

Studie

Authentifizierungsdienst der Schweizer Behörden AGOV

Klassifizierung	nicht klassifiziert
Status	genehmigt zur Nutzung
Projektleiter	Philipp Dasen
Version	1.2
Datum	13. Juli 2023
Auftraggeber	Peppino Giarritta
Autor/Autoren	Stefan Minder
Verteiler	Kantone, DVS, BK, BIT

Änderungsverzeichnis

Siehe Anhang Kapitel 27.1

Beschreibung

Die vorliegende Studie beschreibt den Identitätsprovider und Identitätsverbund AGOV, welcher Webapplikationen und native Mobile Apps (Zielapplikationen) der Schweizer Behörden föderativ – mittels OIDC und SAML – mit Authentifizierungsleistungen versorgt, spricht mit Logins von Bürgerinnen, Bürgern und Vertretenden der Wirtschaft (End-User). AGOV bietet ein End-User-Portal an, über welches im Self-Service ein AGOV-Login erstellt werden kann, es wird dort ein Step-Up auf eine geprüfte elektronische Identität inklusive Angabe der geprüften AHV-Nummer angeboten. AGOV bietet ein Integrationsportal (Self-Service) an, wo die Applikationseigner (Kantone und ihre Gemeinden und die Bundesverwaltung) ihre Zielapplikationen anschliessen können respektive durch ihre Lieferanten anschliessen lassen können. AGOV unterstützt auch das Credential-Linking mit anderen Identitäts Providern, mit dem Zweck, dass Identitätsprovider Dritter (insbesondere kantonale) an AGOV angeschlossen werden können und mit deren Authentifizierungsleistung durch AGOV hindurch Logins möglich sind. Ebenfalls die zukünftige Schweizer E-ID wird via AGOV als Credential (Mittel zum Einloggen) an die an AGOV angeschlossenen Zielapplikationen vermittelt werden, ohne dass letztere einer Anpassung bedürften. Bezüglich Schweizer E-ID ist AGOV der demnächst im EMBAG verbriefte Schweizer Behörden-Authentifizierungsdienst.

Inhalt

1	Ausgangslage	4
2	Ziele.....	4
3	Anforderungen	4
4	Stakeholder	5
5	Projektorganisation	6
5.1	Organisation nach HERMES	6
5.2	Organisation agiler PoC	7
5.3	Organisation nach SAFe (produktiver Betrieb im BIT, Wartung)	7
6	Rechtsgrundlagen.....	8
7	Semantik und Namensgebung	8
8	Kosten und Finanzierung	9
9	Supportorganisation für End-User	10
10	AGOV - logische Komponenten	10
11	Monolithische Sicht auf AGOV und die effektiv nicht monolithische Architektur darin	12
12	Loginfaktoren (Credentials)	13
13	Authentifizierungsqualität und Credentials.....	14
13.1	Die AGOV-Authentifizierungsqualität (AGOVaq) «ungeprüft»	14
13.2	Die AGOV-Authentifizierungsqualität (AGOVaq) «zustellbarkeitsgeprüft»..	15
13.3	Die AGOV-Authentifizierungsqualität (AGOVaq) «stark identitätsgeprüft».	15
13.4	Die AGOV-Authentifizierungsqualität (AGOVaq) «LOA3»	15
14	Identitätsabklärungsverfahren.....	15
15	AHV-Nummer	16
16	Resultierendes Attribut-Set	16
17	End-User-Flow	17
17.1	Registrierung.....	17
17.2	Login	17
18	Kompatibilität mit Identitätsprovider Dritter (Identitätsverbund)	18
19	Kompatibilität mit der staatlichen Schweizer E-ID.....	18
20	Sondernutzungen	18
20.1	Qualifizierte elektronische Signaturen	18
20.2	Elektronisches Patientendossier	18
21	Schnitt des PoC per August 2023	18
22	Gouvernanz	19
23	Weitere Prozesse.....	19
24	Produktkatalog (Basisangebot und Zusatzangebote).....	19

