A-SIT Plus GmbH

ID Austria

Technisches Whitepaper für Endnutzer*innen

27. Dezember 2021

Inhaltsverzeichnis

1. Einleitung ... 4
2. Die ID Austria im Überblick ... 6
   2.1. Funktionen der ID Austria ... 6
   2.2. Grundlegende Eigenschaften der ID Austria ... 6
   2.3. Historie: Von der Bürgerkarte und Handy-Signatur zur ID Austria ... 8
   2.4. Rechtliche Grundlagen ... 10
3. Der Weg zur persönlichen ID Austria ... 11
   3.1. Registrierung der ID Austria ... 11
      3.1.1. Registrierungsschritte zur Aktivierung der ID Austria ... 11
      3.1.2. Ausprägungen der ID Austria ... 12
      3.1.3. Technische Voraussetzungen einer Registrierung ... 13
      3.1.4. Registrierungsvarianten ... 13
   3.2. Verwendung der ID Austria ... 16
      3.2.1. Anmeldung bei einem Service-Provider ... 16
      3.2.2. Erstellen einer qualifizierten Signatur ... 18
   3.3. Widerruf der ID Austria ... 20
   3.4. Verlustes oder Diebstahls des mobilen Geräts ... 21
   3.5. Verlust oder Diebstahl von Anmeldedaten ... 24
4. Hinter den Kulissen ... 25
   4.1. Architekturüberblick ... 25
   4.2. Eindeutige Identifikatoren ... 27
      4.2.1. ZMR-Zahl ... 27
      4.2.2. Stammzahl ... 28
      4.2.3. Bereichsspezifisches Personenkennzeichen (bPK) ... 28
5. Sicherheit und Datenschutz ... 30
   5.1. Sichere Registrierungs- und Akkreditierungsprozesse ... 30
   5.2. Sichere und korrekte Auslieferung von persönlichen Attributen ... 30
   5.3. Schutz der Privatsphäre von personenbezogenen Daten ... 31
   5.4. Kontrolle der vereinfachten Weiterverwendung einer vorherigen Authentifizierung ... 31
   5.5. Sicherheitselemente in Smartphones ... 32
      5.5.1. Android: Secure Elements ... 32

5.5.2. iOS: Secure Enclave 32
6. Fazit 33

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. Authentifizierungsmethoden basierend auf mehreren unterschiedlichen Authentifizierungsfaktoren finden hingegen nur langsam Akzeptanz und Verbreitung. In Österreich ist eine solche sichere Methode der Mehrfaktorauthentifizierung an Online-Anwendungen schon seit Jahren in Form der Bürgerkarte bzw. der Handy-Signatur verfügbar. Handy-Signatur und Bürgerkarte bieten seit jeher neben der sicheren und zuverlässigen Benutzerauthentifizierung Benutzer*innen auch die Möglichkeit, Dokumente elektronisch qualifiziert zu unterschreiben. Die qualifizierte elektronische Signatur ermöglicht auf technischer Ebene die zuverlässige Identifizierung nachträglicher Änderungen von signierten Inhalten und ist rechtlich der handschriftlichen Unterschrift weitgehend gleichgestellt.

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) in Online-Verfahren 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 grundsätzlich 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 innerhalb einer App zuverlässig über die ID Austria zu authentifizieren.

---

[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

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

Für eine strukturierte Beschreibung dieser Inhalte wird in diesem Dokument nachfolgend ein kurzer Überblick betreffend den Funktionsumfang und die Eigenschaften der ID Austria geboten. Im Anschluss wird der Lebenszyklus einer ID Austria beschrieben, der mit der Registrierung startet und einem möglichen Widerruf oder Ablauf der Gültigkeit endet. Abschließend werden relevante Informationen über ausgewählte Sicherheits- und Datenschutzaspekte behandelt. Der Fokus wird dabei speziell auf für Bürger*innen relevante Informationen gelegt.

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 Dienstanbietern (Service-Owner), die Funktionalität des Logins bzw. der Anmeldung von Benutzer*innen über deren persönliche ID Austria in ihre Service-Provider (Web-Applikationen, Apps, etc.) zu integrieren. Bürger*innen können sich dabei mit folgenden Authentifizierungsverfahren bei einem Service-Provider anmelden:

- **ID Austria.** Anmeldung mittels ID Austria (ehemals Handy-Signatur bzw. Bürgerkarte) bzw. vereinfachte Weiterverwendung der ID Austria[3] gemäß E-Government-Gesetz (EGovG).
- **EU-Login.** Anmeldung mittels EU-Login (via eIDAS-Framework) für Benutzer*innen mit ausländischer elektronischer Identität (eID).

Neben der sicheren Authentifizierung von Benutzer*innen bietet die ID Austria auch die Möglichkeit, qualifizierte – und damit rechtsgültige – elektronische Unterschriften von Benutzer*innen erstellen zu lassen. 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. Eine Mehrfaktorauthentifizierung setzt zumindest zwei unterschiedliche Authentifizierungsfaktoren (z.B. Fingerprint (Faktor „Inhärenz“) und Eingabe eines Passworts (Faktor „Wissen“) voraus, die zur Anmeldung bei einem Service-Provider von Bürger*innen nachgewiesen werden müssen.
- **Staatliche Register als Basis.** Zuverlässige Identifizierung von Benutzer*innen über eindeutigen (jedoch sektorspezifischen) Identifikator (verknüpft mit österreichischen staatlichen Registern) und Minimum Dataset (bestehend aus Vornamen, Familiennamen und Geburtsdatum). Eine eindeutige Identifizierung von Bürger*innen stellt eine

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

Grundvoraussetzung für die sichere Nutzung des österreichischen E-Government Angebots dar.

- **Unterstützung ausländischer nationaler eID-Systeme.** Unterstützung der Authentifizierung von Benutzer*innen mit notifizierter ausländischer eID über Anbindung der ID Austria an das europäische eIDAS-Framework[4].
- **Behördlicher Ausstellungsprozess.** Registrierungs- und Ausstellungsprozess einer ID Austria für Bürger*innen in behördlicher Qualität. Bürger*innen müssen zur Registrierung der ID Austria persönlich bei einer ermächtigten Registrierungsbehörde erscheinen, um ihre Identität nachzuweisen.
- **Grenzüberschreitende Verwendbarkeit.** Tauglichkeit für den grenzüberschreitenden Einsatz der ID Austria zum Beispiel zur Anmeldung an Service-Providern anderer EU-Mitgliedsstaaten. Mit einer grenzüberschreitenden Verwendbarkeit der ID Austria können die in Österreich staatlich anerkannten Authentifizierungsmittel auch international genutzt werden, was die Anzahl an potenziell verfügbaren Services vor allem in Zukunft erhöhen wird.
- **Mobile-Ready.** Unterstützung von mobilen Nutzungsszenarien wie zum Beispiel App-basierte Service-Provider. Bisher war es für Service-Provider nicht möglich, die Handy-Signatur für eine Authentifizierung ausschließlich in einer mobilen App zu verwenden, da die Sicherheit des Authentifizierungsvorgangs unter anderem von der Verwendung zweier verschiedener Geräte (PC und Mobiltelefon/Smartphone) abhing. Die ID Austria bietet auch rein app-basierten Service-Providern die Möglichkeit, eine sichere Authentifizierung mit ID Austria zu integrieren.
- **Erweitertes Attribut-Set.** Auslieferung von weiteren persönlichen Attributen an Service-Provider. Zusätzliche Attribute werden aus zugänglichen Datenquellen (z.B. Verwaltungsregister) bezogen und nach Zustimmung der Benutzer*in an anfragende Service-Provider ausgeliefert. Benutzer*innen können somit nach wie vor bei jedem Anmeldeprozess entscheiden, ob sie einem Service-Provider vertrauen und der Weitergabe von persönlichen Merkmalen einwilligen.
- **Nachhaltigkeit.** Nachhaltige und anpassungsfähige technische Architektur, die sich durch einen modularen Aufbau, eine einfache Anbindung von Service-Providern über Standard-Identitätsprotokolle sowie die künftige Anbindung an den österreichischen Register- und Systemverbund auszeichnet.
- **Qualifizierte Signatur als Zusatzfeature.** Neben einer möglichen Anmeldung an Service-Providern bietet die ID Austria Bürger*innen auch die Möglichkeit, rechtsgültige qualifizierte elektronische Signaturen (z.B. PDF-Signaturen) zu erstellen.

[4] 2014 veröffentlichte die EU eine Verordnung, die die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen (eIDAS) reguliert. Seit dem Außerkrafttreten des Signaturgesetzes in 2016 ist die eIDAS Verordnung in Bezug auf Signatur- und Vertrauensdienste anzuwenden.

Die Summe dieser Eigenschaften bringt nicht nur für Bürger*innen zahlreiche Vorteile, sondern macht die ID Austria auch für Service-Provider zu einer attraktiven Identitätsmanagementlösung und berücksichtigt damit die Interessen aller im System beteiligten Akteure.

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 hinter 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[6] 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.

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

[6] Qualifizierte Zertifikate werden für die Erstellung von qualifizierten elektronischen Signaturen benötigt, die einer eigenhändigen Unterschrift einer Person gleichgestellt sind.

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 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 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)[7] und dessen letzte Novelle[8], sowie durch die Verordnung der Europäischen Union über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS Verordnung[9]) 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[10]) 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.

