an den Service-Provider retourniert. SAML2 definiert dafür verschiedene Protokollvarianten, von denen bewusst nicht alle durch die ID Austria unterstützt werden. Dieser Abschnitt illustriert daher anhand eines beispielhaften Authentifizierungsprozesses die vorgesehene Interaktion zwischen ID Austria und Service-Provider.

Der gesamte SAML2-basierte Authentifizierungsprozess ist in der ID Austria gemäß dem Portalverbund PVP2 S-Profil[17] umgesetzt. Um Benutzer*innen zu authentifizieren, muss der SP einen SAML2 Authentifizierungs-Request erstellen, der an den Browser der Benutzer*in retourniert wird. Der Browser folgt dem Authentifizierungs-Redirect und sendet den SAML2-Request an die ID Austria, konkret an den Identity-Provider (IDP) des ID-Austria-Systems. Hierfür werden durch den Identity-Provider des ID-Austria-Systems sowohl SAML2 POST-Binding als auch SAML2 Redirect-Binding unterstützt.

Im Folgenden werden zum besseren Verständnis die relevanten Schritte eines SAML2-basierten Authentifizierungsprozesses unter Verwendung des SAML2 POST-Binding dargestellt. Im Folgenden wird dazu zunächst die Übermittlung des SAML2-basierten Authentifizierungs-Request über den Web-Browser der Bürger*in an das ID-Austria-System illustriert.

```
POST https://eid.oesterreich.gv.at/auth/idp/profile/SAML2/POST/SSO HTTP/1.1
Host: eid.oesterreich.gv.at
```

Im Body des HTTP-POST-Requests wird der Authentifizierungs-Request („SAMLRequest“) entsprechend der SAML2-POST-Binding-Spezifikation übermittelt. Der Request wird dabei Base64-kodiert übertragen. Dies ist im Folgenden für einen beispielhaften SAML2-Authentifizierungs-Request dargestellt.


```
SAMLRequest=
PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48c2FtbDJwOkF1dGhuUmVxdWVzdCB4bWxuczpzYW
1sMnA9InVybjpvYXNpczpuYW1lczp0YzpTQU1MOjIuMDpwcm90b2NvbCIgQXNzZXJ0aW9uQ29uc3VtZXJTZXJ2aWNl
SW5kZXg9IjAiIEF0dHJpYnV0ZUNvbnN1bWluZ1NlcnZpY2VJbmRleD0iMCIgRGVzdGluYXRpb249Imh0dHBzOi8vZW
lkLm9lc3RlcnJlaWNoLmd2LmF0L2F1dGgvaWRwL3Byb2ZpbGUvU0FNTDIvUE9TVC9TU08iIElEPSJfMTU1NjBkYzY2
```


[17] https://neu.ref.wien.gv.at/at.gv.wien.ref-live/documents/20189/79677/PVP2-S-Profil_2_1_3_20171020.pdf/e35fd2ee-9b86-42f4-8daf-18fdfcdae28e?version=1.0

```
ZTJhZTAxNzZjNjc5OWUzNGFhYTYwNGUiIElzc3VlSW5zdGFudD0iMjAyMS0wMS0xNFQxNjoyODozMS4yMzBaIiBWZX
JzaW9uPSIyLjAiPjxzYW1sMjpJc3N1ZXIgeG1sbnM6c2FtbDI9InVybjpvYXNpczpuYW1lczp0YzpTQU1MOjIuMDph
c3NlcnRpb24iIEZvcm1hdD0idXJuOm9hc2lzOm5hbWVzOnRjOlNBTUw6Mi4wOm5hbWVpZC1mb3JtYXQ6ZW50aXR5Ij
5odHRwczovL2VpZC5lZ2l6Lmd2LmF0L2VpZHBpbG90L3NlcnZsZXQvbWV0YWRhdGE8L3NhbWwyOklzc3Vlcj48ZHM6
U2lnbmF0dXJlIHhtbG5zOmRzPSJodHRwOi8vd3d3LnczLm9yZy8yMDAwLzA5L3htbGRzaWcjIj48ZHM6U2lnbmVkSW
5mbz48ZHM6Q2Fub25pY2FsaXphdGlvbk1ldGhvZCBBbGdvcml0aG09Imh0dHA6Ly93d3cudzMub3JnLzIwMDEvMTAv
eG1sLWV4Yy1jMTRuIyIvPjxkczpTaWduYXR1cmVNZXRob2QgQWxnb3JpdGhtPSJodHRwOi8vd3d3LnczLm9yZy8yMD
AwLzA5L3htbGRzaWcjcnNhLXNoYTEiLz48ZHM6UmVmZXJlbmNlIFVSST0iI18xNTU2MGRjNjZlMmFlMDE3NmM2Nzk5
ZTM0YWFhNjA0ZSI+PGRzOlRyYW5zZm9ybXM+PGRzOlRyYW5zZm9ybSBBbGdvcml0aG09Imh0dHA6Ly93d3cudzMub3
JnLzIwMDAvMDkveG1sZHNpZyNlbnZlbG9wZWQtc2lnbmF0dXJlIi8+PGRzOlRyYW5zZm9ybSBBbGdvcml0aG09Imh0
dHA6Ly93d3cudzMub3JnLzIwMDEvMTAveG1sLWV4Yy1jMTRuIyIvPjwvZHM6VHJhbnNmb3Jtcz48ZHM6RGlnZXN0TW
V0aG9kIEFsZ29yaXRobT0iaHR0cDovL3d3dy53My5vcmcvMjAwMC8wOS94bWxkc2lnI3NoYTEiLz48ZHM6RGlnZXN0
VmFsdWU+elZ4SGFzdmhsZzNTNkoyekw0b3cvcmlrdG93PTwvZHM6RGlnZXN0VmFsdWU+PC9kczpSZWZlcmVuY2U+PC
9kczpTaWduZWRJbmZvPjxkczpTaWduYXR1cmVWYWx1ZT5RUzFJcFRKY1FkOU51eTVuWlE5dHdmVnN6WVlzV096OXh6
YW9QUWxDcFRBK3d0MHZmS0p2cWQ1M1R2TmpkMjNiQ1hnSllIME9ZaUJWV2hiREh4cXk3S0paejBWSEplM3YxczNHMm
s4SDZ2UWNQL3RwVkFJdWpEL0tLNXJGZzFLTWplNWRwckU5Y1RxUUdtd1ZjaDdFSzdhcEgzUVhKY3dXRTBESFdmM3FQ
K2F6UjErNE9LdmtNNVA2Rm92dkl6Z3dMczhQUGNaWkRSVHBGV0dSSlJ4MHNONXFHdWk1NG9LbUo4Mkc4c09rcXNRWm
hTbnN2TlNVUFZpM3ZkZUR2R20yQzdwVnlIL1dtTWxoVTNjYnlIUVZRRk5Ob0l5NXQwZTB5ZEFKcWk0VWg0VFFnZHJR
Y25BdDgzTmszUFJZK0x2aGNxb1hLWDA4dHU1Y21yODdOTXlTd3c9PTwvZHM6U2lnbmF0dXJlVmFsdWU+PGRzOktleU
luZm8+PGRzOktleVZhbHVlPjxkczpSU0FLZXlWYWx1ZT48ZHM6TW9kdWx1cz5uUFFhQnNXb3Q3R1dGRmZHcjFlVlUz
RG9mN0YvZkpDRGlLSng1RGpacGZvT2pMYlNwTHlER3AyaDAxSzFTNWpxS2orWUJKcVlsYXJ0CmpoL0tNU3hNZU1LQ0
xja0ZHclkzdGdhZlNFa1R0ZlhIQko1a0VIc1FjRlZVOFNHZjBFNllTWlllTDdPU2NJc0lGQzNTcEh3NFQ1dFUKelZj
SHpPSXNDdk93WFo0eVdudlVSQkV1QWY3ZEtmY3RkTGNJQXlyWkVBUE5VdVZMSUtBdFZQL29BYlVkaFBnQk9LdkJrTD
E4MnNrVwpIQ3orWWY0WnVCZVBNb1QvNm5vTzFJaEhVc1Fsa0RtampFMkJVdk5ObWIrTExSSkZlNE9BdnNvUGNHeW45
bS9IT09QTmp1TEsxdjB1CmdkeXZsOWtTWUJWSFdMWUdTQXUvTk1UK2NNWi9xRGlETWVwSHJRPT08L2RzOk1vZHVsdX
M+PGRzOkV4cG9uZW50PkFRQUI8L2RzOkV4cG9uZW50PjwvZHM6UlNBS2V5VmFsdWU+PC9kczpLZXlWYWx1ZT48L2Rz
OktleUluZm8+PC9kczpTaWduYXR1cmU+PC9zYW1sMnA6QXV0aG5SZXF1ZXN0Pg==
```


Ergänzend dazu zeigt folgende Darstellung denselben exemplarischen SAML2-Authentifizierungs-Request Base64-dekodiert im XML-Format.


```
<saml2p:AuthnRequest AssertionConsumerServiceIndex="0" AttributeConsumingServiceIndex="0"
Destination="https://eid.oesterreich.gv.at/auth/idp/profile/SAML2/POST/SSO"
ID="_15560dc66e2ae0176c6799e34aaa604e" IssueInstant="2021-01-14T16:28:31.230Z"
Version="2.0">
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">https://eid.egiz.gv.at/eidpilot/servlet/metadata</saml2:Issuer>
  <ds:Signature>
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <ds:Reference URI="#_15560dc66e2ae0176c6799e34aaa604e">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue>zVxHasvhlg3S6J2zL4ow/riktow=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>
QS1IpTJcQd9Nuy5nZQ9twfVszYYsWOz9xzaoPQlCpTA+wt0vfKJvqd53TvNjd23bCXgJYH0OYiBVWhbDHxqy7KJZz0
VHJe3v1s3G2k8H6vQcP/tpVAIujD/KK5rFg1KMje5dprE9cTqQGmwVch7EK7apH3QXJcwWE0DHWf3qP+azR1+4OKvk
M5P6FovvIzgwLs8PPcZZDRTpFWGRJRx0sN5qGui54oKmJ82G8sOkqsQZhSnsvNSUPVi3vdeDvGm2C7pVyH/WmMlhU3
cbyHQVQFNNoIy5t0e0ydAJqi4Uh4TQgdrQcnAt83Nk3PRY+LvhcqoXKX08tu5cmr87NMySww==
    </ds:SignatureValue>
    <ds:KeyInfo>
      <ds:KeyValue>
        <ds:RSAKeyValue>
          <ds:Modulus>
nPQaBsWot7GWFFfGr1eVU3Dof7F/fJCDiKJx5DjZpfoOjLbSpLyDGp2h01K1S5jqKj+YBJqYlart
jh/KMSxMeMKCLckFGrY3tgagSEkTtfXHBJ5kEHsQcFVU8SGf0E6YSZYeL7OScIsIFC3SpHw4T5tU
zVcHzOIsCvOwXZ4yWnvURBEuAf7dKfctdLcIAyrZEAPNUuVLIKAtVP/oAbUdhPgBOKvBkL182skW
```

```
HCz+Yf4ZuBePMoT/6noO1IhHUsQlkDmjjE2BUvNNmb+LLRJFe4OAvsoPcGyn9m/HOOPNjuLK1v0u
gdyvl9kSYBVHWLYGSAu/NMT+cMZ/qDiDMepHrQ==
          </ds:Modulus>
          <ds:Exponent>AQAB</ds:Exponent>
        </ds:RSAKeyValue>
      </ds:KeyValue>
    </ds:KeyInfo>
  </ds:Signature>
</saml2p:AuthnRequest>
```


Die ID Austria übermittelt anschließend eine Auswahl der zur Verfügung stehenden Authentifizierungsmethoden (Abbildung 3) an den Web-Browser. Neben einer Authentifizierung über die persönliche ID Austria können Benutzer*innen derzeit auch noch eine Authentifizierung mit einer bestehenden persönlichen Handy-Signatur wählen. Für Benutzer*innen mit ausländischer eID steht zudem die Variante einer Anmeldung über das eIDAS-Framework zur Verfügung („Anmeldung mit EU-Login“).