25 Roadmap	20
26 Varianten für die Umsetzung von AGOV	20
26.1 Umsetzungsvarianten.....	20
26.2 Umsetzungsausführungsvarianten	21
26.3 Betriebsvarianten	21
27 Anhänge	22
27.1 Änderungsverzeichnis	22
27.2 Ausführungen zum Mock-Modus	22
27.3 Tabellarische Darstellung von AGOVs Authentifizierungsqualitäten.....	23
27.4 LOA3 in AGOV	23
27.5 Besonderheiten bezüglich der AHV-Nummer	23

1 Ausgangslage

Die Schweizer Behörden setzen verschiedene Lösungen ein, damit Bürgerinnen, Bürger und Vertretende der Wirtschaft sich auf die Behörden-Applikationen (Webapplikationen und native Mobile Apps) einloggen können. Dieser Kontext der digitalen Zusammenarbeit wird unter dem Begriff E-Government zusammengefasst. Die aktuellen Lösungen beinhalten selbstbetriebene Identitätsprovider und Identitätsprovider Dritter, z. B. kommerzielle Anbieter.

2 Ziele

AGOV soll ein einheitliches Schweizer Behörden-Login sein, einerseits indem in AGOV selber direkt elektronische Identitäten geführt werden, andererseits durch Anschluss der existierenden Identitätsprovider-Lösungen und dannzumal durch Anschluss der Schweizer E-ID. Es entsteht somit ein Identitätsverbund. AGOV ist also keine Antithese zu kantonalen Identitätsprovidern und der Schweizer E-ID, sondern ein technisch-organisatorisches Element zur harmonischen Konzertierung. Bezüglich Schweizer E-ID ist AGOV der demnächst im EMBAG verbriefte Schweizer Behörden-Authentifizierungsdienst.

3 Anforderungen

Gemäss aktuellem Entwurfsstadium muss das AGOV folgende acht Anforderungen erfüllen:

Leistungen in Scope

- 1. Versorgung von Web-Applikationen und nativen Mobile-Apps mit Authentisierungen**
Mit dem AGOV-eigenen IdP und jedem an AGOV angeschlossenen Dritt-IdP (Kantone und edu-ID) kann in jeder Zielapplikation eingeloggt werden, adäquates LOA vorausgesetzt.
- 2. Anschluss von Web-Applikationen und nativen Mobile-Apps mittels SAML und OIDC im Self-Service**
Dies wird ohne Support durch die Bundesverwaltung möglich sein, so wie es bei der SuisseID war und wie es heute bei Google ist (Google-Login).
- 3. Anschluss von Identitätsprovidern am Verbund mittels SAML und OIDC (Beauftragung via DVS)**
Hat ein Kanton oder eine andere Schweizer Verwaltungsebene einen Identitätsprovider der Bürgerlogin zur Verfügung stellt, kann dieser am Verbund AGOV angeschlossen werden, dies unabhängig von der gelieferten Authentisierungsqualität, da der Verbund einen Step-Up anbietet.
- 4. Weitergabe des Levels of Assurance kommend vom Identitätsprovider**
Leistet ein kantonaler Identitätsprovider ein adäquates LoA, kann im Verbund AGOV direkt darauf vertraut werden und das AGOV kann auf den Step-Up verzichten.
- 5. Identitätsabklärung und Step-Up**
Genügt die Authentifizierungsqualität der elektronischen Identität von AGOV oder der kommend von einem Dritt-IdP nicht, bietet AGOV Identitätsabklärungsverfahren an, um diese nachhaltig zu erhöhen. Die Identitätsabklärung ist im Dokument «Produkt Katalog» <https://work.agov.ch?c=agovstudie> in Grundangebot und Zusatzangebote aufgeteilt.

6. **Ergänzung der Angaben kommend vom Identitätsprovider mit der AHV-Nummer**
In den selbst deklarierten Personalien soll der Benutzer seine AHV-Nummer deklarieren, welche mit der ZAS (Zentrale Ausgleichsstelle) abgeglichen wird. Die AHV-Nummer wird in den Authentisierungstokens mitgegeben.
7. **Übersetzung der zukünftigen staatlichen Schweizer E-ID in die Föderationsprotokolle SAML und OIDC in Koexistenz der klassischen Identitätsprovider als Alternative zur zukünftigen staatlichen Schweizer E-ID**
Das AGOV ist somit der nationale Authentisierungsdienst für Schweizer Behörden gemäss EMBAG Art. 11.
8. **AGOV-IdP und Dritt-IdPs als E-ID-Alternative**
Ist der Einsatz der E-ID in bestimmten Settings unmöglich oder unerwünscht, bleiben der AGOV-IdP und die an AGOV angeschlossenen IdPs Dritter (Kantone und edu-ID) auch nach Einführung der staatlichen Schweizer E-ID als Alternativen erhalten.