---

[7] E-Government-Gesetz: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003230

[8] Novelle zum E-Government-Gesetz: https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2020_I_169/BGBLA_2020_I_169.html

[9] IDAKS Verordnung: https://eur-lex.europa.eu/eli/reg/2014/910/oj?locale=de

[10] DSGVO: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32016R0679

3. Der Weg zur persönlichen ID Austria

In diesem Kapitel wird der gesamte Lebenszyklus der persönlichen ID Austria einer Bürger*in beschrieben, der mit der Registrierung startet und einem möglichen Widerruf oder dem Auslaufen der Gültigkeit endet. Nachfolgend werden die einzelnen Phasen des ID-Austria-Lebenszyklus mit Fokus auf sicherheitstechnische Belange näher beschrieben.

3.1. Registrierung der ID Austria

Im Zuge der Registrierung wird die persönliche ID Austria einer Bürger*in erstellt. Nach erfolgreicher Registrierung kann die ID Austria der Bürger*in in weiterer Folge z.B. für Anmeldungen an Service-Providern verwendet werden. Dementsprechend ist eine erfolgreiche Registrierung eine notwendige Voraussetzung für eine spätere Verwendung (oder Verwaltung) der ID Austria durch die Benutzer*in. Die Registrierung der ID Austria kann prinzipiell von allen natürlichen Personen vorgenommen werden, die im österreichischen Stammzahlenregister (SZR) aufgefunden werden können. Hierbei gibt es unterschiedliche Varianten, wie Personen über das SZR auffindbar sein können. Dazu zählen:

1) Personen, die ihren festen Wohnsitz in Österreich haben, sind im ZMR eingetragen und somit auch über das SZR auffindbar.

2) Personen, die ihren festen Wohnsitz im Ausland haben, können manuell, z.B. im Zuge der Registrierung der ID Austria, im Ergänzungsregister für natürliche Personen (ERnP) erfasst werden. Personen, die sich mit einer eIDAS-konformen ausländischen eID an einem österreichischen Service-Provider anmelden werden im Zuge des ersten Anmeldeprozesses automatisch im ERnP eingetragen.

3.1.1. Registrierungsschritte zur Aktivierung der ID Austria

Im Rahmen der Registrierung und Erstellung einer ID Austria sind prinzipiell die folgenden notwendigen Schritte vorgesehen:

- **Identitätsfeststellung:** Die Identität der Bürger*innen wird durch eine öffentliche Behörde oder eine andere autorisierte Organisation zweifelsfrei festgestellt. Dazu müssen Bürger*innen persönlich anwesend sein und ihre Identität über ein gültiges Ausweisdokument (Reisepass, Personalausweis, etc.) nachweisen. Die Identitätsfeststellung über einen physischen Amtsweg garantiert die Authentizität von Benutzer*innen der ID Austria und stellt sicher, das elektronische Identitäten (d.h. die persönliche ID Austria) mit der korrekten natürlichen Person verknüpft wird.

- **Erstellung der ID Austria:** Im ID-Austria-System wird die ID Austria der jeweiligen Person erstellt bzw. angelegt. Unter anderem umfasst dies die Ausstellung eines qualifizierten

Signaturzertifikats[11] für die zu registrierende Person und die Verknüpfung dieses Zertifikats mit ihrer (verschlüsselten) Stammzahl.

- **Registrierung von Authentifizierungsfaktoren:** Benutzer*innen werden mit Authentifizierungsfaktoren (Zertifikaten) ausgestattet, mit Hilfe derer sie sich in weiterer Folge zur Verwendung ihrer ID Austria am ID-Austria-System authentifizieren können. Authentifizierungsfaktoren umfassen ein geheimes Passwort und ein mobiles Endnutzergerät, das kryptographisch an die ID Austria der Benutzer*in gebunden wird. Dazu wird am mobilen Gerät ein asymmetrisches Schlüsselpaar erstellt, über das ein Challenge-Response-Verfahren umgesetzt wird. Da der Zugriff auf den privaten Schlüssel zusätzlich über eine lokale Authentifizierungsmethode (Face-ID/Fingerprint) am mobilen Gerät geschützt ist, ist sichergestellt, dass die mit dem Gerät verknüpfte ID Austria ausschließlich von der legitimen Benutzer*in verwendet werden kann.

Die drei oben beschriebenen Schritte stellen die wesentlichen Elemente der Registrierung einer persönlichen ID Austria für Bürger*innen dar. Die Reihenfolge der Durchführung dieser drei Schritte ist jedoch nicht fix vorgegeben und kann je nach Umsetzung des Registrierungsprozesses variieren.

3.1.2. Ausprägungen der ID Austria

Die Einführung der ID Austria bedingt, dass bestehende Benutzer*innen der Handy-Signatur und Bürgerkarte auf die neue Lösung umsteigen müssen. Um diesen Umstieg so fließend wie möglich zu gestalten, ist in einer Übergangsphase die ID Austria in zwei Ausprägungen verfügbar. Bürger*innen können sich dementsprechend zwischen den folgenden zwei Varianten entscheiden:

- **ID Austria:** In dieser Variante erfolgt die Registrierung der ID Austria entsprechend den oben genannten Schritten. Benutzer*innen steht damit sofort die gesamte Funktionalität der ID Austria zur Verfügung, die Registrierung bedingt jedoch ein persönliches Erscheinen der Benutzer*in bei einer zur Registrierung der ID Austria befugten Behörde.

- **Basis ID Austria:** In dieser Variante wird eine bestehende Handy-Signatur oder Bürgerkarte einer Person in eine sogenannten Basis ID Austria umgewandelt. Hierbei wird ausschließlich die ID Austria der jeweiligen Person erstellt und es werden deren Authentifizierungsfaktoren registriert. Die Identitätsfeststellung vor Ort bei der Behörde ist nicht notwendig, da diese bereits bei der Aktivierung der Bürgerkarte/Handy-Signatur vorgenommen wurde. Die resultierende Basis ID Austria hat bis auf wenige Ausnahmen den gleichen Funktionsumfang wie eine vollständige ID Austria. Einschränkungen ergeben sich aber bei der Bereitstellung zusätzlicher mit der ID Austria verknüpfter Attribute[12]. Die Gültigkeit der Basis ID Austria ist auf die verbleibende Gültigkeitsdauer des ursprünglich mit der Handy-Signatur oder Bürgerkarte verknüpften qualifizierten Signaturzertifikats beschränkt. Eine Verlängerung der Gültigkeit der Basis ID Austria ist nicht

[11] Qualifizierte Zertifikate ermöglichen die Erstellung von qualifizierten elektronischen Signaturen, die einer handschriftlichen Unterschrift gleichgestellt sind und als Identifikationsmittel zur Authentifizierung am Vertrauensdiensteanbieter des ID-Austria-Systems dienen.

[12] Konkret darf das ID-Austria-System im Falle einer Basis ID Austria an Service-Provider neben dem bPK nur den Mindestdatensatz (Vorname, Nachname, Geburtsdatum) ausliefern.

möglich. Nach Ablauf der Gültigkeit ihrer Basis ID Austria muss die jeweilige Person eine ID Austria über die vorgesehenen Registrierungsprozesse registrieren, sofern diese Person die Funktionalität der ID Austria weiterhin nutzen möchte.

3.1.3. Technische Voraussetzungen einer Registrierung

Die Registrierung einer ID Austria oder einer Basis ID Austria bedingt die Installation und Initialisierung der Digitales-Amt-App[13]. Die Digitales-Amt-App ist eine mobile App mit breitem Funktionsumfang, die Bürger*innen kostenlos zur Verfügung gestellt wird. So dient diese App unter anderem als zentraler Einstiegspunkt in diverse mobile E-Government-Services. Darüber hinaus bietet die App auch die notwendigen Benutzerschnittstellen für Bürger*innen zur Interaktion mit dem ID-Austria-System.

Die Digitales-Amt-App wird im Zuge der Registrierung einer persönlichen ID Austria an den Vertrauensdiensteanbieter[14] und das ID-Austria-System gebunden (falls eine Bindung nicht schon durch eine frühere Nutzung der App durchgeführt wurde). Konkret werden bei der Initialisierung der Digitales-Amt-App kryptographische Schlüssel in der sicheren Hardware des Smartphones erzeugt, welche in weiterer Folge für die Authentifizierung gegen den Vertrauensdiensteanbieter (VDA) oder, im Falle einer vereinfachten Weiterverwendung der ID Austria, für die Authentifizierung gegen den Identity Provider (IDP) des ID-Austria-Systems verwendet werden. Für die Authentifizierung gegen den VDA bzw. gegen den IDP werden dabei unterschiedliche Schlüssel verwendet. Smartphones älterer Generationen, die nicht über eine sichere Hardware zur Erzeugung und Speicherung der Schlüssel oder über biometrische Authentifizierungsmethoden wie Fingerprint/Face-ID verfügen, dürfen aus Sicherheitsgründen nicht verwendet werden. Diese spezielle Hardware (Secure Element/Enclave) ist essenziell für die Sicherheit eines Authentifizierungsvorgangs und muss daher verpflichtend verwendet werden.

3.1.4. Registrierungsvarianten

Für die Registrierung einer ID Austria stehen Bürger*innen mehrere Varianten zur Verfügung. Die verschiedenen Varianten ergeben sich aus dem Umstand, dass gewisse Teile des Registrierungsprozesses vor Ort bei einer ermächtigten Behörde und andere Teile außerhalb der Behörde durch die Benutzer*in selbst durchgeführt werden müssen. Konkret können Bürger*innen somit entscheiden, ob sie den Registrierungsprozess zu Hause starten und in der Behörde abschließen, oder aber umgekehrt, in der Behörde starten und zu Hause abschließen, möchten.