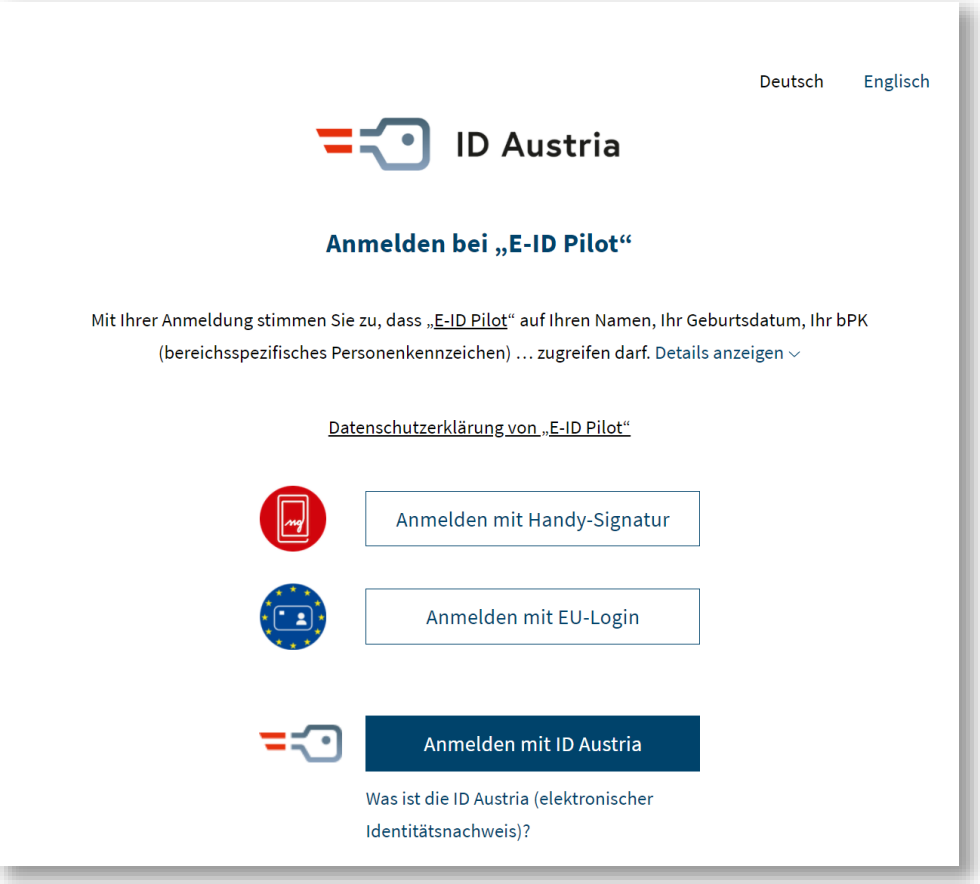

Abbildung 3.Auswahl der Authentifizierungsmethode.

Anschließend führt die Benutzer*in die gewählte Authentifizierungsmethode (z.B. via ID Austria) über ihren Web-Browser durch. Nach erfolgreicher Benutzerauthentifizierung erstellt die ID Austria eine SAML2-Assertion, d.h. eine signierte Datenstruktur, die u.a. die Attribute der Benutzer*in enthält. Die

SAML2-Assertion wird von der ID Austria verschlüsselt über eine Authentifizierungs-Response an den Browser der Benutzer*in übermittelt.

Im Folgenden ist ein Beispiel für eine SAML2-basierten Authentifizierungs-Response gegeben, die an den Web-Browser der Bürger*in retourniert wird.

```
HTTP/1.1 200 OK
SAMLResponse:
"PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPHNhbWwycDpSZXNwb25zZSBEZXN0aW5hdGlvb
j0ia..."
```

Der Browser sendet die erhaltene SAML2-Authentifizierungs-Response entsprechend dem in diesem Beispiel verwendeten SAML2-POST-Binding mittels HTTP-POST-Request an den Service Provider. Dies ist im Folgenden beispielhaft dargestellt.

```
POST https://beispielService.at/saml2/ HTTP/1.1
Host: beispielService.at
```

Im Body des HTTP-POST-Request wird die SAML2-Authentifizierungs-Response über den Parameter „SAMLResponse“ übermittelt. Die SAML2-Authentifizierungs-Response wird dabei Base64-kodiert übertragen. Dies ist im Folgenden illustriert.

```
SAMLResponse=PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz48c2...
```

Ein vollständiges Beispiel für eine bereits Base64-dekodierte und entschlüsselte SAML2-Authentifizierungs-Response ist im Folgenden gegeben.

```
<saml2p:Response Destination="https://eid.egiz.gv.at/saml2_demo/demoapplication"
ID="_a5ea22f2c448bc8aee96bf97a9ba1ea0" InResponseTo="_a67f2dca9cb921099f82835205e8f53d"
IssueInstant="2021-01-15T08:23:36.688Z" Version="2.0">
  <saml2:Issuer>https://eid.egiz.gv.at/idp/shibboleth</saml2:Issuer>
  <ds:Signature>
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
      <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
      <ds:Reference URI="#_a5ea22f2c448bc8aee96bf97a9ba1ea0">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <ds:DigestValue/>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue/>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>
MIIDKzCCAhMCBFrxKO4wDQYJKoZIhvcNAQELBQAwWjELMAkGA1UEBhMCQVQxDTALBgNVBAoMBEVH
SVoxGDAWBgNVBAsMD2RlbW8uZWdpei5ndi5hdDEiMCAGA1UEAwwZTU9BLUlEIElEUCAoVGVzdC1W
ZXJzaW9uKTAeFw0xODA1MDgwNDM0NTRaFw0yMTAxMzEwNDM0NTRaMFoxCzAJBgNVBAYTAkFUMQ0w
```

```
CwYDVQQKDARFR0laMRgwFgYDVQQLDA9kZW1vLmVnaXouZ3YuYXQxIjAgBgNVBAMMGU1PQS1JRCBJ
RFAgKFRlc3QtVmVyc2lvbikwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCaFnqoaYoq
UptenemC6FiVDg5F2hEjpjix8+ow6/6QhUl2cPOS0uwZHaIvwT/RVbJ9CPdil6+11qaCPfZ+FoY+
M+ke7TRd2RS1DqFbe1KC0imEnwemyLQrYe5Pm7DNcaY/kHTTq+k0eeGbYH0U/Iopyi0VuN5OWl4F
Vg45pf7knhXkaimItdjnCXnKcYM91mmltCf6TDgUrz7US7PmgvinnhfBgdITAT4GRr4ehliT+/jt
1OzHEyWRHanBGIpXNeZNqxgnpnGtaDh4JZuYR8qfH+GRK6dtW2ziej6rGIiUElGVCkXsohgxMNzq
nWeD9JT8+yyp1XZlyQf+IxhhESQLAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAIFejAFQepaEl/kC
VLvidMR+MXq5LCGHthUiI6eDTQZ+H7lZdHlj547XwEdX15b6Md3h7eSJ4hwlfV4go/0FaoLPzvVq
itwtYY5htywB3B6ZV34Eyi6C59Gl34XrV8CWxH4KKwLsVAjAy+/p/Xh0q2pzSBkeOChzBMBkjmyc
2Ue4MEKdL9guzp6+Yc/HL/phHAKYapkVyFwvsdqWOgyRzxAHINko8ExImMMB3xB5a52kfqLcui5O
fzEhjwLFJaGBMmFCmFGGOUwtIvl/6ZQ2LLzOE9+giVK9WsIgH11Pu+ejPFAbXf8cf4oWhbAfTkiy
4jpXrp77JXFRSDWddb0yePc=
        </ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </ds:Signature>
  <saml2p:Status>
    <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </saml2p:Status>
  <saml2:Assertion ID="_dc30d5f516599e113e5e9df666ed9bc3" IssueInstant="2021-01-
15T08:23:36.688Z" Version="2.0">
    <saml2:Issuer>https://eid.egiz.gv.at/idp/shibboleth</saml2:Issuer>
    <ds:Signature>
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256"/>
        <ds:Reference URI="#_dc30d5f516599e113e5e9df666ed9bc3">
          <ds:Transforms>
            <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>
          <ds:DigestValue>B0HMy15fIOZhjd+rFNgOdWhufI3CFfPn1CavYpzr5N0=
          </ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>
FMs24jNUZonFdRZYo+euAAcYM2TGXvbfrowH8FRjnM6IkxnIfxCORkBXlKKz+ydcAKR73KskgvQU6jo9h4pdJikh8k
fDGVd1kLZG/y3aqWV2m5DcJg286lXdnDE7x6pRUE4MNFm6yhRopfXlbUVLC1VfjC5x/Ug7UThGdYPNpaDbzFaHOhfS
UPifr8LXOXgLU2Aps93C5/0a+gQwbZgM5zkGmWHLhN2j2mcVqRx28Q693uouNkDmijVUaZD97EmRTy1t/Sa+UAhu/t
wKQ3O2BcqSTvzCd0/VPFUoDJW0QiRb3uX/5r7lpNFN93iohym9GifdlLQBICwRdS3+XDpyGw==
      </ds:SignatureValue>
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>
MIIDKzCCAhMCBFrxKO4wDQYJKoZIhvcNAQELBQAwWjELMAkGA1UEBhMCQVQxDTALBgNVBAoMBEVH
SVoxGDAWBgNVBAsMD2RlbW8uZWdpei5ndi5hdDEiMCAGA1UEAwwZTU9BLUlEIElEUCAoVGVzdC1W
ZXJzaW9uKTAeFw0xODA1MDgwNDM0NTRaFw0yMTAxMzEwNDM0NTRaMFoxCzAJBgNVBAYTAkFUMQ0w
CwYDVQQKDARFR0laMRgwFgYDVQQLDA9kZW1vLmVnaXouZ3YuYXQxIjAgBgNVBAMMGU1PQS1JRCBJ
RFAgKFRlc3QtVmVyc2lvbikwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCaFnqoaYoq
UptenemC6FiVDg5F2hEjpjix8+ow6/6QhUl2cPOS0uwZHaIvwT/RVbJ9CPdil6+11qaCPfZ+FoY+
M+ke7TRd2RS1DqFbe1KC0imEnwemyLQrYe5Pm7DNcaY/kHTTq+k0eeGbYH0U/Iopyi0VuN5OWl4F
Vg45pf7knhXkaimItdjnCXnKcYM91mmltCf6TDgUrz7US7PmgvinnhfBgdITAT4GRr4ehliT+/jt
1OzHEyWRHanBGIpXNeZNqxgnpnGtaDh4JZuYR8qfH+GRK6dtW2ziej6rGIiUElGVCkXsohgxMNzq
nWeD9JT8+yyp1XZlyQf+IxhhESQLAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAIFejAFQepaEl/kC
VLvidMR+MXq5LCGHthUiI6eDTQZ+H7lZdHlj547XwEdX15b6Md3h7eSJ4hwlfV4go/0FaoLPzvVq
itwtYY5htywB3B6ZV34Eyi6C59Gl34XrV8CWxH4KKwLsVAjAy+/p/Xh0q2pzSBkeOChzBMBkjmyc
2Ue4MEKdL9guzp6+Yc/HL/phHAKYapkVyFwvsdqWOgyRzxAHINko8ExImMMB3xB5a52kfqLcui5O
fzEhjwLFJaGBMmFCmFGGOUwtIvl/6ZQ2LLzOE9+giVK9WsIgH11Pu+ejPFAbXf8cf4oWhbAfTkiy
4jpXrp77JXFRSDWddb0yePc=
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </ds:Signature>
    <saml2:Subject>
```

```
      <saml2:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
NameQualifier="https://eid.egiz.gv.at/idp/shibboleth"
SPNameQualifier="https://eid.egiz.gv.at/saml2_demo/">VWSYPP3SQ7WNRSHSISQ4I6KWFRUXHNPP
      </saml2:NameID>
      <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <saml2:SubjectConfirmationData Address="129.27.152.209"
InResponseTo="_a67f2dca9cb921099f82835205e8f53d" NotOnOrAfter="2021-01-15T08:28:36.733Z"
Recipient="https://eid.egiz.gv.at/saml2_demo/demoapplication"/>
      </saml2:SubjectConfirmation>
    </saml2:Subject>
    <saml2:Conditions NotBefore="2021-01-15T08:23:36.688Z" NotOnOrAfter="2021-01-
15T08:28:36.688Z">
      <saml2:AudienceRestriction>
        <saml2:Audience>https://eid.egiz.gv.at/saml2_demo/</saml2:Audience>
      </saml2:AudienceRestriction>
    </saml2:Conditions>
    <saml2:AuthnStatement AuthnInstant="2021-01-15T08:23:36.444Z"
SessionIndex="_d928375d88bdf664033f3fb97dbe3320">
      <saml2:SubjectLocality Address="129.27.152.209"/>
      <saml2:AuthnContext>
        <saml2:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
        </saml2:AuthnContextClassRef>
      </saml2:AuthnContext>
    </saml2:AuthnStatement>
    <saml2:AttributeStatement>
      <saml2:Attribute FriendlyName="BPK" Name="urn:oid:1.2.40.0.10.2.1.1.149"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml2:AttributeValue>ZP-MH:XuvzD+oq8QERJ2ZWswTg/qoYW6c=</saml2:AttributeValue>
      </saml2:Attribute>
      <saml2:Attribute FriendlyName="PRINCIPAL-NAME"
Name="urn:oid:1.2.40.0.10.2.1.1.261.20" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri">
        <saml2:AttributeValue>XXXŁódź</saml2:AttributeValue>
      </saml2:Attribute>
      <saml2:Attribute FriendlyName="BIRTHDATE" Name="urn:oid:1.2.40.0.10.2.1.1.55"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml2:AttributeValue>1964-04-26</saml2:AttributeValue>
      </saml2:Attribute>
      <saml2:Attribute FriendlyName="PVP-VERSION" Name="urn:oid:1.2.40.0.10.2.1.1.261.10"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml2:AttributeValue>2.1</saml2:AttributeValue>
      </saml2:Attribute>
      <saml2:Attribute FriendlyName="GIVEN-NAME" Name="urn:oid:2.5.4.42"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml2:AttributeValue>XXXLudmilla</saml2:AttributeValue>
      </saml2:Attribute>
      <saml2:Attribute FriendlyName="ENC-BPK-LIST" Name="urn:oid:1.2.40.0.10.2.1.1.261.22"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
        <saml2:AttributeValue>
(BMF+WT-
UR|gUE8KhCy7rf13aeMAkKqBvo0Il82nr8vyN7LLAfNDdqqyO8ytJ4YD4CDTZxygTMaQQAC8Mxbv/+kr97ZdpmkC5Z
eMZaqhCCvpwR1hiIwiHP4l7JUKBfDaRfa5ioiZajGl+XmHCQsFYurVephMKawnzIoD9F61mfnQCHblXNLzj0=)
        </saml2:AttributeValue>
      </saml2:Attribute>
    </saml2:AttributeStatement>
  </saml2:Assertion>
</saml2p:Response>
```