Nicht in Scope

- a) OAuth-Flow
- b) Session Sharing
- c) Rechteverwaltung, z. B. Rollen und Profile (sog. Accessmanagement)

4 Stakeholder

Primär-Stakeholder von AGOV sind erstens die Applikationseigner (Kantone und ihre Gemeinden und die Bundesverwaltung), welche AGOV für ihre Zielapplikationen nutzen wollen; diese sind im ganzen Vorhaben von Anfang an adäquat zu involvieren. Primär-Stakeholder von AGOV sind zweitens die End-User (Bürgerinnen, Bürger und Vertretenden der Wirtschaft), welche AGOV zwecks Logins in Behördenapplikationen nutzen werden. Die End-User werden in der Aufbauphase von AGOV nicht direkt involviert, weil der Phänotyp von AGOV, sprich Selbstregistrierung, ggf. Step-Up und dann wiederholt Login, ein Gemeinplatz des aktuellen Digitalisierungsstandes in der Schweiz ist. Die Sicherstellung der Adäquanz für die End-User geschieht über drei Wege indirekt, erstens Usabilitytests mit Probanden, zweitens Accessibilitytests mit Probanden und drittens über Evaluationsaufträge an den wissenschaftlichen Beirat des Fachausschusses AGOV (vgl. Abschnitt «Projektorganisation»); als Beispiel eines Evaluationsauftrags sei hier die Definition des Angebotes von möglichen Loginzweifaktoren in AGOV aufgeführt, die Bedeutung eines starken Smartphonebezuges dabei und das Potential der Abschaffung des unsicheren Loginzweifaktors SMS-mTAN.

Als weiterer zentraler Stakeholder identifiziert wurden identifiziert:

- Das Schweizer E-ID-Projekt, weil AGOV auch für den E-ID-Einsatz genutzt werden wird aber technologisch dediziert separiert von der E-ID ist, was gemeinsam kommunikativ korrekt abgebildet werden muss.
- Das BAG zwecks AGOV-Einsatzes für das elektronische Patientendossier
- Das SECO zwecks AGOV-Einsatzes für EasyGov speziell vor dem Hintergrund des Unternehmensentlastungsgesetzes UEG.

Die Primär-Stakeholder in der Projektführung des Vorhabens AGOV sind die DVS als Auftraggeberin, die BK DTI als Architektur- und temporäre Vorgabenstelle, das BIT als Leistungserbringer und das BBL als Beschaffungsträger, letzteres im Auftrage des BIT.

Folgende weiter entfernte Stakeholder wurden identifiziert:

Die IKT-Lieferanten der Schweizer Behörden. AGOV wird für deren Arbeit einfach zugänglich sein, da auf weltweit anerkannten Föderationsverfahren (OIDC und SAML) abstellend.

Nicht-behördliche Identitätsprovider und nicht-behördliche Applikationseigner (wobei bei SaaS der Abonnent, z. B. Kanton, als Eigner gilt und nicht der SaaS-Anbieter). Das EMBAG wird definieren, wo die Behördengrenze für die Nutzungslegitimation von AGOV sein wird, was voraussichtlich zum Ausschluss nicht klassisch behördlicher Entitäten führen wird.

5 Projektorganisation

Das Projekt wird nach HERMES geführt, die Umsetzung erfolgt agil. Die DVS hat die BK DTI mit dem Vorhaben AGOV via Vereinbarung beauftragt und überträgt die Mittel entsprechend. Die BK DTI beauftragt das BIT mit der agilen Umsetzung und führt in der Rolle Business-Owner und alimentiert mittels Dienstleistungsvereinbarung. Das BIT unterakkordiert Lieferanten.