Start: zu Hause → Abschluss: Behörde

Entscheidet sich eine Person dafür, den Registrierungsprozess zunächst zu Hause zu starten und dann später in einer Behörde abzuschließen, stehen wiederum zwei Varianten zur Verfügung:

- **Variante 1 – Online-Vorregistrierungssystem:** In der ersten Variante führen Bürger*innen zunächst zu Hause eine Vorregistrierung durch, im Rahmen derer über ein bereitgestelltes

[13] Digitales-Amt-App: https://www.oesterreich.gv.at/ueber-oesterreichgvat/faq/app_digitales_amt.html
[14] Vertrauensdiensteanbieter erfüllen Anforderungen des Vertrauensdienstegesetzes (VDG) sowie der Vertrauensdiensteverordnung (VDV) und stellen damit die Vertrauenswürdigkeit von Transaktionen im Internet sicher.

Online-Vorregistrierungssystem notwendige Authentifizierungsfaktoren festgelegt und registriert werden. Im Anschluss an diese Vorregistrierung wird die Registrierung in der Behörde durch die Durchführung der Identitätsfeststellung abgeschlossen.

- **Variante 2 – Handy-Signatur:** Für die Wahl der zweiten Variante ist eine Voraussetzung, dass eine Person bereits über eine gültige Handy-Signatur verfügt. In diesem Fall kann die Vorregistrierung über das Vorregistrierungssystem entfallen. Notwendige Daten werden in diesem Fall statt vom Online-Vorregistrierungssystem direkt von der Handy-Signatur bezogen.

Start: Behörde → Abschluss: zu Hause

Alternativ kann sich eine Person auch dafür entscheiden, den Registrierungsprozess in der Behörde zu starten und dann im Anschluss zu Hause abzuschließen. Entscheidet sich eine Person für diese Variante, stehen ihr wiederum drei unterschiedliche Varianten zur Verfügung. Diese unterscheiden sich hauptsächlich in der Art und Weise, wie die Digitales-Amt-App an die ID Austria der jeweiligen Person gebunden wird, um in weiterer Folge als Authentifizierungsfaktor fungieren zu können. Konkret stehen folgende Varianten zur Auswahl:

- **Variante 1 – App:** In dieser Variante bringt die zu registrierende Person zur Identitätsfeststellung in der Behörde bereits ihr Smartphone mit installierter Digitales-Amt-App mit. In der Behörde erfolgt die Identitätsfeststellung, sowie die kryptographische Bindung der Digitales-Amt-App an die eben erstellte ID Austria. Im Anschluss schließt die Person die Registrierung zu Hause durch Festlegung von Username und Passwort ab. Das Endresultat dieser Variante entspricht der Variante, in der die Registrierung zu Hause gestartet und in der Behörde abgeschlossen wird. In beiden Varianten verfügen Benutzer*innen nach Abschluss der Registrierung über Usernamen/Passwort und eine Digitales-Amt-App, die kryptographisch an die ID Austria gebunden ist.

Abbildung 1. Registrierung unter Verwendung der Digitales-Amt-App

- **Variante 2 – SMS-TAN:** In dieser Variante bringt eine Person zur Identitätsfeststellung in der Behörde zwar ihr Mobiltelefon mit, hat auf diesem jedoch keine Digitales-Amt-App installiert. Die Bindung des Mobiltelefons an die ID Austria der zu registrierenden Person erfolgt daher via SMS-TAN. Vor Ort in der Behörde wird die Telefonnummer der Person über Zusendung eines SMS-TAN überprüft und abgespeichert. Im Anschluss schließt die Person die Registrierung zu Hause ab. Dabei werden einerseits Username/Passwort festgelegt und andererseits die mittlerweile installierte Digitales-Amt-App an die ID Austria der jeweiligen Person gebunden. Der Besitz des Mobiltelefons wird dabei über Zusendung eines SMS-TAN an die zuvor verifizierte und gespeicherte Telefonnummer überprüft. Das Endresultat dieser Variante entspricht wiederum jenen Registrierungsvorgängen, die eine Verwendung der Digitales-Amt-App bereits bei der Behörde vorsehen. Nach Abschluss der Registrierung verfügt die registrierte Person über Username/Passwort und eine Digitales-Amt-App, die kryptographisch an die ID Austria gebunden ist. Zusätzlich wurde auch die Rufnummer über einen SMS-TAN an die ID Austria der Person gebunden.

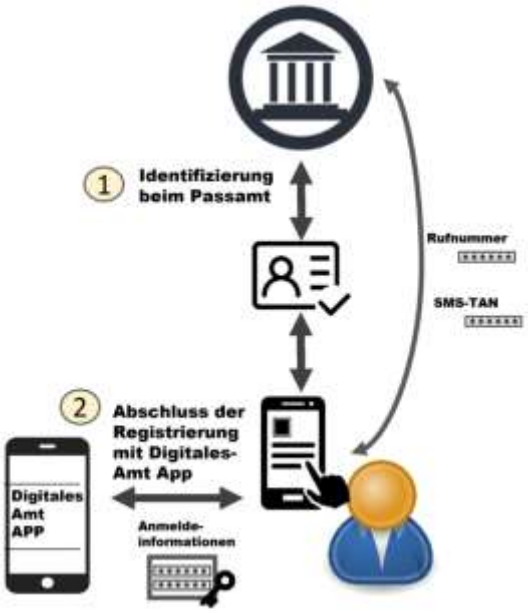

Abbildung 2. Registrierung mit SMS-TAN

- **Variante 3 – Post-TAN:** In dieser Variante erscheint die Person bei der Behörde zur Registrierung ihrer ID Austria, bringt jedoch kein Mobiltelefon mit. In dieser Variante erhält die Person bei der Behörde lediglich einen Ausdruck mit Freischalt-Code, eine Gerätebindung findet bei der Behörde noch nicht statt. Die Registrierung wird durch die jeweilige Person zu Hause unter Verwendung des Freischaltcodes abgeschlossen. Das angelegte Konto wird im Rahmen eines zweistufigen Prozesses unter Verwendung eines per Post versendeten TAN an die ID Austria der Person gebunden. Dabei erfolgt auch eine Bindung der Digitales-Amt-App. Die Telefonnummer der Person wird in dieser Registrierungsvariante nicht verifiziert.

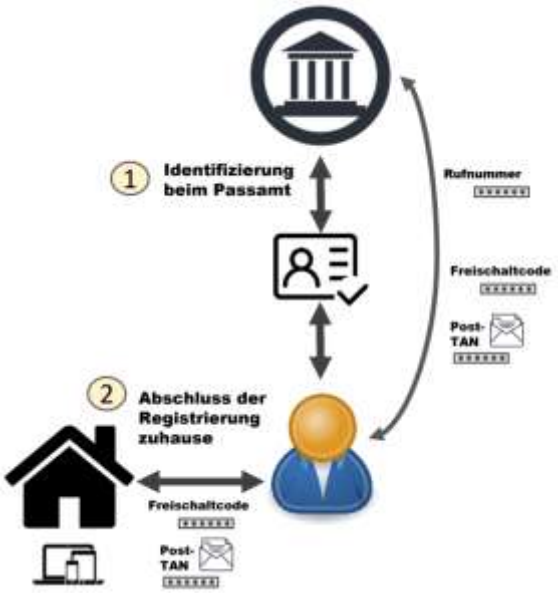

Abbildung 3. Registrierung mit Post-TAN

Unabhängig von der gewählten und durchgeführten Registrierungsvariante kann nach erfolgter Registrierung von folgenden Voraussetzungen ausgegangen werden:

- Die Identität der registrierten Person wurde durch die Behörde festgestellt.
- Für die Bürger*in wurde eine ID Austria im ID-Austria-System angelegt.
- Die registrierte Person verfügt über Username/Passwort. Diese Zugangsdaten dienen als Authentifizierungsfaktor zur VDA-basierten Authentifizierung gegen das ID-Austria-System im Zuge der Verwendung der ID Austria.
- Bürger*innen haben die Digitales-Amt-App auf ihren Smartphones installiert und diese ist kryptographisch an ihre ID Austria gebunden.

3.2. Verwendung der ID Austria

Eine registrierte ID Austria kann von einer registrierten Person zur Anmeldung an einem Service-Provider oder zur Erstellung einer qualifizierten Signatur verwendet werden. Die beiden möglichen Anwendungsfälle der ID Austria werden nachfolgend näher beschrieben.

3.2.1. Anmeldung bei einem Service-Provider

Die mögliche Anmeldung bei einem Service-Provider mittels ID Austria stellt den Hauptanwendungsfall dar. Im Zuge einer Anmeldung erfolgt eine Authentifizierung gegen das ID-Austria-System unter Verwendung der persönlichen ID Austria. Das ID-Austria-System fungiert gegenüber dem Service-Provider als IDP. Für die Authentifizierung gegen das ID-Austria-System stehen drei unterschiedliche Optionen zur Verfügung:

1) **Authentifizierung am VDA:** Mehrfaktor-Authentifizierung unter Verwendung der im Zuge der Registrierung festgelegten Authentifizierungsfaktoren (Passwort, kryptographisch gebundene Digitales-Amt-App).

2) **Vereinfachte Weiterverwendung einer Authentifizierung**: Authentifizierung via vereinfachte Weiterverwendung einer vorherigen erfolgreichen Mehrfaktor-Authentifizierung am VDA unter Verwendung einer kryptographischen Bindung zum IDP der ID Austria, oder einer vorherigen erfolgreichen Authentifizierung über das eIDAS-Framework.