Der Service-Provider kann aus der erhaltenen SAML2-Assertion, die Teil der SAML2-Authentifizierungs-Response ist, die von der ID Austria bestätigten Daten (Attribute) der Benutzer*in extrahieren und diese so in seiner Anwendung anmelden.

Abschließend sei nochmal darauf hingewiesen, dass der hier skizzierte Ablauf als Beispiel zu verstehen ist, dessen Ziel eine Vermittlung der prinzipiellen Abläufe ist. Abhängig von diversen Parametern, wie z.B. dem verwendeten SAML2-Binding-Profil, können sich die resultierenden Schritte des Authentifizierungsprozesses in einigen Punkten unterscheiden.

4.3.2. Anbindung via OIDC

Open ID Connect (OIDC) hat sich speziell im mobilen Umfeld als präferierter Standard zur Umsetzung von Identitätsmanagementsystemen und für die Interaktion zwischen Service-Providern und Identity-Providern etabliert. Dementsprechend unterstützt auch die ID Austria OIDC zur Interaktion mit (mobilen) Service-Providern. Details zur Verwendung der ID Austria durch Service-Provider unter Verwendung von OIDC sind in diesem Abschnitt beschrieben.

Generell erfolgt die Umsetzung der Anbindung von Service-Provider an die ID Austria via OIDC gemäß den OIDC-Spezifikationen. Bei der Verwendung von OIDC zur Kommunikation mit der ID Austria sind für Service-Provider folgende Punkte speziell zu beachten:

- **Authorization-Code-Flow.** Von der ID Austria wird ausschließlich der Authorization-Code-Flow (Response-Type: „code“) entsprechend der OIDC-Spezifikation unterstützt. Andere Code-Flows, die OIDC prinzipiell auch definiert, werden von der ID Austria bewusst nicht unterstützt.
- **Scopes.** Intern erfolgt bei ID Austria die Anforderung von Attributen über das Applikationsregister der ID Austria. Aus diesem Grund wird in diesem Zusammenhang empfohlen, die Scopes „openid“ und „profile“ anzufragen.
- **Claims.** Zusätzlich zu den in OIDC spezifizierten Claims, welche im Scope „profile“ definiert sind, unterstützt die ID Austria auch noch weitere spezifische Claims. Diese Claims sind gemäß dem PVP2-Attribut-Profil umgesetzt und dem OIDC-Scope „profile“ zugeordnet.

Im Gegensatz zu SAML2 können mit OIDC auch App-basierte Authentifizierungsprozesse umgesetzt werden. Mobile Apps können somit via OIDC eine Anmeldung mittels ID Austria integrieren. Die Verwendung von OIDC ist jedoch nicht auf mobile Szenarien beschränkt. Vielmehr kann eine ID Austria basierte Anmeldung mittels OIDC in sämtlichen Szenarien durchgeführt werden. Beispiele dafür sind:

- **Klassisch.** Anmeldung mit einem herkömmlichen Web-Browser auf einem PC/Laptop.
- **Mobile App.** Anmeldung mit einer nativen App auf einem mobilen Gerät.
- **Mobiler Browser.** Anmeldung mit einem mobilen Browser auf einem Smartphone.

Die konkreten Prozessschritte eines OIDC-basierten Authentifizierungsprozesses hängen von verschiedenen Faktoren ab. Aus Sicht des Service-Providers ist der Ablauf jedoch im Wesentlichen immer gleich. Der folgende Unterabschnitt skizziert daher zunächst einen generischen OIDC-basierten Authentifizierungsprozess. Auf Besonderheiten eines solchen Authentifizierungsprozesses unter Verwendung einer nativen mobilen App wird im nachfolgenden Unterschabschnitt eingegangen.

4.3.2.1. OIDC-basierter Authentifizierungsprozess

Startpunkt jeder OIDC-basierten Authentifizierung ist ein Authentifizierungs-Request, der vom Service-Provider an den Identity-Provider geschickt wird. Dieser Request wird üblicherweise vom Client (Browser, App, etc.) als HTTP-GET-Request oder HTTP-POST-Request an den Identity-Provider geschickt. In dieser Hinsicht ist OIDC nicht unähnlich zu SAML2.

Im Folgenden ist ein Beispiel für einen OIDC-basierten Authentifizierungs-Request gegeben, der über den Client der Bürger*in an die ID Austria übermittelt wird.

```
GET https://eid.oesterreich.gv.at/auth/idp/profile/oidc/authorize?response_type=code
&client_id=https%3A%2F%2Fbeispielservice.at
&redirect_uri=https%3A%2F%2Fbeispielservice.at%2Fcb
&scope=openid+profile&state=1234567890 HTTP/1.1

Host: eid.oesterreich.gv.at
```

Über den dargestellten Request werden folgende Parameter an die ID Austria übertragen:

- **„response_type“.** Der Response-Typ muss mit „code“ angegeben werden da von der ID Austria nur der Authorization-Code-Flow entsprechend der OIDC-Spezifikation unterstützt wird.
- **„client_id“.** Der eindeutige Identifikator des Service-Providers. Dieser muss zuvor in der ID Austria über die definierten Registrierungsprozesse für Service-Provider registriert worden sein.
- **„scope“.** Definiert in OIDC das Set von Identitätsinformationen, welche vom Identity-Provider angefordert werden. Bei der ID Austria erfolgt die Anforderung von Attributen über das Applikationsregister des ID Austria. Es wird daher in diesem Zusammenhang empfohlen, die Scopes „openid“ und „profile“ anzufragen.
- **„redirect_uri“.** Die Redirect-URI definiert die Client-Callback-URI, an welche die ID Austria die finale Authentifizierungs-Response an den Service-Provider ausliefern soll.
- **„state“.** Optionaler jedoch empfohlener Parameter, der als Schutz gegen Cross-Site-Request-Forgery (CSFR/XSRF) dient, indem der State zwischen Request und Callback beibehalten wird.

Die ID Austria antwortet dem Client daraufhin mit einer Auswahl an Authentifizierungsmethoden. Auch hier ergibt sich ein ähnliches Verhalten zum oben beschriebenen SAML2-basierten Authentifizierungsprozess.

Nachdem die Benutzer*in ihre präferierte Authentifizierungsmethode gewählt und den Authentifizierungsprozess erfolgreich durchlaufen hat, antwortet die ID Austria dem Client mit einer Authentifizierungs-Response, die den Authorization-Code gemäß dem durch OIDC definierten Authorization-Code-Flow beinhaltet.

Ein Beispiel für eine Authentifizierungs-Response, die von ID Austria an den Client retourniert wird, ist im Folgenden gegeben.

```
HTTP/1.1 302 Found
Location: https://beispielservice.at/cb?code=QXV0aEhhbmRsZXIxfDIwMjA...&state=af0ifjsldkj
```

Über die an den Client retournierte Response wird der Client an den Service-Provider weitergleitet. Der erhaltene Authorization-Code wird dabei vom Client der Bürger*in an den Service-Provider übermittelt. Im Anschluss sendet der Service-Provider den Authorization-Code in einem sogenannten Token-Request an den Token-Endpoint der ID Austria. Teil dieses Token-Request ist optional auch ein Client-Secret, mit dem sich der Service-Provider gegen die ID Austria authentifiziert.

Ein Beispiel für einen Token-Request ist im Folgenden gegeben. Wichtig in diesem Zusammenhang ist, dass dieser Request nicht über den Client der Benutzer*in, sondern direkt vom Service-Provider an den entsprechenden Endpunkt der ID Austria gesendet wird.

```
POST https://eid.oesterreich.gv.at/auth/idp/profile/oidc/token
HTTP/1.1
```

Im Body des POST-Request werden auch die Parameter „code“, „grant_type“, „client_secret“ (falls erforderlich), „redirect_uri“ und „client_id“ übermittelt. Dies ist im Folgenden exemplarisch dargestellt.

```
code=QXV0aEhhbmRsZXIxfDIwMjAtMDMtMzAgMTM6NTk....
&grant_type=authorization_code
&client_secret=secret
&redirect_uri=https://beispielservice.at/cb
&client_id=https%3A%2F%2Fbeispielservice.at
```