5.1 Organisation nach HERMES

Projektausschuss:

Peppino Giarritta (Vorsitz, Auftraggeber)

Philipp Dasen (PL AGOV BK DTI)

Daniel Markwalder (Delegierter des Bundesrates DTI)

Dirk Lindemann (Direktor BIT)

René Staudenmann (BO IAM BIT)

Bruno Frutiger (Leiter DBS BK DTI)

Stefan Minder (BO AGOV eIAM BK DTI)

Marcel Kessler (Programmkoordination DVS)

Pilotkantone und interessierte Kantone sind Mitglied des Fachausschusses. Ein Vertreter, eine Vertreterin pro Pilotkanton kann auf Wunsch Mitglied des Projektausschusses sein. Pilotkantone definieren sich durch ihre Absichtserklärung, AGOV als Identitätsprovider und/oder Identitätsverbund produktiv zu nutzen.

Fachausschuss:

Zusammensetzung: Vertreter der Kantone, welche AGOV nutzen möchten oder daran interessiert sind. Vertreter der Bundesverwaltung. Wissenschaftlicher Beirat («Think Tank», Beratung und Ausführung von Evaluationsaufträgen und Rechtsanalysen; als Beispiel eines Evaluationsauftrags sei hier die Definition des Angebotes von möglichen Loginzweifaktoren in AGOV aufgeführt, die Bedeutung eines möglichen starken Smartphonebezuges dabei und das Potential der Abschaffung des unsicheren Loginzweifaktors SMS-mTAN, Aspekte der IAMV-Revision etc.). Aktuelle Fragen und Ergebnisse siehe <https://work.agov.ch?c=thinktank>)

Ziel des Fachausschusses ist die Formulierung von Empfehlungen zuhanden des Projektausschusses auf der Grundlage solide erhobener Fakten und Ansichten. Der Fachausschuss mit seinem wissenschaftlichen Beirat löst das Problem, dass bis jetzt im Vorhaben AGOV die Bundesverwaltung die wissensgebende Rolle dominiert.

5.2 Organisation agiler PoC

Kernteam:

Stefan Minder (BO BK DTI)

Stefan Hediger (Gesamtverantwortung PoC AGOV seitens Lieferanten)

Andres Aeschlimann (PL)

Hans Burger (PoC-Umsetzungsarchitekt)

Thomas Kinshofer (CISO AGOV eIAM)

Dominik Kuhn (Architekt QS und Kompatibilität BIT)

Das PoC-Kernteam steuert die agilen PoC-Teams beim Lieferanten für den Aufbau des funktionalen PoC per August 2023.

Team Entwicklung beim Lieferanten bis und mit produktive Fertigstellung Ende 2023:

PM (René Karoff)	Vier Frontend Developers (alternierend)
Business Analystin/Requirements Engineer	Vier Backend Developers (z.T. Juniors)
Zwei UX Spezialisten	Security Consultant
Ein PO Proxy (Andres Aeschlimann)	Drei IAM Engineers (z.T. Juniors)
Ein Software Architect	

5.3 Organisation nach SAFe (produktiver Betrieb im BIT, Wartung)

Agiler Release Train BIT:

René Staudenmann (BO IAM BIT)	Alexander Marti (RTE BIT)
Stefan Minder (BO AGOV eIAM BK DTI)	Christoph Grossmann (RTE BIT)
Michael Misteli (PPLM eIAM BIT)	Thomas Kinshofer (CISO AGOV eIAM)
Beat Schnyder (PM und Architekt BIT)	David Hyams (Architekt)
Lukas Scheuner (PM BIT)	Dominik Kuhn (Architekt)

Die Teams des Agile Release Train eIAM, rund 80 Personen, werden gemäss Umsetzungsausführungsvarianten Entscheid, welche im Kapitel 26.2 beschrieben sind, eingesetzt.

6 Rechtsgrundlagen

Der rechtliche Rahmen für die Nutzung von AGOV durch die Schweizer Behörden, auch ausserhalb der Bundesverwaltung, wird durch das Bundesgesetz über den eidgenössischen Finanzhaushalt FHG und das Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben EMBAG gesetzt. Der rechtliche Rahmen für den Umgang mit den Kerndaten in AGOV setzt die Verordnung über Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes IAMV. AGOV-nutzende Behörden müssen sich per Vereinbarung der IAMV unterstellen. Der rechtliche Rahmen für den Umgang mit den Randdaten von AGOV setzt die Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen (ugs. «Randdatenverordnung»). Da AGOV von der Bundesverwaltung betrieben wird und die Randdaten in dieser verbleiben, braucht es keine Unterstellung der AGOV-nutzenden Behörden ausserhalb der Bundesverwaltung unter die vorgenannte Randdatenverordnung. Die in den behördlichen Zielapplikationen anfallenden Randdaten, sofern die Zielapplikationen nicht der Bundesverwaltung im engeren oder weiteren Sinne gehören, fallen nicht unter die vorgenannte Randdatenverordnung, sondern sind kantonal zu regeln.