3) **eIDAS-Anmeldung**: Anmeldung mit einer eIDAS-konformen ausländischen elektronischen Identität. Eine Authentifizierung über eine ausländische elektronische Identität erfolgt über das eIDAS-Framework und den zentralen nationalen eIDAS-Knoten.

Nachfolgend wird die Authentifizierung am VDA sowie das Konzept der vereinfachten Weiterverwendung einer Benutzer-Authentifizierung im Detail beschrieben. Bei einer eIDAS-Anmeldung handelt es sich um länderspezifische Authentifizierungsprozesse unter Verwendung einer ausländischen elektronischen Identität. Da es sich dabei um ein alternatives Authentifizierungsverfahren handelt, betrifft eine eIDAS-basierte Anmeldung den Lebenszyklus der ID Austria nicht direkt und wird hier nicht näher beschrieben.

3.2.1.1. Authentifizierung am VDA

Bei einer erstmaligen Anmeldung mit ID Austria an einem Service-Provider wird die zu authentifizierende Person vom IDP an den VDA (A-Trust) weitergeleitet. Während der Authentifizierung muss ein Passwort bereitgestellt und eine lokale biometrische Authentifizierung via Fingerprint/Face ID über die Digitales-Amt-App am Smartphone durchgeführt werden, sodass die Digitales-Amt-App als zweiter Authentifizierungsfaktor gegen den VDA verwendet werden kann. Durch Verwendung der Faktoren Passwort und Digitales-Amt-App ergibt sich insgesamt eine Mehrfaktor-Authentifizierung.

Nach einer erfolgreichen Authentifizierung am VDA wird der Zeitpunkt der VDA-Anmeldung der jeweiligen Person in einem speziellen Datenspeicher (User Store) des ID-Austria-Systems eingetragen oder aktualisiert. Dieser Zeitpunkt stellt den letzten Zeitpunkt einer durchgeführten Authentifizierung am VDA dar und ist für die Gültigkeit einer vereinfachten Weiterverwendung einer Authentifizierung entscheidend, da Service-Provider die höchstmögliche Dauer einer zurückliegenden VDA-Authentifizierung bestimmen können. Service-Provider können demnach indirekt vorgeben, wann Benutzer*innen eine Authentifizierung am VDA durchführen müssen, um ihren angebotenen Service zu nutzen.

3.2.1.2. Vereinfachte Weiterverwendung einer Authentifizierung

Das Konzept der vereinfachten Weiterverwendung wurde mit der ID Austria neu eingeführt, um die Benutzerfreundlichkeit von Anmeldeprozessen zu erhöhen. Nach einer erfolgreichen VDA-basierten Authentifizierung können Benutzer*innen ihr mobiles Gerät unter Verwendung der Digitales-Amt-App an den IDP des ID-Austria-Systems kryptographisch binden. Mit dieser Bindung kann in weiterer Folge eine vereinfachte Authentifizierung gegen den IDP des ID-Austria-Systems erfolgen. Nach einer lokalen Authentifizierung über Face-ID oder Fingerprint erfolgt die Authentifizierung gegen den IDP des ID-Austria-

Systems über die zuvor erstellte kryptographische Bindung des mobilen Geräts[15]. Dadurch entfällt im Vergleich zu einer Authentifizierung via VDA die Eingabe von Username/Passwort.

Die Sicherheit dieser vereinfachten Weiterverwendung einer vorhergehenden 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 zum ID-Austria-System 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.

Obwohl somit die Sicherheit der sogenannten vereinfachten Weiterverwendung (vorheriger Authentifizierungen) gegeben ist, ermöglicht die ID Austria angebundenen Service-Providern trotzdem eine weitgehende Kontrolle der Verwendung dieses Features. So kann ein Service-Provider im Zuge seiner Registrierung/Akkreditierung die Unterstützung der vereinfachten Weiterverwendung einer vorherigen Authentifizierung über Definition diverser Parameter steuern. Im Extremfall kann für einen Service-Provider so die Verwendung der vereinfachten Weiterverwendung einer vorherigen Authentifizierung vollkommen unterbunden und Benutzer*innen stets zur Durchführung VDA-basierter Authentifizierungsprozesse gezwungen werden. Es ist dadurch jedem Service-Provider überlassen, das geeignete Mittelmaß zwischen Sicherheit und Benutzerfreundlichkeit zu wählen.

Für die Erstellung einer kryptographischen Bindung, die für eine vereinfachte Weiterverwendung einer Authentifizierung verwendet werden kann, authentifizieren sich Bürger*innen gegen den VDA unter Verwendung der Digitales-Amt-App. Alternativ kann eine kryptographische Bindung zum zentralen IDP des ID-Austria-Systems auch unter Verwendung einer ausländischen eIDAS-konformen elektronischen Identität (eID) erstellt werden. In diesem Fall erfolgt die Authentifizierung für die Erstellung der Bindung über die ausländische eID.

3.2.2. Erstellen einer qualifizierten Signatur

Neben der möglichen Anmeldung bei einem Service-Provider, bietet die ID Austria die Option zur Erstellung einer qualifizierten Signatur (PDF-Signatur). Das dafür nötige qualifizierte Zertifikat bzw. der mit diesem Zertifikat verknüpfte private Signaturschlüssel werden zentral und sicher durch den VDA verwaltet. Zur Erstellung einer qualifizierten Signatur authentifiziert sich die Benutzer*in mit den für ihre ID Austria registrierten Authentifizierungsfaktoren am VDA (bspw. User-ID/Passwort und Fingerprint in der App), woraufhin dieser die Signatur für die Benutzer*in erstellt.

Die Erstellung einer qualifizierten Signatur kann clientseitig sowohl im Web-Browser als auch in nativen mobilen Apps gestartet werden. In beiden Fällen können diese Client-Komponenten (mobile App, Web-Browser) den Signaturerstellungsprozess selbstständig triggern oder dies im Zusammenspiel mit einer serverseitigen Service-Provider-Komponente durchführen. Beispielsweise könnten App oder Web-Browser lediglich als Benutzerschnittstelle eines serverseitigen PDF-Signaturservices fungieren. Sind solche serverseitigen Komponenten nicht im Spiel, muss die gesamte notwendige Funktionalität durch die

[15] 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 Vertrauensdiensteanbieter etabliert wird.

Client-Komponente selbst implementiert werden. Bei Verwendung von mobilen Apps ist dies technisch einfach möglich, da die Funktionalität mobiler Apps durch Entwickler frei definiert werden kann. Bei Verwendung von Web-Browsern sind die Möglichkeiten beschränkter, eine rein clientseitige Abwicklung von Signaturerstellungsprozessen ist hier aber beispielsweise über entsprechende JavaScript-Lösungen denkbar. In der Regel wird bei Verwendung von Web-Browsern als Client-Komponente aber zusätzlich eine serverseitige Komponente zum Einsatz kommen.

Im mobilen Kontext, d.h. bei Verwendung einer mobilen App als Client-Komponente, ergeben sich für die Erstellung einer qualifizierten Signatur damit folgende Varianten:

1. **Signaturerstellung über Service-Provider-App:** Die verwendete Service-Provider-App erstellt selbstständig einen Signaturerstellungs-Request und übermittelt diesen direkt an den VDA. Am Ende des Prozesses wird die beim VDA erstellte Signatur direkt an die Service-Provider-App retourniert.

2. **Signaturerstellung über serverseitige Komponente des Service-Providers:** Die verwendete Service-Provider-App dient nur als Benutzerschnittstelle für eine serverseitige Komponente (z.B. Online-Anwendung). Der Signaturerstellungsprozess wird durch eine Interaktion des Benutzers in der App gestartet, der Signaturerstellungs-Request jedoch in der serverseitigen Komponente erstellt und von dort an den VDA übermittelt. Nach erfolgter Benutzerauthentifizierung zur Autorisierung der Signaturerstellung wird die erstellte Signatur an die serverseitige Komponente retourniert.

3. **Signaturerstellung über Digitales-Amt-App:** In dieser Variante bietet die Digitales-Amt-App eine lokale Signaturerstellungs-API an. Service-Provider-Apps, die sich am gleichen Gerät wie die Digitales-Amt-App befinden, können Signatur-Requests an diese API schicken. Zur Erstellung der qualifizierten Signatur übermittelt die Digitales-Amt-App einen entsprechenden Signaturerstellungs-Request an den VDA. Die erstellte Signatur wird vom VDA zunächst an die Digitales-Amt-App retourniert, welche die Signatur über die lokale API dann an die aufrufende Service-Provider-App weiterleitet.

Neben diesen unterschiedlichen mobilen Varianten zur Signaturerstellung werden parallel dazu auch weiterhin Web-Browser-basierte Varianten unterstützt, sodass z.B. auch webapplikationsbasierte Service-Provider im Rahmen ihrer Workflows Benutzer*innen zur Signaturerstellung auffordern können. Die Funktion der Signaturerstellung wird für Benutzer*innen einer ausländischen eIDAS-konformen elektronischen Identität hingegen nicht unterstützt. Dies erfolgt aus zweierlei Gründen. Zunächst kann eine Unterstützung qualifizierter Signaturen durch ausländische Identitätssysteme nicht angenommen werden. Tatsächlich existiert eine Reihe von ausländischen Identitätssystemen, die zwar eine zuverlässige Authentifizierung von Benutzern, nicht aber die Erstellung qualifizierter Signaturen unterstützen. Zum anderen bietet die aktuelle Version des eIDAS-Protokolls, das zur Anbindung ausländischer Identitätssysteme benötigt wird, keine Unterstützung für die Erstellung qualifizierter elektronischer Signaturen.