Nach erfolgreicher Validierung des Authorization-Codes durch die ID Austria antwortet diese mit einer OIDC-Successful-Token-Response, die das signierte und verschlüsselte ID-Token enthält. Dieses ID-Token liefert die angeforderten Attribute (Claims) in Form eines JSON-Web-Tokens an den Service-Provider. Das ID-Token ist somit das OIDC-Äquivalent zur SAML2-Assertion. Ein Beispiel für eine OIDC-Successful-Token-Response ist im Folgenden gegeben.


```
{
  "id_token":
"eyJraWQiOiJkZWZhdWx0UlNBU2lnbiIsImFsZyI6IlJTMjU2In0.eyJhdF9oYXNoIjoiLWFseHhZOFlQM01WVHJwZ
VZ6QU5WdyIsInNlYiI6IlpQLUlIOktRTVk4U2w5V3NtQnhyWXJZT2lGUzJWa0x5bz0iLCJ1cm46cHZwZ3ZhdDpvaWR
jLmVpZF9pc3N1aW5nX25hdGlvbiI6IkFUIiwiYmlydGhkYXRlIjoiMTk4My0wNi0wNCIsInVybjpwdnBndmF0Om9pZ
GMucHZwX3ZlcnNpb24iOiIyLjEiLCJpc3MiOiJodHRwczpcL1wvZWlkLmVnaXouZ3YuYXQiLCJnaXZlbl9uYW1lIjo
iWFhYxZB6Z8O8ciIsInVybjpwdnBndmF0Om9pZGMuZW5jX2Jwa19saXN0IjoiKEJNRitaUC1URHxNMDJRdyt2S0U3Y
1hSTDRDd1wvVWZobW9haU9oVEd2M3U4RkJHVnZSTng2d1wvdE53MjJPdG1tK1FsR1Q2czExdXNWcmY4QkdPWDZqVGs
2elBQV2doalwvVTRuQmZMUlczT21WTEJJYmhFWDNGME8xVWhGdzh3TjB5MjRKUGdnVktIWHRiTXRRVVEyRU9FYzh3S
05uaGdQbnlCWjJVdEJxZXk1UGpaQlVuZU9lMjQ9KTsoQk1GK1dULVVSfFVPc3pLV0VKYjA1MEdwSXp6cnFzNjlNWkQ
3TmVYVUg0aTRcL0xaOHhXQ2pvXC9KSU1CWXpGXC9HTEhranc0cCtQWEhCSGZMMG9YVFA5VExcL284THAxRlV2MVlad
Wk0VWZ6a28yZGJOMkNHV2ZUcVUyRHowNnJPZjFUY29Ga2dzODgxZE9RYUFnTWNPb3VRemExWHJFOXlESGNTc2JLSVl
nYWVOK3g4bWhpdU5sUjA9KTsod2JwaytYRk4rMTk1NzM4YXxKQ2FuZm1GMm8yQzN3VHJ4V0YwYkhoUmlDak80NFVZM
kVFT1dUMjA5N0crbERSaHJ5NnYraGtWWkpqcENBS3FEcnlLbWtiaUo0RWV4dHRRS1Y4Tkt2UlJkSFdqQVN1OHF2QVp
nNllLNERlZXVjcWtIU3VYWDVjdjNLOHowNzZ3RGpWVEFpMm83WkJBRWN6eUE4c3hiM2RsY3VCckRpTUNCck1MelwvM
m96QUlIRUFYS3NSSUZ4amY5UGVJVG5sT2RkaWlqS2dNTlJLNWFrV0paRXpHaGNGcHdwSXArTUJ5RGRYZ3RYVm91TTV
YTVwvUTZYVklSNDkxYlNqajBnOFU1YmlEN0xBTk91d2ZQVWlnVW1KY2JIK1VxbVorTnF4UWQ5TmpYRGJsMWpLeENER
0tJUGFnUW01aENldVFKa1hjaTVMc2FRYTRLNXIxRWw0VitUTEdsZ3YwMmVuU1ExQVFVeUtZbHh5aWRnMXYxNG9HcEJ
1RXNiWmN1UUZrTW56WnRRSHNhaE14enJEZkZRMkNWMERqZjIySnB1MFE5VzdLcHdlVE5uMGlBSFZobU9ZWExzUUZvc
```

```
Fd4K1JrMzFiN3BaS1YrenpScTg5cG1KZUh5XC9Bd2lYdVEySExoakFNREdMWnhCb3NLVVN5S2Y2VjJhOFJLWjVRemR
4eWxOZUJzdTMwRlNDMlRBMUJWNTVGeWd5N1A2bUZqN3lLTkx0QjZFQ0lmRWpEYnorbDczSzZmN2UrZW1pWVFLNTdZa
XlFM3pPdytJYmxuNTFDNHNsNUcrTW0wOEQ5eUZyaFVvNHRjTWw5eGY0QlwvSmZpcnpPR3BXZlhaOXBTNHhYbFNSekF
XbXpRTjhrR2kwa2xoMTFSaHVZQVwvZlwvd2wzRThRVHBlUHFYRmVJcjZVK21YWjdRQT0pOyhTSFYrU1Z8b3dlaFdiU
XFPV1ZHWStVZ3VcL3BPcHRMUldqRXV1VDlUK1hjZXdBeFExVVhyYjZkTjJpNWlcL1Y0VkJaXC8rMlpJTVFuS0NvamR
Rc3B4SUNEOXFWSStpRWorNHVXeDhZOWtjT21xQ1NINVd3dDFyM3VlSlFiOEVwQkVkajdtU1h1QUJ4ZzhIWW5iaHBIW
FBqeGwzMWsxbkZlNU9ZN0pKYTE2VHpZcGpyRXhBeDYwPSk7KEJNSitKUnxaV2RIMThzQmtmRWZcL1FoVG9yK3BaOW9
lUlwvOFhoRGdUZ2ZPK25nSlwvUnJlZ25PTTJ0Q2ZRVit6MmZuTTZtVDFJeTFGemNiM0FPMnRBU0hPQUR1VHJ3bHNHb
Uk1SExyTFBEUmcyMGZGXC9VTGZueURyYmNwU1RmM1IxZmZJZXRlMHdqSmRHSklPS08yTndjMVhJQ0J4cEt0WnFwWlN
LbmpLUW5pNlFXZGZKd2JcL2NCS050YmFyd1N4T2FadXY3KzNjNHFTcCsrRTgwYkVYYk9lUnU2MUNGUmN3dElCMDE2R
EdaSlFMMFNIWmNQZWcxOVArVHM4OTdWWTR5V1J5SElyQ0dCYlpVbm5Ocnl3VExQYU55U3B3aDFSd3lxOEFyWnB5OTN
CWjdUdDBFRVwvZDNcL1RESzBjdDRjUGV4M0RsR3NqTFpSYTArcU1HMXluejdSV3pEZ01jaXFnPT0pOyh3YnBrK1hGT
isyMDQ3MTlofFhqTDNpRGNBcDlBa2tORUszTmZERWMzOE8rR0V0RGp2em5NVTAzM2dlOTQ2aFFmVjhLRkJ4aFFJcmd
hOUxlXC9zVlNZdTZoU3M1ZVBXa2FpY3dMMkhiY3pUWHhCZm9PXC8zZk5weTU0d3ZzaVpDRTRRTUdTOWtLNFRnclNvZ
nlPUndjek1RMUdQM0JkOU9aZ3FHeWphbXJyYVlpWFNqSjREdVJrUEJ1OUxNeVFrRXcxYVZQZk43N1RIR0ZidGFWYTV
0TlQ2TFRPbGxPY0hyajJSZWxyMUNheUp0QkFWSGZwd01TbjhBR25PUWdFWGJDOEdwN2wyZW40cXh3dVwvWFFCV1AzT
GcwcU9hVnZnVkVua1UzWGRtOUNRU2hTQVZlWW9PUmRHNkwwU21FVzNkbTUwRGx3V2ZYd284MFNcLzdpK1JrYWdsWDM
yaXVXTUJhNUYwc0toSDRiMXc9PSk7KEJNRitTQXxRWWo1SVZLd0V6MWhxXC9WbE5pSU9Nb2QxV3Y3TWczZmYxenM4b
GZcL0t1VVlCWHVhYTYxeWJUdFRkVTE1RFNTNFRleGJMNTJvanRYN0VVVXRYVUlqMFBsdmlRT2Q1c0NFVEZmb01kcFw
vSmhIbGZHdUZ3S05OUmozUkR3c1VnS1c1TklYRnRHVGErYVRxeGVZSGhQcGtwN1E5TU11NjQxcnNVWDBNcFR5b1NKY
VE9KTsoQk1JK1pQfFNVYk5WcEF6WDVnR0pyUWFwOEVJc1dHRklqdFlKbVBnTkFUcTR1NlJnbkJFeURCODNDY0Nhb3I
zdEZiUkRsZWJkMXZNUVJSUTFWVkxNQ3g1N0tqbFRReHo5ZkRYME9iUklzYldOam81SXFPVEF2K2t0UFVtVzB6SFY0e
klQVUxTc0NHcnRrdThMc1NVYWhpNkpUQ1JkUWdVcU5sXC9adzE4STJxN283Z1U2VWc9KTsoWlVTRUFNT0QrWlV8VmZ
Xa0pjOEptdDFcL0tyVCsrMEZ5eG4rVU5SQVRyb0xKdjlHN2YyS3RrK2tiTW9xSVkzNVN2TXRhRVFwZ0hEcWNqQ2RyQ
2crMXhCQkFFenkyZXpCdG1yRGNVbDJUOWlCcFwvVGZ1aWNaWEVOV0FBK1BZS3FPWVA5SkNGc2Y1NnMwK2lUUDQ5Q2J
IZmRhSitcL2FLXC9NUGlCaVl0OEc3bTFcLzBVdmtRb1Q5ajNtMm89KSIsImF1ZCI6Imh0dHBzOlwvXC9zZWN1cmUzL
m9lc3RlcnJlaWNoLmd2LmF0XC9hdXRoXC9zcFwvTWV0YWRhdGEiLCJhdXRoX3RpbWUiOjE2MTA3MDgyNTAsInVybjp
wdnBndmF0Om9pZGMuYnBrIjoiWlAtTUg6S1FNWThTbDlXc21CeHJZcllPaUZTMlZrTHlvPSIsImV4cCI6MTYxMDcxM
Tg2NCwiaWF0IjoxNjEwNzA4MjY0LCJmYW1pbHlfbmFtZSI6IlhYWFTDvHpla8OnaSJ9.LvIZ5smcAwTMOzhbAfAQRS
7KUzHIib8tKZB1CsdPXBbnBtSIBDmz1YQpZzvEmG_n_5XJNKmsHLWy2JwOoNokqPAyVL3u_nS8eAQc27leLzsJNRwK
5uVW_27ynAvNHXg_n1CE-tVgpzuqQESlvRP70Dt6z40Wzuq6szrgaYbXrQWS26c-G75d-
6jap9iDJJH1rfPgh2SLAoHaktNNprrGpTMv7NpiempdrrXGrNrWJqHzHP_ON-
RQgyAoaA1xSRfDKuORCvChtFnYsnKyVbgAHs7P6eQFvcZWmFbuAScqI53u60WHp7l_yLs7dodcx3VAnilegBhahy0Z
d6uFT8oH_w",
  "token_type": "Bearer",
  "expires_in": 600
}
```