3.3. Widerruf der ID Austria

Der Lebenszyklus einer ID Austria kann einerseits mit einem Widerruf, angestoßen durch Bürger*innen oder durch eine autorisierte Organisation (Behörde, VDA, etc.), und andererseits durch eine auslaufende Gültigkeit beendet werden. Konkret handelt es sich bei letzterem um ein Überschreiten des Gültigkeitszeitraums des qualifizierten Signaturzertifikats, das vom VDA im Zuge der Registrierung ausgestellt wird und welches mit der ID Austria verknüpft ist. Die Gültigkeit eines qualifizierten Signaturzertifikats beträgt in der Regel fünf Jahre. Nach Ablauf dieser Frist muss ein neues Zertifikat beim VDA beantragt werden, sofern Bürger*innen weiterhin die Funktionalität der ID Austria nutzen möchten.

Da in der Variante der Basis ID Austria bestehende Handy-Signaturen oder Bürgerkarten in eine ID Austria umgewandelt werden, richtet sich der Gültigkeitszeitraum der Basis ID Austria ab dem Zeitpunkt ihrer Registrierung somit nach der verbleibenden Gültigkeitsdauer des Signaturzertifikats. Die Gültigkeit einer regulären ID Austria beträgt hingegen immer fünf Jahre ab dem Zeitpunkt ihrer Registrierung.

Neben der Inhaber*in einer ID Austria kann ein Widerruf auch von einer Behörde oder gegebenenfalls dem VDA unter anderem aus den folgenden Gründen vorgenommen werden:

- Versterben der Benutzer*in
- Antrag auf Widerruf durch Benutzer*innen
- Bekanntwerden von berechtigten Zweifeln an der Identität der Benutzer*in

Im Zuge eines Widerrufs identifiziert die Behörde die jeweilige Person im Identitätsdokumentenregister (IDR) und übermittelt den Widerrufs-Auftrag inklusive der verschlüsselten bPK an den VDA, der die relevanten Daten der Person löscht und eine Bestätigung des Widerrufs zurück an das IDR sendet. Diese Vorgänge werden im IDR protokolliert.

Um eine ID Austria zu verwalten, wird Bürger*innen ein Widerrufsservice durch das ID-Austria-System bereitgestellt. Die Möglichkeit des Widerrufs kann für Bürger*innen speziell in folgenden Fällen notwendig sein:

1) **Verlust oder Diebstahl eines oder mehrerer mobiler Geräte**, auf denen eine Benutzer*in die Digitales-Amt-App installiert und initialisiert hat und die potentiell für eine vereinfachte Weiterverwendung einer Benutzerauthentifizierung am ID-Austria-System verwendet werden könnten. Eine Anmeldung mit einer persönlichen ID Austria für einen Angreifer würde allerdings auch den Diebstahl des biometrischen Merkmals (Fingerprint/Face ID) bedingen, welches für die vereinfachte Weiterverwendung einer Authentifizierung gegen das ID-Austria-Systems ebenfalls benötigt wird. Wurde die Digitales-Amt-App nicht kryptographisch an den IDP gebunden und besteht somit nicht die Möglichkeit zur Verwendung der vereinfachten Authentifizierung, muss ein Angreifer für eine mögliche ID Austria Anmeldung zusätzlich das Signaturpasswort kennen, welches zur Erstellung der qualifizierten Signatur im Zuge der Authentifizierung beim VDA benötigt wird.

2) **Verlust oder Diebstahl von Anmeldeinformationen**, die eine Person für die Authentifizierung gegen den VDA oder den IDP des ID-Austria-Systems benötigt. Konkret betrifft dies das

Passwort, welches bei einer Authentifizierung gegen den VDA zur Entschlüsselung des Signaturschlüssels notwendig ist, sowie eine zusätzliche technische Kompromittierung von biometrischen Merkmalen, die für eine lokale Authentifizierung am Smartphone beim Zugriff auf kryptographisches Schlüsselmaterial, das in der Digitales-Amt-App zur Authentifizierung gegen den VDA und/oder den IDP des ID-Austria-Systems verwendet wird, notwendig sind.

3) **Vergessen von Anmeldeinformationen,** die eine Person für die Authentifizierung gegen den VDA oder den IDP des ID-Austria-Systems benötigt. Konkret betrifft dieser Fall ausschließlich das Passwort zur Authentifizierung gegen den VDA.

Um auf diese unterschiedlichen Fälle entsprechend reagieren zu können, steht Bürger*innen zur Verwaltung ihrer ID Austria ein Dashboard/Self-Service bereit, mit welchem mehrere Arten eines Widerrufs durchgeführt werden können und die nachfolgend beschrieben werden. Die Konsequenzen richten sich je nach Art des Widerrufs.

3.3.1. Verlust oder Diebstahl des mobilen Geräts

Um den beschriebenen Risiken bei einem Verlust oder Diebstahl des mobilen Geräts entgegenzuwirken, besteht für Bürger*innen die Möglichkeit eines **Widerrufs des Bindungszertifikats der ID-Austria-Komponente in der Digitales-Amt-App:**

In dieser Variante wird das Bindungszertifikat einer Person widerrufen, das für eine vereinfachte Weiterverwendung einer Authentifizierung am ID-Austria-System verwendet werden kann. Die Digitales-Amt-App bietet Benutzer*innen die notwendige Funktionalität, um das Bindungszertifikat selbst zu widerrufen. Demnach müssen sich Benutzer*innen nicht zwingend am Dashboard/Self-Service anmelden, um dieses Bindungszertifikat zu widerrufen. Nach einem erfolgten Widerruf des Bindungszertifikats müssen Benutzer*innen anschließend erneut eine kryptographische Bindung für ihr mobiles Gerät durchführen, um eine vereinfachte Weiterverwendung einer Authentifizierung am ID-Austria-System nutzen zu können. Ein Widerruf des Bindungszertifikats der ID-Austria-Komponente der Digitales-Amt-App führt nicht zwangsläufig auch zum Widerruf des qualifizierten Signaturzertifikats der Benutzerin bzw. des Benutzers. Allerdings wird ebenfalls auch die kryptographische Bindung der Digitales-Amt-App zum VDA widerrufen. Die Digitales-Amt-App muss dementsprechend neu an die ID Austria der Person gebunden werden. Abbildung 4 zeigt die Screenshots beim Rücksetzen der Digitales-Amt-App (App zurücksetzen), was den Widerruf des Bindungszertifikats der ID-Austria-Komponente auslöst.

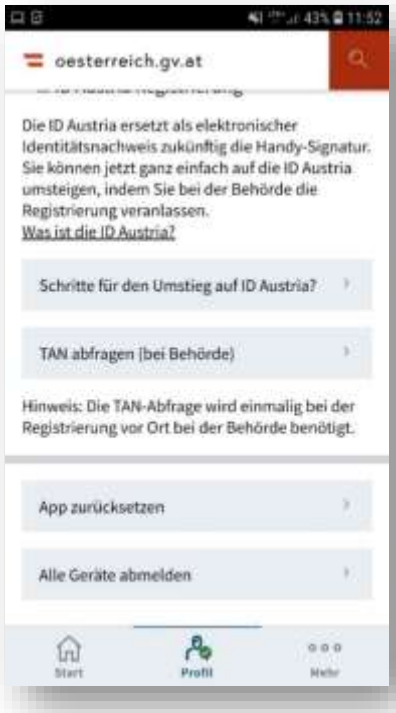

Abbildung 4. Widerruf des Bindungszertifikats in der Digitales-Amt-App

Bei Verlust mehrerer verschiedener mobiler Geräte, auf denen die Digitales-Amt-App installiert und initialisiert ist, besteht die Möglichkeit des **Widerrufs aller Bindungszertifikate der ID-Austria-Komponente auf den mobilen Geräten:**

Bürger*innen können hierfür die Funktion „Alle Geräte abmelden“ in der Digitales-Amt-App nutzen oder eine Abmeldung am Desktop via oesterreich.gv.at vornehmen. Abbildung 5 zeigt die Möglichkeit des Widerrufs aller Bindungszertifikate unter der gleichnamigen Funktion, wie sie auch in der Digitales-Amt-App zur Verfügung steht. Die Variante des Widerrufs am Desktop ist speziell für den Fall des Verlustes von mobilen Geräten entscheidend.

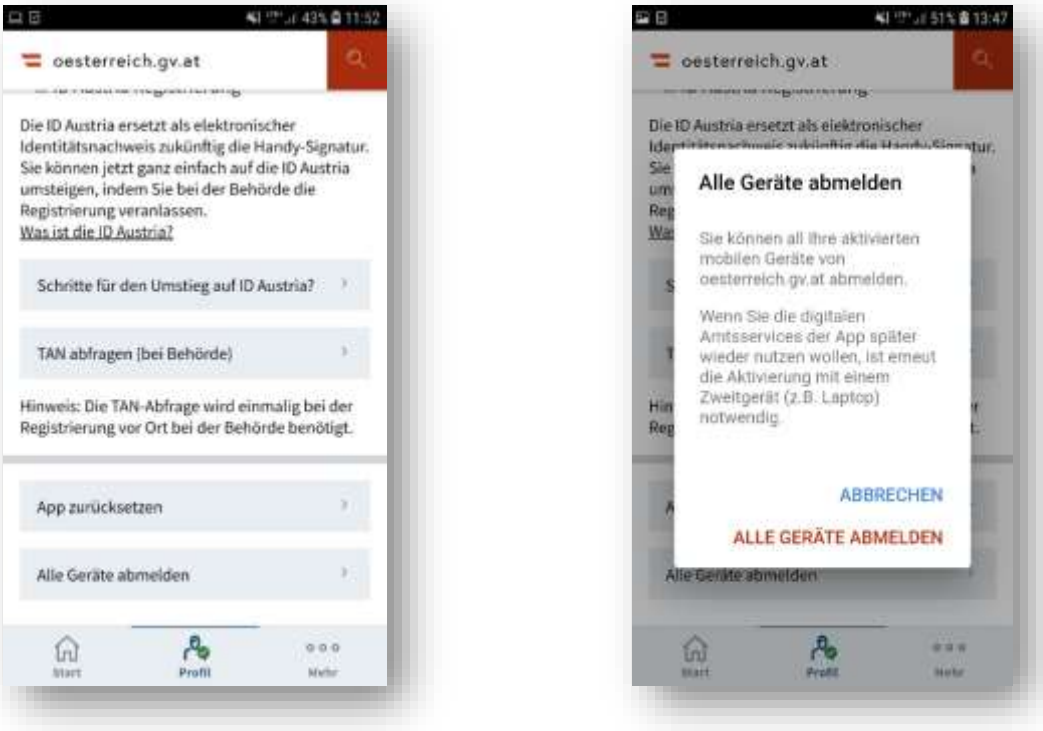

Abbildung 5. Widerruf aller Bindungszertifikats in der Digitales-Amt-App

Abbildung 6 zeigt die Möglichkeit des Widerrufs aller Bindungszertifikate am Desktop via oesterreich.gv.at unter der gleichnamigen Funktion, wie sie auch in der Digitales-Amt-App zur Verfügung steht. Die Variante des Widerrufs am Desktop ist speziell für den Fall des Verlustes von mobilen Geräten entscheidend.

Abbildung 6. Widerruf aller Bindungszertifikats auf oesterreich.gv.at

Widerruf des Bindungszertifikats der VDA-Komponente der Digitales-Amt-App: In dieser Variante wird das Bindungszertifikat einer Person widerrufen, das für die Authentifizierung der VDA-Komponente der Digitales-Amt-App gegen den VDA verwendet wird. Nach erfolgtem Widerruf dieses Bindungszertifikats der VDA-Komponente muss die kryptographische Bindung erneut hergestellt werden, um eine Authentifizierung am VDA durchführen zu können. Auch ein Widerruf dieses Bindungszertifikats führt nicht automatisch zum Widerruf des qualifizierten Signaturzertifikats der Benutzer*in. Allerdings werden bestehende kryptographische Bindungen zum IDP des ID-Austria-Systems automatisch widerrufen.

3.3.2. Verlust oder Diebstahl von Anmeldedaten

Bei Bekanntwerden eines Diebstahls von Anmeldeinformationen können Bürger*innen einen **Widerruf des qualifizierten Signaturzertifikats** veranlassen, welches vom VDA bei der Registrierung der ID Austria ausgestellt wurde:

In dieser Variante widerrufen Bürger*innen ihr qualifiziertes Signaturzertifikat beim VDA. Dadurch werden automatisch auch alle kryptographischen Bindungen (Bindungen der VDA-Komponente der Digitales-Amt-App zum VDA, kryptographische Bindungen der ID-Austria-Komponente der Digitales-Amt-App zum IDP des ID-Austria-Systems) widerrufen. Nach Widerruf des Signaturzertifikats muss erneut ein vollständiger Registrierungsprozess durchlaufen werden, um die ID Austria wieder nutzen zu können.

Der Widerruf des qualifizierten Signaturzertifikats kann auch im Falle des Vergessens des Passworts zur Authentifizierung gegen den VDA durchgeführt werden. Ein Abrufen bzw. Zurücksetzen des Passworts ist nicht möglich, da auch der VDA selbst diese Passwörter nicht speichert. Demnach ist bei Verlust des Signaturpassworts eine erneute Registrierung der ID Austria notwendig.

4. Hinter den Kulissen

Das Ziel der ID Austria ist es, Service-Providern Merkmale (Attribute) und einen eindeutigen Identifikator einer Person bereitzustellen, die diese Person zu einer Nutzung der Online-Anwendung des jeweiligen Service-Providers autorisieren. Im Gegensatz zur Bürgerkarte/Handy-Signatur werden bei der ID Austria nur Attribute an die Service-Provider ausgeliefert, zu deren Erhalt sie berechtigt sind. Damit wird der Schutz personenbezogener Daten von Bürger*innen erhöht. Ein Anmelde- bzw. ein Signaturerstellungsprozess bedingt die Zusammenarbeit bzw. Kommunikation zahlreicher technischer Komponenten des ID-Austria-Systems. Aus diesem Grund bietet dieses Kapitel einen Überblick über die technische Architektur und deren Komponenten, die in verschiedenen Domains angesiedelt sind und beschreibt zusätzlich das Konzept der eindeutigen Identifikation von Bürger*innen in diesem System.

4.1. Architekturüberblick

Bei der ID Austria handelt es sich um ein komplexes System, das sich aus diversen Einzelkomponenten zusammensetzt. Diese Einzelkomponenten sind in verschiedenen Domains zusammengefasst. Jede Domain enthält eine oder mehrere Komponenten des Gesamtsystems. Der Begriff Domain bezeichnet hier einen Teil des Gesamtsystems, dessen Komponenten von einer Organisation (z.B. BRZ, BM.I, 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*innen, sowie deren verwendete Endnutzergeräte umfasst.

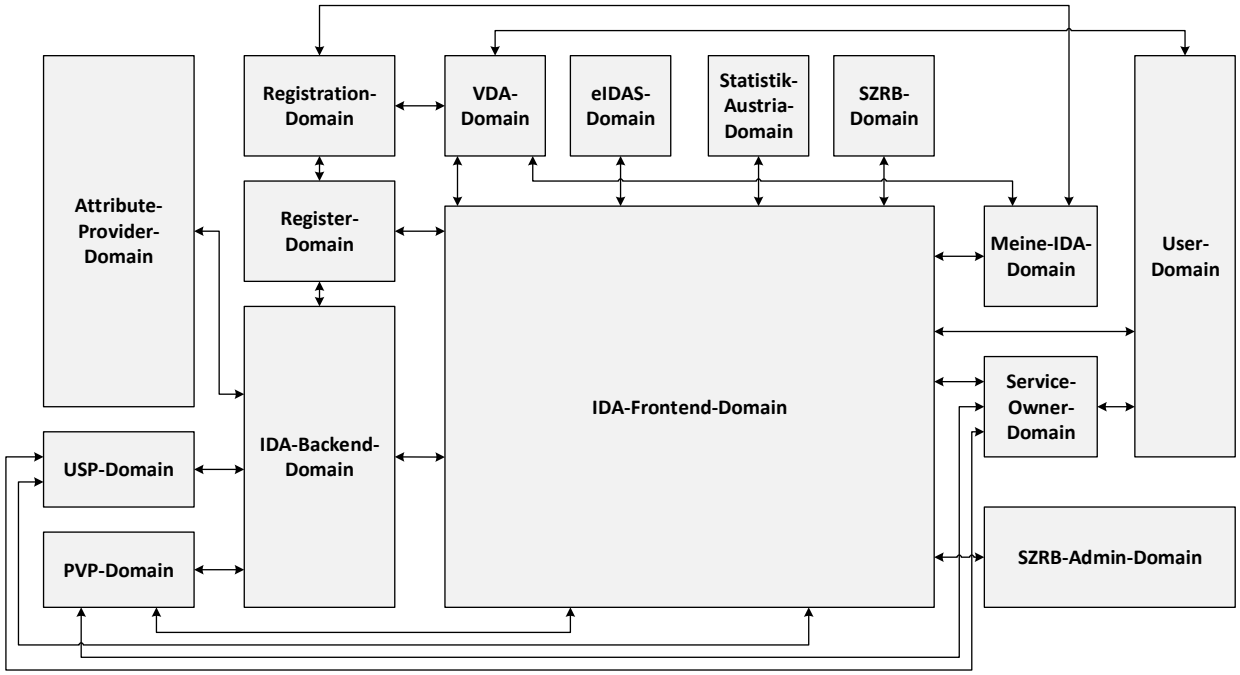

Abbildung 7. Gesamtarchitektur der ID Austria – Domain-Ebene.

Im Sinne einer übersichtlichen Darstellung zeigt Abbildung 7 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 der ID Austria gegeben werden. Diese sind im Folgenden zusammengefasst.

Vor einer Verwendung der ID Austria müssen Bürger*innen 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 Benutzer*innen mit ihren Endgeräten mit Komponenten der Registration-Domain interagieren müssen. 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 Vertrauensdiensteanbieters, der im Zuge der Registrierung einer ID Austria ein qualifiziertes Signaturzertifikat für die Benutzer*in ausstellt.

Nach erfolgter Registrierung können Benutzer*innen ihre persönliche ID Austria zur Anmeldung an Service-Providern verwenden. Service-Provider sind in der Service-Provider-Domain angesiedelt. Die Service-Provider-Domain verfügt über eine Schnittstelle zur User-Domain, über welche Benutzer*innen bereitgestellte Dienste des Service-Providers in Anspruch nehmen können. Der Service-Provider nutzt die ID Austria zur Authentifizierung der Benutzer*innen. 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.