Der Service-Provider kann das erhaltene ID-Token schließlich entschlüsseln und dekodieren und mit den darin enthaltenen Attributen die Benutzer*in in der Anwendung anmelden. Im Folgenden ist ein Beispiel für ein entschlüsseltes ID-Token gegeben.


```
{
  "at_hash": "-alxxY8YP3MVTrpeVzANVw",
  "sub": "ZP-MH:KQMY8Sl9WsmBxrYrYOiFS2VkLyo=",
  "urn:pvpgvat:oidc.eid_issuing_nation": "AT",
  "birthdate": "1983-06-04",
  "urn:pvpgvat:oidc.pvp_version": "2.1",
  "iss": "https://eid.egiz.gv.at",
  "given_name": "XXXŐzgür",
  "urn:pvpgvat:oidc.enc_bpk_list": "(BMF+ZP-
TD|M02Qw+vKE7cXRL4Cw/UfhmoaiOhTGv3u8FBGVvRNx6w/tNw22Otmm+QlGT6s11usVrf8BGOX6jTk6zPPWghj/U4
nBfLRW3OmVLBIbhEX3F0O1UhFw8wN0y24JPggVKHXtbMtQUQ2EOEc8wKNnhgPnyBZ2UtBqey5PjZBUneOe24=);(BM
F+WT-
UR|UOszKWEJb050GpIzzrqs69MZD7NeXUH4i4/LZ8xWCjo/JIMBYzF/GLHkjw4p+PXHBHfL0oXTP9TL/o8Lp1FUv1Y
Zui4Ufzko2dbN2CGWfTqU2Dz06rOf1TcoFkgs881dOQaAgMcOouQza1XrE9yDHcSsbKIYgaeN+x8mhiuNlR0=);(wb
pk+XFN+195738a|JCanfmF2o2C3wTrxWF0bHhRiCjO44UY2EEOWT2097G+lDRhry6v+hkVZJjpCAKqDryKmkbiJ4Ee
xttQKV8NKvRRdHWjASu8qvAZg6YK4DeeucqkHSuXX5cv3K8z076wDjVTAi2o7ZBAEczyA8sxb3dlcuBrDiMCBrMLz/
2ozAIHEAXKsRIFxjf9PeITnlOddiijKgMNRK5akWJZEzGhcFpwpIp+MByDdXgtXVouM5XM/Q6XVIR491bSjj0g8U5b
iD7LANOuwfPUigUmJcbH+UqmZ+NqxQd9NjXDbl1jKxCDGKIPagQm5hCeuQJkXci5LsaQa4K5r1El4V+TLGlgv02enS
Q1AQUyKYlxyidg1v14oGpBuEsbZcuQFkMnzZtQHsahMxzrDfFQ2CV0Djf22Jpu0Q9W7KpweTNn0iAHVhmOYXLsQFop
Wx+Rk31b7pZKV+zzRq89pmJeHy/AwiXuQ2HLhjAMDGLZxBosKUSyKf6V2a8RKZ5QzdxylNeBsu30FSC2TA1BV55Fyg
y7P6mFj7yKNLtB6ECIfEjDbz+l73K6f7e+emiYQK57YiyE3zOw+Ibln51C4sl5G+Mm08D9yFrhUo4tcMl9xf4B/Jfi
```

```
rzOGpWfXZ9pS4xXlSRzAWmzQN8kGi0klh11RhuYA/f/wl3E8QTpePqXFeIr6U+mXZ7QA=);(SHV+SV|owehWbQqOWV
GY+Ugu/pOptLRWjEuuT9T+XcewAxQ1UXrb6dN2i5i/V4VBZ/+2ZIMQnKCojdQspxICD9qVI+iEj+4uWx8Y9kcOmqCS
H5Wwt1r3ueJQb8EpBEdj7mSXuABxg8HYnbhpHXPjxl31k1nFe5OY7JJa16TzYpjrExAx60=);(BMJ+JR|ZWdH18sBk
fEf/QhTor+pZ9oeR/8XhDgTgfO+ngJ/RregnOM2tCfQV+z2fnM6mT1Iy1Fzcb3AO2tASHOADuTrwlsGmI5HLrLPDRg
20fF/ULfnyDrbcpSTf3R1ffIete0wjJdGJIOKO2Nwc1XICBxpKtZqpZSKnjKQni6QWdfJwb/cBKNtbarwSxOaZuv7+
3c4qSp++E80bEXbOeRu61CFRcwtIB016DGZJQL0SHZcPeg19P+Ts897VY4yWRyHIrCGBbZUnnNrywTLPaNySpwh1Rw
yq8ArZpy93BZ7Tt0EE/d3/TDK0ct4cPex3DlGsjLZRa0+qMG1ynz7RWzDgMciqg==);(wbpk+XFN+204719h|XjL3i
DcAp9AkkNEK3NfDEc38O+GEtDjvznMU033ge946hQfV8KFBxhQIrga9Le/sVSYu6hSs5ePWkaicwL2HbczTXxBfoO/
3fNpy54wvsiZCE4QMGS9kK4TgrSofyORwczMQ1GP3Bd9OZgqGyjamrraYiXSjJ4DuRkPBu9LMyQkEw1aVPfN77THGF
btaVa5tNT6LTOllOcHrj2Relr1CayJtBAVHfpwMSn8AGnOQgEXbC8Gp7l2en4qxwu/XQBWP3Lg0qOaVvgVEnkU3Xdm
9CQShSAVeYoORdG6L0SmEW3dm50DlwWfXwo80S/7i+RkaglX32iuWMBa5F0sKhH4b1w==);(BMF+SA|QYj5IVKwEz1
hq/VlNiIOMod1Wv7Mg3ff1zs8lf/KuUYBXuaa61ybTtTdU15DSS4TexbL52ojtX7EUUtXUIj0PlviQOd5sCETFfoMd
p/JhHlfGuFwKNNRj3RDwsUgKW5NIXFtGTa+aTqxeYHhPpkp7Q9MMu641rsUX0MpTyoSJaQ=);(BMI+ZP|SUbNVpAzX
5gGJrQap8EIsWGFIjtYJmPgNATq4u6RgnBEyDB83CcCaor3tFbRDlebd1vMQRRQ1VVLMCx57KjlTQxz9fDX0ObRIsb
WNjo5IqOTAv+ktPUmW0zHV4zIPULSsCGrtku8LsSUahi6JTCRdQgUqNl/Zw18I2q7o7gU6Ug=);(ZUSEAMOD+ZU|Vf
WkJc8Jmt1/KrT++0Fyxn+UNRATroLJv9G7f2Ktk+kbMoqIY35SvMtaEQpgHDqcjCdrCg+1xBBAEzy2ezBtmrDcUl2T
9iBp/TfuicZXENWAA+PYKqOYP9JCFsf56s0+iTP49CbHfdaJ+/aK/MPiBiYt8G7m1/0UvkQoT9j3m2o=)",
  "aud": "https://secure3.oesterreich.gv.at/auth/sp/Metadata",
  "auth_time": 1610708250,
  "urn:pvpgvat:oidc.bpk": "ZP-MH:KQMY8Sl9WsmBxrYrYOiFS2VkLyo=",
  "exp": 1610711864,
  "iat": 1610708264,
  "family_name": "XXXTüzekçi"
}
```


4.3.2.2. Verwendung von OIDC in nativen Apps

Die Verwendung von OIDC ist grundsätzlich in allen Szenarien ähnlich, d.h. unabhängig davon, ob OIDC zur Anmeldung an einem Service-Provider über einen Web-Browser verwendet wird, oder ob als Client eine mobile App zur Anwendung kommt, über die eine Authentifizierung gegen einen serverseitigen Service-Provider erfolgt. Ist eine mobile App in den Anmeldeprozess als Client-Komponente involviert, müssen jedoch folgende Punkte beachtet werden.

- **Rücksprungadresse.** Wird OIDC in eine native mobile App integriert, kann als Rücksprungadresse (Parameter „redirect_uri“) auch ein App-/URL-Scheme (z.B.: „com.example.app:/oauth2redirect/example-provider“) angegeben werden. In diesem Fall erfolgt nach erfolgreicher Durchführung des Anmeldeprozesses unmittelbarer ein Rücksprung in die mobile App.
- **Code-Authorization-Flow.** Bei der Verwendung von OIDC in nativen mobilen Apps empfiehlt RFC 8252 die Verwendung des OIDC Code-Authorization-Flows, da nur dieser Flow mit dem Verfahren „Proof Key for Code Exchange (PKCE)“ nach RFC 7636 abgesichert werden kann. Eine Verwendung von PKCE in nativen mobilen Apps wird aus Sicherheitsgründen dringend empfohlen.

4.4. Migration von Bürgerkarte und Handy-Signatur auf die ID Austria

Für Service-Provider (bzw. die entsprechenden verantwortlichen Service-Owner) ergibt sich durch die Überführung des bisherigen Bürgerkarte-/Handy-Signatur-Systems auf die Nachfolgelösung ID Austria Handlungsbedarf. Konkret müssen Service-Provider in Zukunft Authentifizierungs-Requests direkt an die ID Austria senden und nicht mehr wie bisher an eine MOA-ID-Instanz, die die Anmeldung über Bürgerkarte oder Handy-Signatur durchführt.

Die für die ID Austria vorgesehene direkte Anbindung von Service-Providern über SAML2 oder OIDC wurde im vorherigen Abschnitt bereits ausführlich besprochen. Ergänzend dazu stellt dieser Abschnitt nun noch die Komponente „MOA E-ID Proxy“[18] vor. Diese kann Service-Provider temporär bei der Umstellung auf die ID Austria unterstützen. Die folgenden Unterabschnitte beschreiben das Konzept des MOA E-ID Proxys und geben einen ersten Einblick in dessen Konfiguration.

4.4.1. MOA E-ID Proxy

Die ID Austria stellt aus abstrakter Sicht einen zentralen Identity-Provider dar, der die aktuell dezentral betriebenen MOA-ID-Instanzen ersetzt. Service-Provider übermitteln in Zukunft Authentifizierungs-Requests direkt an die ID Austria. Die ID Austria macht dadurch den Betrieb und die Verwendung von MOA-ID obsolet.

Eine direkte Anbindung von Service-Providern mittels des veralteten Authentifizierungsprotokolls SAML1, welches in MOA-ID bereits seit der Version 2.x aus dem Jahr 2014 als „deprecated“ (veraltet) markiert war, ist bei der ID Austria nicht mehr möglich. Eine Anbindung kann ausschließlich über die Protokolle SAML2 oder OIDC erfolgen. Alle Service-Provider, welche aktuell noch über SAML1 an MOA-ID angebunden sind und weder SAML2 noch OIDC unterstützen, können somit nicht mehr direkt (mittels SAML1) an die ID Austria ankoppeln.

Für Service-Provider, für die eine kurzfristige direkte Anbindung oder ein kurzfristiger Umstieg auf SAML2 oder OIDC nicht möglich ist, wurde mit dem MOA E-ID Proxy eine Übergangslösung geschaffen. Der MOA E-ID Proxy wurde als MOA-ID Version 4.1.x im Jahr 2020 veröffentlicht. Als zusätzliches Feature enthält diese Version von MOA-ID eine Proxy-Funktion, die als Bindeglied zwischen SAML1-basierten Service-Providern und der ID Austria fungiert. Alle Service-Provider, die die MOA-ID-Instanz bisher nutzten, um Anmeldungen über Bürgerkarte oder Handy-Signatur durchzuführen, können über die Proxy-Funktion nun auch direkt an die ID Austria angebunden werden. Technische Änderungen am Service-Provider selbst sind dadurch vorerst nicht nötig.

Der MOA E-ID Proxy, d.h. MOA-ID Version 4.1.x oder jünger, bietet Anwendungen dieselbe SAML1/SAML2/OIDC-Schnittstellen, wie sie bereits aus den vorangegangenen Versionen von MOA-ID bekannt ist. Ist die Proxy-Funktion aktiviert, leitet MOA-ID alle Authentifizierungsanfragen an die ID Austria weiter. Diese Variante der Anbindung von Service-Providern an die ID Austria ist in der folgenden Abbildung veranschaulicht.

[18] Die Bezeichnung „MOA E-ID Proxy“ basiert noch auf dem Arbeitstitel „E-ID“, unter dem die ID Austria zunächst entwickelt wurde. Diese Bezeichnung findet sich auch noch in den relevanten legislativen Vorgaben der ID Austria. Der die Bezeichnung „MOA E-ID Proxy“ bereits einigermaßen etabliert ist, wurde zur Vermeidung von Missverständnissen auf eine Umbenennung verzichtet.

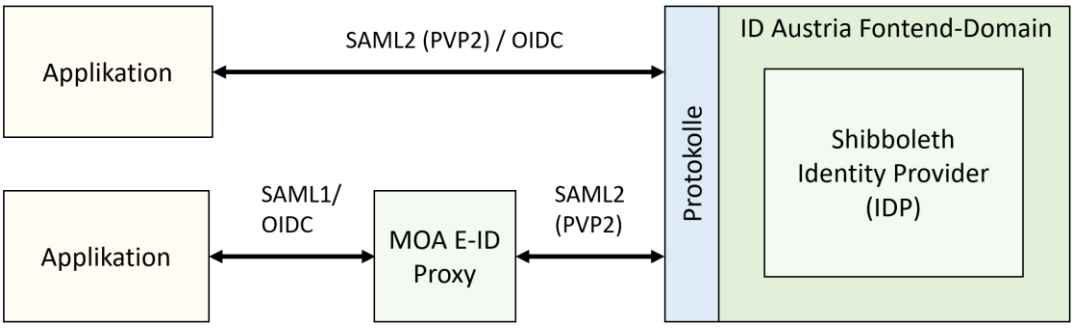

Abbildung 4. Verwendung des MOA E-ID Proxy zur Anbindung von Service-Providern („Applikation“) an die ID Austria.

Die Installation und der Betrieb des MOA E-ID Proxy sind im Wesentlichen identisch zur Version 3.x von MOA-ID. Details können dem Handbuch zu MOA-ID entnommen werden.