Kernaufgabe der Frontend-Domain ist die Authentifizierung von Benutzer*innen. Die Authentifizierung erfolgt im Falle der Verwendung einer registrierten, persönlichen ID Austria über den Vertrauensdiensteanbieter (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, 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 SZRB-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

persönliches Dashboard/Self-Service[16] 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 Benutzer*innen ihre persönliche ID Austria registrieren können und sich in weiterer Folge mit ihrer registrierten ID Austria an Service-Providern anmelden können. Die notwendige Funktionalität wird durch technische Komponenten, die in den verschiedenen Domains angesiedelt sind, bereitgestellt.

4.2. Eindeutige Identifikatoren

Eine Kernaufgabe der ID Austria ist es, Service-Provider nach erfolgter Authentifizierung der Benutzer*innen mit einem eindeutigen Identifikator der jeweiligen Person zu versorgen. Dieser wird zusammen mit anderen Attributen der Benutzer*in an den Service-Provider übertragen. An Service-Provider übermittelte Identifikatoren basieren auf Daten aus behördlichen Registern. Dies unterscheidet die ID Austria von anderen herkömmlichen Identitäts-Providern. Aus diesem Grund wird in diesem Abschnitt auf die im Rahmen der ID Austria verwendeten Identifikatoren, ihre Ableitung und ihre Eigenschaften näher eingegangen.

4.2.1. ZMR-Zahl

Das Zentrale Melderegister stellt den Ausgangspunkt und die Basis zur Erstellung aller elektronischen Identitäten im österreichischen E-Government dar. Bürger*innen in Österreich werden mit ihrem Hauptwohnsitz und wenn vorhanden, auch ihrem Nebenwohnsitz, im Zentralen Melderegister (ZMR) erfasst. Das ZMR ist ein Register des öffentlichen Sektors, welches im BM.I eingerichtet ist. Eintragungen in dieses Register werden von den unterschiedlichen Meldebehörden, Standesämtern und Staatsbürgerschaftsstellen vorgenommen, welche dafür online auf das ZMR zugreifen können.

Neben Personenmerkmalen wie Vorname, Nachname und Geburtsdatum wird im ZMR eine zusätzliche, für Bürger*innen eindeutig zugewiesene **ZMR-Zahl** (auch Basiszahl genannt), registriert. Aus Gründen des Datenschutzes darf diese Zahl aber nicht zur Identifizierung von Bürger*innen in behördlichen elektronischen Prozessen verwendet werden, da die Verwendung eines einzigen Identifikators einen Rückschluss auf die Nutzung aller elektronischen Services durch eine Person ermöglichen würde

[16] Das Dashboard/Self-Service ist derzeit noch in Entwicklung. Der Begriff „Dashboard/Self-Service“ ist ein Arbeitstitel, der endgültige Name dieser Anwendung, die der Benutzer*in die Verwaltung ihrer ID Austria ermöglicht, steht noch nicht fest.

(Tracking). Daher wird die ZMR-Zahl lediglich zur Berechnung einer sogenannten Stammzahl herangezogen, die dann in weiterer Folge zur Berechnung bereichsspezifischer Personenkennzeichen verwendet wird.

4.2.2. Stammzahl

Die Stammzahl ist der eindeutige, persistente Identifikator einer Bürger*in und wird direkt von ihrer ZMR-Zahl abgeleitet. Für die Berechnung der Stammzahl wird ein symmetrischer Verschlüsselungsalgorithmus verwendet. Die Berechnung wird ausschließlich von der Stammzahlenregisterbehörde unter Verwendung eines geheimen und nur der Stammzahlenregisterbehörde bekannten kryptographischen Schlüssels durchgeführt. Mit Hilfe dieses Schlüssels verschlüsselt die Stammzahlenregisterbehörde die ZMR-Zahl der Bürger*in. Resultat dieser Verschlüsselungsoperation ist die Stammzahl. Da nur die Stammzahlenregisterbehörde den verwendeten Schlüssel kennt, ist auch nur diese in der Lage, aus der Stammzahl wieder auf die ZMR-Zahl zurückzurechnen.

Voraussetzung zur Ableitung der Stammzahl einer Person ist somit das Vorhandensein einer ZMR-Zahl. Personen, die keinen Wohnsitz in Österreich haben und demnach über keinen ZMR-Eintrag und keine ZMR-Zahl verfügen, aber dennoch elektronische Services des österreichischen E-Government nutzen möchten, werden im Ergänzungsregister für natürliche Personen (ERnP) eingetragen. Diesen Personen wird im ERnP eine Ordnungsnummer zugewiesen, die anstelle der ZMR-Zahl für die Berechnung der Stammzahl herangezogen wird.

Die Berechnung von Stammzahlen findet über das Stammzahlenregister (SZR) statt. Das SZR wird vom Bundesministerium für Inneres (BM.I) im Auftrag der Stammzahlenregisterbehörde betrieben, welche im Bundesministerium für Digitalisierung und Wirtschaft (BMDW) angesiedelt ist.

4.2.3. Bereichsspezifisches Personenkennzeichen (bPK)

Die direkte Verwendung der Stammzahl von Bürger*innen zu deren Identifizierung bei Service-Providern ist in Österreich nicht zulässig, da dies ein Tracking von Personen über Service-Provider-Grenzen hinweg ermöglichen würde. Service-Provider werden von der ID Austria daher nicht mit der Stammzahl, sondern mit sogenannten bereichsspezifischen Personenkennzeichen (bPK) als eindeutige Identifikatoren versorgt. Ein Bereich bezeichnet bei Service-Providern des öffentlichen Sektors einen Bereich der öffentlichen Verwaltung (z.B.: Gesundheit, Finanzen, etc.). Die verschiedenen öffentlichen Bereiche werden in der E-Government-Bereichsabgrenzungsverordnung (E-Gov-BerAbgrV[17]) definiert. Bei privatwirtschaftlichen Service-Providern ergibt sich für jede Organisation (Unternehmen, Verein, etc.) ein eigener Bereich. Wie der Name bereits suggeriert, wird jeder Bereich mit einem anderen bereichsspezifischen Personenkennzeichen für ein und dieselbe Person versorgt. Damit ist ein Tracking von Personen über Bereichsgrenzen hinweg unmöglich.

Alle bereichsspezifischen Personenkennzeichen werden über eine Einwegfunktion von der Stammzahl der Bürger*in abgeleitet und stellen einen eindeutigen und persistenten Identifikator dar, der vom Service-Provider zur Identifizierung der Bürger*in verwendet werden kann. In die Ableitung des bPK einer Bürger*in geht neben deren Stammzahl auch ein Identifikator des Bereichs ein, für den das bPK berechnet

[17] https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003476

wird. Die zum Einsatz kommende Einwegfunktion zur Ableitung von bPKs muss diverse Eigenschaften aufweisen, um den vorgesehenen Effekt zu erzielen. So darf die Ableitung nicht umkehrbar sein, von einem bPK darf also nicht auf die Stammzahl rückgeschlossen werden können. Außerdem darf vom bPK eines Bereichs nicht auf das bPK eines anderen Bereichs geschlossen werden können. Die Berechnung von bPKs wird ebenfalls von der Stammzahlenregisterbehörde durchgeführt, da nur diese über die unverschlüsselte Stammzahl der Bürger*in verfügt.

Benötigt eine Behörde zur Identifikation einer Person in bereichsübergreifenden E-Government-Verfahren ein bPK aus einem anderen Verfahrensbereich, darf dieses durch die Stammzahlenregisterbehörde berechnet und ausgeliefert werden. Die Stammzahlenregisterbehörde übermittelt dieses bPK jedoch ausschließlich verschlüsselt an die anfragende Behörde. Für die Verschlüsselung eines bPK werden öffentliche Schlüssel von Behörden aus einem Schlüsselverzeichnis verwendet. Dies stellt sicher, dass nur jene Behörde, die für diesen Fremd-Verfahrensbereich zuständig ist, ein jeweiliges bPK entschlüsseln kann. Das für einen anderen Verfahrensbereich verschlüsselte bPK wird als Fremd-bPK bezeichnet.

5. Sicherheit und Datenschutz

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 dem jahrelangen Betrieb und der Verwendung von Handy-Signatur und Bürgerkarte gewonnen werden konnten, und hat zum Ziel, das Sicherheitsniveau für alle Beteiligten (Bürger*innen, Service-Provider, etc.) zu erhöhen.

Dieser Abschnitt gibt einen Überblick über ausgewählte Aspekte der ID Austria, die speziell für Bürger*innen das erreichbare Sicherheitsniveau positiv beeinflussen. Die ausgewählten Aspekte werden in den folgenden Unterabschnitten näher diskutiert.

5.1. Sichere Registrierungs- und Akkreditierungsprozesse

Die Verwendung von Handy-Signatur und Bürgerkarte stand prinzipiell allen Service-Providern zur Benutzerauthentifizierung zur Verfügung und konnte einfach in ihre Anwendungen integriert werden. Dadurch hatte der Anbieter dieses nationalen Identitätsmanagementsystems wenig Einfluss auf die Auslieferung von staatlich bestätigten Benutzerinformationen (Attributen) an Service-Provider, die die Handy-Signatur oder Bürgerkarte für eine Benutzerauthentifizierung verwendeten. Damit wurde den Benutzer*innen die Entscheidung überlassen, ob ein Service-Provider vertrauenswürdig und zum Erhalt persönlicher Attribute berechtigt ist. Obwohl dies ein zulässiger Ansatz ist, besteht in der Praxis die Gefahr, dass Bürger*innen die Konsequenzen der Datenweitergabe oder die Vertrauenswürdigkeit eines Service-Providers nicht immer richtig einschätzen können.