Prinzipiell kann im MOA E-ID Proxy (d.h. in MOA-ID Version 4.1.x) pro Service-Provider konfiguriert werden, ob Benutzerauthentifizierungen wie bisher über Bürgerkarte/Handy-Signatur oder bereits über die ID Austria durchgeführt werden sollen. Es könnte daher die Verlockung bestehen, alle Service-Provider (auch jene, die bereits SAML2 unterstützen) über den MOA E-ID Proxy an die ID Austria anzubinden. Es wird jedoch dringend empfohlen, alle Service-Provider, die SAML2 ohnehin bereits unterstützen, direkt, d.h. ohne Umweg über den MOA E-ID Proxy, an die ID Austria anzubinden. Der MOA E-ID Proxy ist als Übergangslösung konzipiert. Nach dessen Einstellung muss in jedem Fall eine direkte Anbindung an die ID Austria erfolgen.

4.4.2. Aktivierung der Anbindung an die ID Austria im MOA E-ID Proxy

Mit der Version 4.1.x von MOA-ID wurde eine neue Proxy-Funktion für die Anbindung von Service-Providern an die ID Austria integriert. Dieser Abschnitt beschreibt, wie diese Proxy-Funktion aktiviert werden kann, um Service-Providern die Benutzerauthentifizierung über ID Austria zu ermöglichen.

Die ab MOA-ID 4.1.x integrierte Proxy-Funktion kann separat für jeden in MOA-ID definierten Service-Provider aktiviert werden. Dies erfolgt über die Konfiguration von MOA-ID. Schon bisher waren in dieser Konfiguration zu jedem Service-Provider, der von MOA-ID serviciert wird, diverse Daten hinterlegt. Neu ist nun das Konfigurations-Flag „E-ID Proxy-Mode aktivieren“. Über dieses Flag kann definiert werden, ob Authentifizierungsprozesse für den betreffenden Service-Provider an die ID Austria weitergeleitet werden sollen.

Name	Optional	Beschreibung
E-ID Proxy-Mode aktivieren	X	Aktiviert die Weiterleitung an die ID Austria für diese Online-Applikation.

Für jeden Service-Provider kann in MOA-ID über die Konfiguration angegeben werden, welche Attribute nach erfolgter Benutzerauthentifizierung an den Service-Provider retourniert werden sollen. Wird für einen Service-Provider der E-ID-Proxy-Mode (d.h. die seit Version 4.1.x integrierte Proxy-Funktion) aktiviert, ändert sich das Set der Attribute, die einem Service-Provider prinzipiell zur Verfügung gestellt werden können. Dies ist darin begründet, dass Benutzer*innen bei aktiviertem E-ID-Proxy-Mode an die ID

Austria weitergeleitet werden. Diese stellt ein anderes Attribut-Set zur Verfügung als Handy-Signatur oder Bürgerkarte.

Bei einer Benutzerauthentifizierung über die ID Austria stehen unter anderem die in der folgenden Tabelle angeführten neuen Attribute zur Verfügung. Die Bezeichnungen der Attribute entsprechen dem PVP2-Attribute-Profil.

Attribut-Name	URN Prefix + OID
ENC-BPK-LIST	1.2.40.0.10.2.1.1.261.22
BPK-LIST	1.2.40.0.10.2.1.1.261.28
MANDATOR-NATURAL-PERSON-ENC-BPK-LIST	1.2.40.0.10.2.1.1.261.72
MANDATOR-NATURAL-PERSON-BPK-LIST	1.2.40.0.10.2.1.1.261.73

Die Proxy-Funktion (E-ID-Proxy-Mode) in MOA-ID sorgt dafür, dass der Wechsel der Benutzerauthentifizierung von Bürgerkarte/Handy-Signatur zu ID Austria für den Service-Provider weitgehend transparent bleibt. Der Service-Provider kann wie bisher Authentifizierungs-Requests an MOA-ID übermitteln. Die Interaktion mit der ID Austria wird vollständig durch MOA-ID abgewickelt.

Service-Provider, die die Proxy-Funktion in MOA-ID zur Anbindung der ID Austria nutzen, sollten sich jedoch trotzdem bewusst sein, dass Benutzerauthentifizierungen dadurch potenziell über die ID Austria abgewickelt werden. Dies vor allem deshalb, da sich je nach Authentifizierungsmethode (Bürgerkarte, Handy-Signatur, ID Austria) das dem Service-Provider von MOA-ID retournierte Attribut-Set unterscheiden kann. Ursache hierfür ist, dass die ID Austria aus rechtlichen Gründen (E-Government-Gesetz) nicht mehr alle bisher über Bürgerkarte/Handy-Signatur bereitgestellten Attribute ausliefern darf. Als Ersatz stehen jedoch in Zukunft die in obiger Tabelle gelisteten Attribute zur Verfügung.

Somit ändert sich je nach gewählter Authentifizierungsmethode der Inhalt der vom MOA E-ID Proxy (d.h. MOA ID ab Version 4.1.x) bereitgestellten SAML2-Assertions/ID-Token in Bezug auf die darin enthaltenen Attribute. Angebundene Service-Provider müssen sich dessen bewusst sein und damit umgehen können, auch wenn sie über den MOA E-ID Proxy nur indirekt an die ID Austria angebunden sind.

4.4.3. Anforderung der ID Austria an den MOA E-ID Proxy

Auch wenn die Proxy-Funktion seit Version 4.1.x in MOA-ID integriert ist (und MOA-ID ab dieser Version daher als MOA E-ID Proxy bezeichnet wird), ist für die Ankopplung eines MOA E-ID Proxy an die ID Austria derzeit mindestens ein MOA E-ID Proxy in der Version 4.1.5 notwendig. Ältere Versionen können aus organisatorischen Gründen nicht bei der ID Austria registriert werden.

4.4.4. Registrierung im zentralen Applikationsregister der ID Austria

Alle Service-Provider, für welche die Proxy-Funktion aktiviert ist, müssen im Applikationsregister der ID Austria registriert (und akkreditiert) sein. Diese Registrierung/Akkreditierung ist über weite Strecken identisch zur Registrierung/Akkreditierung von Service-Providern mit direkter Anbindung an die ID Austria (siehe Abschnitt 4.3). Aus dem Betrieb und der Verwendung eines MOA E-ID Proxy ergeben sich jedoch auch spezielle Anforderungen an die Registrierung/Akkreditierung, wodurch sich punktuell Unterschiede zur Registrierung/Akkreditierung von Service-Providern ergeben, die direkt an die ID Austria angebunden

sind. Die markantesten Unterschiede sind nachfolgend gelistet. Allgemeine Informationen zur Registrierung und Akkreditierung von Service-Providern (und Service-Owners) finden sich in Abschnitt 4.2.

- **Eindeutiger Applikations-Identifier.** Im Zuge der Registrierung eines Service-Providers muss für diesen in jedem Fall ein eindeutiger Applikations-Identifier angegeben werden. Für Service-Provider, die über einen MOA E-ID Proxy an die ID Austria angebunden sind, besteht dieser Applikations-Identifier aus zwei Teilen. Der erste Teil entspricht dem Identifikator des MOA E-ID Proxy, der zweite Teil repräsentiert einen Identifikator für den zu registrierenden Service-Provider selbst. Beide Teile des Identifikators müssen einem definierten Format entsprechen. Um Service-Ownern die Registrierung ihrer Service-Provider zu vereinfachen, stellt der MOA E-ID Proxy ein Feature bereit, über das die Applikations-Identifier für alle Service-Provider, die über den MOA E-ID Proxy angebunden sind, abgefragt werden können (siehe Abschnitt 4.4.4.1).

- **SAML2-Metadaten.** Im Zuge der Registrierung eines Service-Providers müssen auch dessen SAML2-Metadaten bekanntgegeben werden, sodass über diese eine technische Anbindung an die ID Austria erfolgen kann. Bei einer Verwendung des MOA E-ID Proxy müssen im Zuge der Registrierung die SAML2-Metadaten der verwendeten MOA E-ID Proxy Instanz (und nicht jene des Service-Providers) angegeben werden. Grund dafür ist, dass aus Sicht der ID Austria der MOA E-ID Proxy auf technischer Ebene der MOA E-ID Proxy der Kommunikationspartner ist. Um Service-Ownern die Registrierung ihrer Service-Provider zu vereinfachen, stellt der MOA E-ID Proxy ein Feature bereit, über das die SAML2-Metadaten des MOA E-ID Proxy abgefragt werden können (siehe Abschnitt 4.4.4.2).

- **Konfiguration der bPK-Bereiche.** Schon bisher mussten in MOA-ID für alle dort registrierten Applikationen (Service-Provider) die entsprechenden bPK-Bereiche konfiguriert werden. Dies ist nach wie vor notwendig. Zusätzlich muss nun darauf geachtet werden, dass im Zuge der Registrierung/Akkreditierung des Service-Providers bei der ID Austria dieselben bPK-Bereiche definiert werden.

4.4.4.1. Abfrage des eindeutigen Applikations-Identifier

Wie oben erwähnt, muss im Zuge der Registrierung/Akkreditierung eines Service-Provider bei der ID Austria dessen eindeutiger Applikations-Identifier angegeben werden. Für Service-Provider hinter einem MOA-E-ID Proxy muss der Applikations-Identifier einem vordefinierten Format entsprechen. Der MOA E-ID Proxy bietet daher einen Endpunkt an, über welchen der eindeutige Identifier für die Registrierung im Applikationsregister abgefragt werden kann. Dieser Endpunkt wird im Kontext des MOA E-ID Proxy unter folgender URL bereitgestellt.

```
./eid/getappregid
```

Unter Verwendung dieses Endpunkts kann beispielsweise der Applikations-Identifier des Service-Providers *„https://labda.iaik.tugraz.at/demologin/test1“* vom MOA E-ID Proxy, der unter *„https://demo.egiz.gv.at/moa-id-auth“* erreichbar ist, wie folgt abgefragt werden.

```
https://demo.egiz.gv.at/moa-id-
auth/eid/getappregid?OA=https://labda.iaik.tugraz.at/demologin/test1
```

Als Abfrageparameter dienen also dieselben Parameter, die auch für einen SAML1-basierten Authentifizierungs-Request verwendet werden (siehe MOA-ID-Handbuch[19]). Eine Abfrage ist jedoch nur für Online-Applikationen (Service-Provider) möglich, die am betreffenden MOA E-ID Proxy registriert sind.

4.4.4.2. Abfrage der SAML2-Metadaten

Die Registrierung des MOA E-ID Proxy bzw. der über den MOA E-ID Proxy angebundenen Service-Provider bei der ID Austria erfordert auch die Bekanntgabe von SAML2-Metadaten. Zur Vereinfachung des Registrierungsprozesses bei der ID Austria bietet der MOA E-ID Proxy auch einen Endpunkt, über den die relevanten SAML2-Metadaten automatisch generiert und abgefragt werden können. Dieser Endpunkt wird im Kontext des MOA E-ID Proxy unter folgender URL bereitgestellt.

```
./sp/eid/metadata
```

Unter Verwendung dieses Endpunkts können beispielsweise die SAML2-Metadaten eines MOA E-ID Proxys, der unter „*https://demo.egiz.gv.at/moa-id-auth*“ erreichbar ist, wie folgt abgefragt werden.

```
https://demo.egiz.gv.at/moa-id-auth/sp/eid/metadata
```

4.4.5. Änderungen in Bezug auf die GUI-Integration

Bei der Verwendung von Bürgerkarte und Handy-Signatur über MOA-ID war es bei vielen Service-Providern gängige Praxis, GUI-Elemente der ausgelagerten Benutzerauthentifizierung (z.B. Eingabe der Telefonnummer und des Handy-Signatur-Passworts) über einen HTML-IFRAME nahtlos in die eigene HTML-GUI des Service-Providers zu integrieren. Dies hatte den Vorteil, dass die Benutzer*in auch während der Benutzerauthentifizierung (scheinbar) die vertraute Umgebung des Service-Providers nicht verließen.

Bei Verwendung der ID Austria zur Authentifizierung von Benutzer*innen ist eine Integration der GUI-Elemente des Authentifizierungsprozesses via HTML-IFRAME nicht mehr möglich. Stattdessen erfolgt in jedem Fall eine vollständige Weiterleitung des gesamten Browser-Kontexts an die ID Austria. Nach erfolgter Authentifizierung wird die Benutzer*in mit ihrem Browser wieder zurück zum Service-Provider geleitet.

Auch wenn die Benutzer*in dadurch zwischenzeitig die Umgebung des Service-Providers verlässt, ist die vollständige Weiterleitung des gesamten Browser-Kontexts an die ID Austria sinnvoll. Durch diese Weiterleitung kann die Benutzer*in kontrollieren, in welcher Domain sie ihre geheimen Zugangsdaten

[19] MOA ID Handbuch: https://apps.egiz.gv.at/handbooks/moa-id/handbook/protocol/protocol.html#saml1_startauth

eingibt. Damit kann bei Benutzer*innen das Bewusstsein geschärft werden, ihre Zugangsdaten stets nur in der ID-Austria-Domain einzugeben.

Für Service-Provider (bzw. die verantwortlichen Service-Owner) bedeutet dies, dass die Integration des Anmeldeprozesses in den Service-Provider eventuell überarbeitet werden muss, sofern bisher eine Integration via HTML-IFRAME erfolgte.

4.4.6. Verfügbarkeit des MOA E-ID Proxy

Abschließend sei nochmal klar darauf hingewiesen, dass eine langfristige Unterstützung des MOA E-ID Proxy nicht geplant ist. Nach dem End-of-Life des MOA E-ID Proxy müssen Service-Provider in jedem Fall direkt an die IS Austria angebunden sein. SAML1-basierte Service-Provider werden dann nicht mehr unterstützt. Service-Ownern wird also dringend empfohlen, ihre Service-Provider so schnell wie möglich direkt an die ID Austria anzubinden. Der MOA E-ID Proxy sollte nur als kurzfristige Übergangslösung betrachtet werden.

5. Ausgewählte Sicherheitsaspekte

Konzeption und technische Umsetzung der ID Austria unterscheiden sich in einigen Punkten grundlegend von den bisher im Einsatz befindlichen Systemen Handy-Signatur und Bürgerkarte. In vielen Fällen waren Sicherheitsüberlegungen der Grund für vorgenommene Änderungen. Die ID Austria berücksichtig diverse Erfahrungen, die aus jahrelangem Betrieb und der Verwendung von Handy-Signatur und Bürgerkarte gewonnen werden konnten, und hat zum Ziel, das Sicherheitsniveau für alle Beteiligten (Benutzer*innen, Service-Owner, etc.) zu erhöhen.

Dieser Abschnitt gibt einen Überblick über ausgewählte Aspekte der ID Austria, die speziell für Service-Owner und deren Service-Provider das erreichbare Sicherheitsniveau positiv beeinflussen. Die ausgewählten Aspekte werden in den folgenden Unterabschnitten näher diskutiert. Speziell wird dabei auf die Auswirkungen der getroffenen Designentscheidungen auf Service-Provider und deren Sicherheit eingegangen.

5.1. Sicherstellung der Korrektheit und Aktualität ausgelieferter Attribute

Von zentraler Bedeutung für Service-Provider ist die Korrektheit und Aktualität der Attribute (Benutzerdaten), die im Zuge des Anmeldeprozesses einer Benutzer*in erhalten werden. Die ID Austria verbessert das bisher diesbezüglich schon hohe Niveau der Bürgerkarte/Handy-Signatur noch weiter.

Zum einen können Benutzer*innen ihre persönliche ID Austria ausschließlich bei ermächtigten Behörden registrieren und aktivieren[20]. Damit wird sichergestellt, dass die Identität der Benutzer*in zum Zeitpunkt der Ausstellung ihrer persönlichen ID Austria behördlich überprüft wurde. Für Service-Provider ergibt sich damit eine noch höhere Sicherheit, dass die im Zuge eines Anmeldeprozesses via ID Austria erhaltenen Daten (Attribute) zur Benutzer*in korrekt sind und mit den Daten, die über die Benutzer*in in den staatlichen Registern hinterlegt sind, übereinstimmen.

Zum anderen wird die Korrektheit und Aktualität der an den Service-Provider ausgelieferten Daten zur Benutzer*in dadurch sichergestellt, dass diese bei jedem Anmeldeprozess von der ID Austria neu zusammengestellt werden. Bei Bürgerkarte und Handy-Signatur erfolgte eine Abfrage der Daten nur einmalig im Zuge der Registrierung/Aktivierung. Durch die dynamische Aggregation der an Service-Provider ausgelieferten Daten stellt die ID Austria sicher, dass diese Daten stets aktuell sind.

5.2. Sichere Registrierungs- und Akkreditierungsprozesse

Die Verwendung von Handy-Signatur und Bürgerkarte stand prinzipiell allen Service-Ownern und deren Service-Providern offen. Nach Installation der Open-Source-Komponente MOA-ID konnte eine Benutzerauthentifizierung via Bürgerkarte und Handy-Signatur sehr einfach in jeden Service-Provider integriert werden. Der Nachteil dieses offenen Ansatzes war, dass von behördlicher Seite, d.h. vom Anbieter des nationalen Identitätsmanagementsystems, wenig Einfluss darauf genommen werden konnte, an welche Service-Owner und Service-Provider staatlich bestätigte Benutzerinformationen (Attribute)

[20] In der ersten Übergangsphase wird es möglich sein, ein bestehendes Handy-Signatur-Konto in eine persönliche ID Austria (mit eingeschränktem Funktionsumfang) überzuführen. Nach Ablauf dieser selbst aktivierten ID Austria ist aber in jedem Fall eine Registrierung vor Ort bei einer entsprechend ermächtigten Behörde notwendig.

ausgeliefert wurden. Es wurde einzig den Benutzer*innen überlassen zu entscheiden, ob ein Service-Owner oder Service-Provider vertrauenswürdig genug war, um ihm die persönlichen Attribute zu überlassen. Obwohl dies ein zulässiger Ansatz ist, besteht in der Praxis die Gefahr, dass Benutzer*innen die Konsequenzen nicht immer bewusst sind, da ihnen das Detailverständnis (und auch das Interesse) bezüglich der Funktionsweise des nationalen Identitätsmanagementsystems fehlt.

Um diesem Problem entgegenzuwirken, verfolgt die ID Austria einen restriktiveren Ansatz. Jeder Service-Owner und jeder Service-Provider, der die ID Austria zur Anmeldung von Benutzer*innen nutzen möchte, muss zunächst im System der ID Austria registriert werden. Im Zuge der Registrierung gibt der Service-Owner relevante Daten über sich selbst und seine Service-Provider, die die ID Austria nutzen möchten, bekannt. Nachgelagert an den Registrierungsprozess ist – zumindest für privatwirtschaftliche Service-Provider – ein zusätzlicher Akkreditierungsprozess vorgesehen. Im Rahmen dieses Prozesses werden relevante Daten des Service-Providers geprüft. Dies erfolgt zumindest teilweise manuell. Erst nach erfolgreicher Akkreditierung des Service-Providers kann dieser die ID Austria zur Benutzerauthentifizierung nutzen.

Durch diesen im Vergleich zu Bürgerkarte und Handy-Signatur restriktiveren Ansatz ergibt sich auf Seiten der Service-Owner naturgemäß ein höherer organisatorischer Aufwand. Kompensiert wird dies jedoch dadurch, dass alle Beteiligten davon ausgehen können, dass nur geprüfte und damit legitime Service-Owner und Service-Provider die ID Austria nutzen. Dies erhöht insgesamt das Vertrauen in die Sicherheit und Vertrauenswürdigkeit des Gesamtsystems. Davon profitieren auch die das System nutzenden Service-Owner und Service-Provider.

5.3. Kontrolle der vereinfachten Weiterverwendung einer vorherigen Authentifizierung

Benutzer*innen haben die Möglichkeit, innerhalb ihrer Digitales-Amt-App auf ihrem mobilen Gerät eine kryptographische Bindung zur ID Austria zu erstellen. Unter Verwendung dieser Bindung kann in weiterer Folge eine vereinfachte Authentifizierung gegen die ID Austria erfolgen, da für diesen Authentifizierungsvorgang die Eingabe des geheimen Passworts entfallen kann. Die Mehrfaktorauthentifizierung wird über die zuvor erstellte Bindung umgesetzt[21].

Die Sicherheit dieser vereinfachten Weiterverwendung einer vorherigen vollständigen Authentifizierung wird durch die Umsetzung diverser Maßnahmen gewährleistet. So kommen clientseitig am mobilen Gerät der Benutzer*innen sichere Hardware-Elemente zur Anwendung, in denen privates kryptographisches Schlüsselmaterial, über das die Bindung zur ID Austria technisch umgesetzt ist, sicher gespeichert wird. Serverseitig stellt unter anderem eine umfangreiche Public-Key-Infrastruktur (PKI) die sichere Umsetzung der vereinfachten Weiterverwendung vorheriger Authentifizierungen sicher.

[21] Nicht zu verwechseln ist diese kryptographische Bindung zum IDP mit jener kryptographischen Bindung, die im Zuge der oben beschriebenen Registrierungsprozesse zwischen Digitales-Amt-App und dem Vertrauensdienstanbieter etabliert wird.

5.4. Sichere Auslieferung von Identitätsinformationen

Nach einer erfolgreichen Benutzerauthentifizierung durch die ID Austria übermittelt diese dem Service-Provider die Identitätsmerkmale (Attribute) der authentifizierten Person. Bei Verwendung von SAML2 erfolgt die Übermittlung über eine SAML2-Assertion, bei Verwendung von OIDC werden die Attribute zur Person in Form eines ID-Token übertragen. In jedem Fall ist die Sicherheit der Datenübertragung zwischen ID Austria und Service-Provider essenziell.

Beide von der ID Austria unterstützten Protokolle (SAML2, OIDC) bieten verschiedene Varianten, wie SAML2-Assertions bzw. ID-Token zwischen Identity-Provider (ID Austria) und Service-Provider übermittelt werden können. Die verschiedenen Varianten unterscheiden sich zum Beispiel darin, ob die Daten über den Client der Benutzer*in (z.B. Web-Browser) geleitet werden, oder ob ein direkter Datenaustausch zwischen Identity-Provider und Service-Provider stattfindet. Die von der ID Austria unterstützten Protokollvarianten wurden so gewählt, dass sie Sicherheit der ausgetauschten Daten maximiert wird. Dies ist in den folgenden Unterabschnitten näher ausgeführt.

5.4.1. Authentifizierung des Service-Providers an der ID Austria

Bei Wahl des Identitätsprotokolls OIDC zur Anbindung eines Service-Providers an die ID Austria muss dieses im sogenannten Authorization-Code-Flow verwendet werden. Dadurch wird eine Auslieferung der Identitätsmerkmale nach erfolgreicher Benutzerauthentifizierung über eine Back-Channel-Kommunikation erzwungen. Das heißt, der Service-Provider muss das ID-Token, das die Identitätsmerkmale beinhaltet, direkt von der ID Austria beziehen. Dazu erhält der Service-Provider vom Client einen Authorization-Code, der zur Abholung des zugehörigen ID-Tokens berechtigt. Der Authorization-Code wird dem Client von der ID Austria nach erfolgreicher Authentifizierung übermittelt. Zum Abholen des ID-Tokens muss sich der Service-Provider zusätzlich gegenüber der ID Austria mit Hilfe eines zuvor vereinbarten Secrets authentifizieren. Dadurch wird gewährleistet, dass ID-Token nur an authentifizierte Service-Provider ausgegeben werden. Durch die Umgehung des Clients bei der Übertragung des ID-Tokens und durch die dadurch notwendige Authentifizierung des Service-Providers an der ID Austria bietet der Authorization-Code-Flow von OIDC diverse Sicherheitsvorteile. Es ist also sinnvoll, dass eine Verwendung von OIDC im Rahmen der ID Austria auf diesen Flow beschränkt ist.