Um diesem Problem entgegenzuwirken, verfolgt die ID Austria einen restriktiveren Ansatz. Jeder Betreiber (Service-Owner) eines oder mehrerer 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 werden relevante Daten des Service-Owners und seiner Service-Provider erfasst. 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. Erst nach erfolgreicher Akkreditierung des Service-Providers kann dieser die ID Austria zur Benutzerauthentifizierung nutzen.

Dieser im Vergleich zur Bürgerkarte und Handy-Signatur restriktiverer Ansatz stellt sicher, dass ausschließlich 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 speziell für Bürger*innen.

5.2. Sichere und korrekte Auslieferung von persönlichen Attributen

Die Korrektheit und Aktualität der Attribute (Benutzerdaten), die im Zuge der Anmeldeprozesse von Benutzer*innen erhalten werden, ist für eine sichere Datenverarbeitung von zentraler Bedeutung. Die ID Austria verbessert das bisher diesbezüglich schon hohe Niveau der Bürgerkarte/Handy-Signatur noch weiter.

Da die Verwendung und Aktivierung[18] der persönlichen ID Austria für Bürger*innen eine Registrierung an einer ermächtigten Behörde voraussetzt, wird die Identität des Bürgers bzw. der Bürgerin zum Zeitpunkt der Ausstellung der persönlichen ID Austria behördlich überprüft. Anders als bei der Handy-Signatur und Bürgerkarte werden die ausgelieferten Daten bei jedem Anmeldeprozess von der ID Austria neu zusammengestellt. Diese dynamische Aggregation der ausgelieferten Personenmerkmale stellt die Aktualität der Daten sicher.

5.3. Schutz der Privatsphäre von personenbezogenen Daten

Ein Ziel der ID Austria ist eine Minimierung der an Service-Provider übertragenen Personenmerkmale zum Schutz der Privatsphäre von Benutzer*innen. Zu diesem Zweck findet ausschließlich eine selektive Übermittlung von Personenmerkmalen an Service-Provider statt. Personenmerkmale werden ausschließlich entsprechend der Berechtigungen des anfragenden Service-Providers ausgeliefert. Diese Berechtigungen werden im Zuge der Registrierung des Service-Providers am ID-Austria-System sorgfältig geprüft und erteilt. Bei jedem Anmeldeprozess können Benutzer*innen zudem die an den Service-Provider zu übermittelnden Daten einsehen und müssen der Übermittlung zustimmen.

Einen besonderen Schutz erfährt bei der ID Austria die Stammzahl von Bürger*innen, die als Basis für die zum Einsatz kommenden sektorspezifischen Identifikatoren fungiert. Die ID Austria schützt die Stammzahl speziell, indem das zugrundeliegende Konzept vorsieht, dass diese die behördlichen Register zu keiner Zeit unverschlüsselt verlässt.

Der Schutz der Identitätsmerkmale (Attribute) von Bürger*innen ist ein zentrales Design-Prinzip der ID Austria. Die selektive benutzerkontrollierte Übermittlung von Attributen an Service-Provider und der spezielle Schutz der Vertraulichkeit der Stammzahl sind zwei der wichtigsten Maßnahmen, um diesem Design-Prinzip gerecht zu werden.

5.4. 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 lediglich der Nachweis eines biometrischen Merkmals am Smartphone notwendig ist[19].

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

[18] 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 auf einem Passamt notwendig.

[19] 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 Vertrauensdiensteanbieter etabliert wird.

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.

5.5. Sicherheitselemente in Smartphones

Modernere mobile Geräte der neueren Generationen (ab 2015) verfügen über sichere Hardware-Elemente, die es ermöglichen, kryptographisches Schlüsselmaterial sicher im Smartphone zu speichern. Das Schlüsselmaterial lässt sich aus dieser Hardware nicht extrahieren und ist daher an das mobile Gerät gebunden. Darüber hinaus verhindert diese Eigenschaft den Diebstahl der Schlüssel durch potenzielle Angriffe und gewährleistet dadurch eine erhöhte Sicherheit. Der Zugriff auf das Schlüsselmaterial wird durch zusätzliche lokale Authentifizierungsmethoden (z.B. Fingerprint, Gesichtserkennung, etc.) geschützt, wodurch es nur autorisierten Benutzer*innen möglich ist, diese Schlüssel zu verwenden. Abhängig vom Betriebssystem des mobilen Gerätes werden unterschiedliche Hardware-Elemente eingesetzt, die prinzipiell eine vergleichbare Funktionalität bieten.

5.5.1. Android: Secure Elements

Secure Elements sind Chipsätze in Android Smartphones, welche die erforderliche Sicherheit für mobile Apps in Bereichen wie Mobile Payment oder Mobile Banking bieten. Auch bei der ID Austria werden Secure Elements aus mehreren Gründen als sicherer Schlüsselspeichers verwendet. Zum einen erfordert der Zugriff auf geheimes Schlüsselmaterial in Secure Elements eine lokale Authentifizierung (z.B. Fingerprint/Face Recognition). Zum anderen lässt sich das Schlüsselmaterial nicht aus der Hardware extrahieren und ist daher an das mobile Gerät gebunden. Außerdem gibt es im Gegensatz zu iOS auf Android Smartphones die Möglichkeit zur Erbringung eines Nachweises (Key Attestation), dass ein entsprechendes Schlüsselmaterial in einer sicheren Hardware erzeugt und gespeichert wurde.

Secure Elements werden bei der ID Austria als sicherer Schlüsselspeicher Mobile Apps, die auf dem Smartphone ebenfalls installiert sind, haben keinen Zugriff auf das Schlüsselmaterial einer anderen App. Der Zugriff auf das Secure Element ist nur über vertrauenswürdige Apps möglich. Außerdem gibt es im Gegensatz zu iOS auf Android Smartphones die Möglichkeit zur Erbringung eines Nachweises (Key Attestation), dass ein entsprechendes Schlüsselmaterial in einer sicheren Hardware erzeugt und gespeichert wurde.

5.5.2. iOS: Secure Enclave

Die Secure Enclave ist Teil des Apple A7 sowie von neueren Chipsätzen, die speziell für den Zweck der Datensicherheit eingesetzt werden. Prinzipiell stellen Secure Enclaves das Pendant zu den in Android Smartphones eingesetzten Secure Elements dar. Der Zweck der Secure Enclave ist daher ebenso die Verwaltung von kryptographischem Schlüsselmaterial und weiteren sensiblen biometrischen Informationen. Diese Chipsätze sind von anderer Hardware am mobilen Gerät isoliert.

6. Fazit

Die ID Austria ist das neue österreichische nationale elektronische Identitätsmanagementsystem und tritt die Nachfolge von Bürgerkarte und Handy-Signatur an. Als Kernfunktionen ermöglicht sie eine staatlich anerkannte Authentifizierung bei Service-Providern des öffentlichen und privaten Sektors und bietet außerdem die Möglichkeit zur Erstellung von rechtsgültigen, qualifizierten elektronischen Signaturen.

Die ID Austria bietet ein weitaus breiteres Nutzungsspektrum als die bisherige Bürgerkarte bzw. Handy-Signatur. Dies wird, unter anderem durch die Möglichkeit erreicht, neben den üblichen Attributen spezielle zusätzliche Identitätsmerkmale aus privaten oder behördlichen Registern abzufragen. Eine Erweiterung der bisherigen Anwendungsszenarien ergibt sich auch aus der Unterstützung App-basierter Service-Provider und der über diese umgesetzten mobilen Anwendungsfälle. Der Anwendungsbereich der ID Austria wird daher, unter anderem, durch die Erbringung elektronischer Nachweise für bspw. einen Führerschein oder einen Reisepass auf mobilen Geräten erweitert. Neben der Verwendung der ID Austria zur Authentifizierung bei diversen Service-Providern, bietet sie auch die Möglichkeit zur Erstellung von qualifizierten Signaturen (z.B. PDF-Signaturen). Die erhöhte Flexibilität der ID Austria erleichtert die zukünftige sichere Bereitstellung von elektronischen Services für Bürger*innen.

Die Gewährleistung einer sicheren Kommunikation innerhalb des ID-Austria-Systems und mit externen Komponenten basiert auf etablierten und erprobten kryptographischen Methoden. Die darauf basierenden Sicherheitsfunktionen erfüllen die notwendigen Datenschutzanforderungen und bieten einen ausreichenden Zugriffsschutz auf Personenmerkmale. Zusätzlich versichert eine notwendige Registrierung und Akkreditierung von öffentlichen oder privaten Service-Providern, dass die datenverarbeitenden Stellen nur Daten empfangen, zu deren Erhalt sie autorisiert sind. Damit wird der Schutz der Privatsphäre von personenbezogenen Daten weiter erhöht.

Dieses Dokument stellte ausgewählte Aspekte der ID Austria näher vor, um Bürger*innen einen tieferen Einblick in die Funktionsweisen und Sicherheitsfunktionen der ID Austria zu bieten. Um den Umfang des Dokuments im Rahmen zu halten, wurde in einigen Aspekten bewusst auf einen höheren Detailierungsgrad verzichtet. Interessierte LeserInnen 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