Bei der Verwendung von SAML2 stellt sich die Situation etwas anders dar. Hier werden von der ID Austria mit dem SAML2-POST-Binding und dem SAML2-Redirect-Binding zwei Modi unterstützt, bei denen die SAML2-Assertion mit den enthaltenen Identitätsmerkmalen jeweils über den Client der Benutzer*in von der ID Austria an den Service-Provider übertragen wird. Ein Nachteil ergibt sich hier gegenüber OIDC (im Authorization-Code-Flow) jedoch nicht, da die Authentifizierung des Service-Providers gegenüber der ID Austria bereits im Zuge der Übermittlung des initialen Authentifizierungs-Request erfolgt. Bei SAML2 muss dieser – im Gegensatz zu OIDC – immer signiert sein. Eine Authentifizierung des Service-Providers kann hier also bereits über die Signatur des Authentifizierungs-Request erfolgen. Da diese bei OIDC nicht zwingend enthalten ist, muss dort der Umweg über die Back-Channel-Kommunikation erfolgen.

5.4.2. Verschlüsselung der ausgelieferten Identitätsmerkmale

Um ausgelieferte Identifikationsmerkmale vor Kompromittierung zu schützen, werden diese im Zuge der Übertragung zwischen ID Austria und Service-Provider kryptographisch geschützt. Für beide von der ID Austria unterstützen Identitätsprotokolle (SAML2 und OIDC) ist es möglich, Schlüsselmaterial in den Metadaten des Service-Providers anzugeben. Über das angegebene Schlüsselmaterial können die Identitätsmerkmale vor Auslieferung an den Service-Provider verschlüsselt werden. Diese Metadaten und damit auch das Schlüsselmaterial werden im Zuge der Registrierung des Service-Providers am ID-Austria-System hinterlegt. Ein dynamisches Nachladen von Metadaten im Allgemeinen und von Schlüsselmaterial im Speziellen erfolgt nicht. Änderungen am hinterlegten Schlüsselmaterial sind daher stets über die vorgesehenen Prozesse der Service-Provider-Registrierung durchzuführen.

6. Vorgehensmodell für Service-Provider

Dieses Whitepaper fasst alle für Service-Owner und Service-Provider relevanten Informationen und Aspekte über die ID Austria zusammen. Als Ergänzung zu den bisher diskutierten Themenbereichen bietet dieser Abschnitt abschließend als Überblick ein Vorgehensmodell. Sinn des Modells ist es, Service-Ownern einen roten Faden für die Migration ihrer Service-Provider von Bürgerkarte/Handy-Signatur hin zur ID Austria zu bieten. Das Vorgehensmodell ist in Abbildung 5 dargestellt und im Folgenden beschrieben.

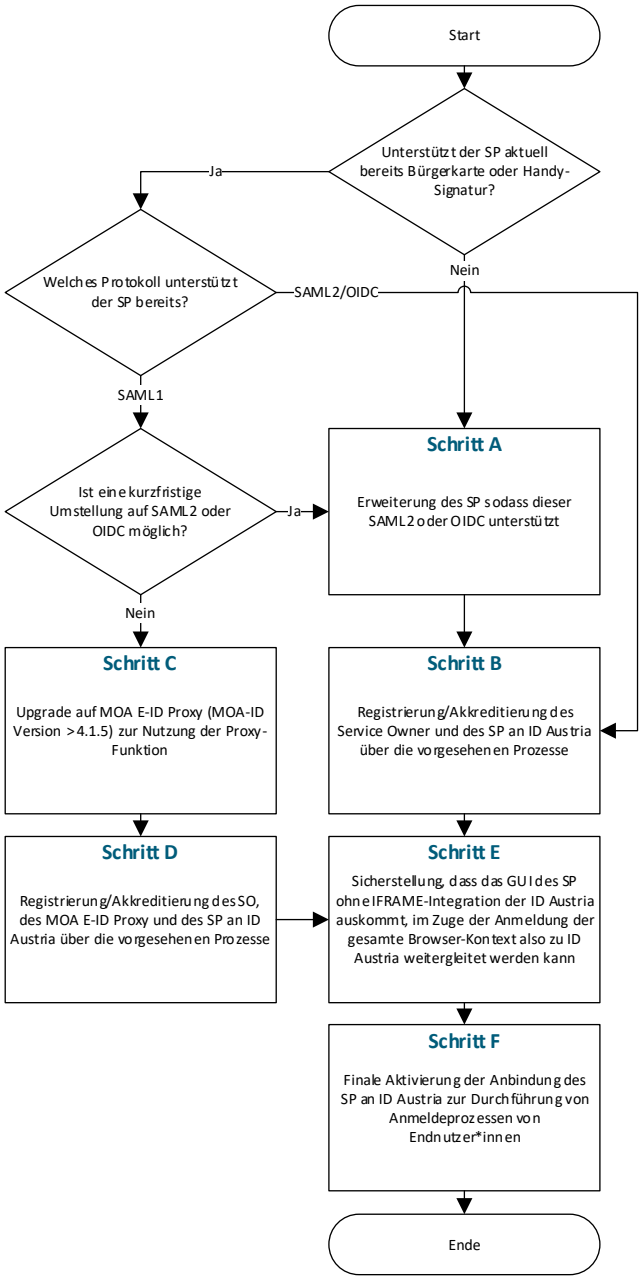

Abbildung 5. Vorgehensmodell zur Migration von Service-Providern aus die ID Austria.

Am Beginn der in Abbildung 5 dargestellten Abfolge von Tätigkeiten steht das Ziel, einen Service-Provider (SP) an die ID Austria anzubinden, um Benutzer*innen die Möglichkeit zu geben, sich über ihre persönliche ID Austria an diesem SP anzumelden. Die erste zentrale Frage, die sich unmittelbar danach stellt, ist, ob der SP bisher schon über eine Anbindung an das Bürgerkarte-/Handy-Signatur-Systems verfügt und Anmeldeprozesse über Handy-Signatur oder Bürgerkarte unterstützt. Abhängig davon sind teilweise unterschiedliche Folgeschritte durchzuführen.

Verfügt der SP bisher noch über keine Unterstützung von Handy-Signatur und/oder Bürgerkarte, muss der Service-Owner (d.h. die hinter dem SP stehende verantwortliche Organisation) in Schritt A fortfahren. Der SP muss also dahingehend erweitert werden, dass dieser die Identitätsmanagementprotokolle OIDC oder SAML2 unterstützt. Dies ist zwingend notwendig, um technisch eine Anbindung an die ID Austria herstellen zu können. Falls der SP keines dieser Protokolle unterstützt, muss eine entsprechende Unterstützung also ergänzt werden. Ist dies erledigt, kann in Schritt B fortgesetzt werden. In diesem Schritt werden Service-Owner und Service-Provider über die vorgesehenen Prozesse an der ID Austria registriert und ggf. akkreditiert. Details zu diesen Prozessen sind in Abschnitt 4.2 beschrieben. Nach erfolgreicher Registrierung/Akkreditierung kann bereits in Schritt E fortgesetzt werden. Im Rahmen dieses Schritts wird überprüft, ob das GUI des SP mit der temporären Weiterleitung des Client-Kontexts zur ID Austria (z.B. Browser-Redirect) umgehen kann. Details zu diesem Aspekt sind in Abschnitt 4.4.5 beschrieben. Ist sichergestellt, dass der SP mit der temporären Weiterleitung des Client-Kontexts umgehen kann, kann in Schritt F fortgesetzt werden, in dem im SP schließlich die Verwendung der ID Austria als externer Identity-Provider endgültig aktiviert wird, indem beispielsweise im SP der Button zum Initiieren des Logins freigeschalten wird. Für Service-Provider, die bisher noch keine Unterstützung für Handy-Signatur und/oder Bürgerkarte aufweisen, sind die durchzuführenden Schritte somit relativ linear (wenn auch potenziell etwas aufwändiger).

Verfügt der Service-Provider zu Beginn bereits über eine Unterstützung von Bürgerkarte und Handy-Signatur, stehen abhängig von verschiedenen Faktoren unterschiedliche Migrationspfade zur Verfügung. Alle Pfade sind in Abbildung 5 dargestellt.

Ist eine Unterstützung von Handy-Signatur und Bürgerkarte bereits gegeben, kann davon ausgegangen werden, dass der SP bereits über eine Anbindung an eine MOA-ID-Instanz verfügt. Hier stellt sich nun die Frage, über welches Protokoll der SP an MOA-ID angebunden ist. Im einfachsten Fall besteht bereits eine Anbindung über die Protokolle SAML2 oder OIDC. In diesem Fall kann unmittelbar in Schritt B gefolgt von den Schritten E und F wie oben beschrieben fortgesetzt werden.

Potenziell komplizierter ist der Sachverhalt, wenn der SP noch über das veraltete SAML1-Protokoll an MOA-ID angebunden ist. In diesem Fall stellt sich die Frage, ob der SP kurzfristig erweitert werden kann, sodass dieser auch die Protokolle SAML2 oder OIDC unterstützt. Ist dies der Fall, kann direkt in Schritt A fortgesetzt werden, indem genau jene Protokollunterstützung im SP ergänzt wird. Nach Schritt A können dann unmittelbar die Schritte B, E und F wie oben beschrieben folgen, um die Migration auf die ID Austria abzuschließen. Ist hingegen eine kurzfristige Erweiterung des SP nicht möglich, muss in Schritt C fortgesetzt werden. In diesem muss MOA-ID auf die aktuelle Version aktualisiert werden, sodass MOA-ID (auch) als MOA E-ID Proxy verwendet werden kann. Alle relevanten Details zur Verwendung des MOA E-ID Proxy sind in Abschnitt 4.4 beschrieben. Ist MOA-ID aktualisiert, wird in Schritt D fortgesetzt. In diesem wird der SP, der verantwortliche SO und auch der MOA E-ID Proxy entsprechend den definierten Prozessen bei der

ID Austria registriert. Details zu diesem speziellen Registrierungs-/Akkreditierungsprozess finden sich in Abschnitt 4.4.4. Ist die Registrierung/Akkreditierung erfolgreich, kann wiederum in Schritte E gefolgt von Schritt F fortgesetzt werden, um die Migration abzuschließen.

7. Fazit und weiterführende Informationen

Die ID Austria ist das neue österreichische nationale elektronische Identitätsmanagementsystem und tritt die Nachfolge von Bürgerkarte und Handy-Signatur an. Service-Provider könnend die ID Austria nutzen, um Benutzer*innen sicher zu authentifizieren und anzumelden. Zudem ermöglicht die ID Austria Benutzer*innen die Erstellung qualifizierter elektronischer Signaturen, die rechtlich handschriftlichen Unterschriften gleichgestellt sind.

Im Vergleich zu Bürgerkarte und Handy-Signatur bieten die ID Austria und ihre technische Umsetzung diverse Vorteile. So kann die ID Austria auch in rein mobile App-basierte Anwendungsszenarien integriert werden. Durch strengere Benutzer- und Service-Provider-Registrierungsprozesse wird zudem auch auf organisatorischer Ebene ein noch höheres Maß an Sicherheit und Vertrauenswürdigkeit sichergestellt.

Für Service-Owner und deren Service-Provider ergibt sich aus dem Auslaufen von Bürgerkarte und Handy-Signatur und der Einführung der ID Austria punktuell Handlungsbedarf. Dies betrifft primär die nun notwendige Registrierung und Akkreditierung von Service-Ownern und Service-Providern an der ID Austria sowie auch die etwas andere technische Anbindung.

Alle für Service-Owner und Service-Provider relevanten Aspekte wurden in diesem Whitepaper zusammengefasst und diskutiert. Das Whitepaper soll damit als zuverlässige Informationsquelle dienen und Service-Providern eine Migration von Bürgerkarte und Handy-Signatur auf die ID Austria erleichtern.

Um den Umfang des Dokuments im Rahmen zu halten, wurde in einigen Aspekten bewusst auf einen höheren Detailierungsgrad verzichtet. Interessierte Leser*innen seien für weiterführende Informationen daher auf folgende Quellen verwiesen:

- **EGIZ-Web.** Informationen zur ID Austria für Service-Provider im Web: https://eid.egiz.gv.at
- **oesterreich.gv.at.** Allgemeine Informationen zur ID Austria auf oesterreich.gv.at: https://www.oesterreich.gv.at/id-austria.html
- **Mailing-Liste.** Registrierung zur Mailing-Liste für Service-Provider zum Erhalt aktueller Informationen: https://labs.cio.gv.at/mailman/listinfo/eid-info
- **Workshops.** Informationsveranstaltungen für Service-Provider: https://eid.egiz.gv.at/infos/veranstaltungen/