7 Semantik und Namensgebung

Semantisch ist AGOV ein Identitätsprovider und ein Identitätsverbund. Die Abkürzung AGOV ist abstrakt zu sehen, kann aber von den englischen Begriffen Authentication und Government hergeleitet werden. Die Definition der Abkürzung folgte den Kriterien, dass sie einfach aussprechbar ist, im näheren Themenfeld nicht anderweitig schon besetzt und nicht in die Landessprachen der Schweiz zu übersetzen, sondern eben abstrakt fungierend.

Die vollständige Bezeichnung des Identitätsproviders und Identitätsverbundes in fünf Sprachen ist wie folgt:

Authentifizierungsdienst der Schweizer Behörden AGOV

Service d'authentification des autorités suisses AGOV

Servizio di autenticazione delle autorità svizzere AGOV

Servetsch d'autentificaziun da las autoritads svizras AGOV

Authentication service of the Swiss authorities AGOV

8 Kosten und Finanzierung

AGOV hat folgende Kostenkomponenten:

1. Aufbau PoC
2. Aufbau Produktion
3. Betrieb und Wartung, ggf. Lizenzen
4. Identitätsabklärungskosten (z. B. Briefversand, Videoabklärung etc.)
5. Weiterentwicklung
6. Supportkosten End-User
7. Supportkosten Applikationseigner

Die Kostenkomponenten 1 und 2 sind durch die Investition durch die DVS gedeckt. Kostenkomponente 3 ist im ersten Produktionsjahr auch durch die Investition der DVS gedeckt. Danach soll eine adäquate Partizipation von DVS - zeitlich begrenzt - und besonders den Kantonen direkt, dies im Sinne der dannzumal im EMBAG verbrieften Kostenverteilungsprinzipien, erfolgen; mit Blick auf Kostenkomponente 3 geht es um die Deckung von 3 bis 4 MCHF p. a. beim Leistungserbringer BIT, beinhaltend auch sein Personal. Bei den Identitätsabklärungskosten (Komponente 4) sind Kosten pro natürliche Person im Bereich von 10 bis 40 CHF pro Rezertifizierungsperiode zu veranschlagen; es könnte von einer fünfjährigen Rezertifizierung ausgegangen werden; wird diese gestreckt, sinken die Kosten. Die Kostenkomponente 4 stellt im Pilot- und im Regelbetrieb ggf. eine Herausforderung dar. DVS stellt Überlegungen an, wie sie dabei unterstützen könnte.

End-User wollen auf eine behördliche Applikation zugreifen. Gelingt ihnen dies nicht, sollen sie sich primär an die applikationseignende Behörde wenden. Trotzdem muss es einen AGOV-Support geben. Der AGOV-End-User-Support hat das Potential, Vorläuferstruktur des E-ID-Supports zu sein. Das AGOV-Supportkonzept orientiert sich am Supportkonzept von Apple (vgl. Kapitel 9).

Die Kostenkomponente 7 wird als marginal eingeplant, weil der Anschluss von Zielapplikationen an AGOV im AGOV-Integrationsportal durch die Behörden respektive deren IKT-Dienstleister im Self-Service erfolgt, vergleichbar mit dem Anschluss einer Applikation an den Google-OIDC-IdP. Die Unterstützung der Behörden durch die Bundesverwaltung ist im Pilotbetrieb durch die Investition von DVS gedeckt, wenn diese in einem machbaren Rahmen liegt. Der machbare Rahmen kann so definiert werden, dass die im AGOV-Integrationsportal Handelnden dahingehend matur sein müssen, dass sie ohne fremde Hilfe mit den üblichen im Internet verfügbaren Anleitungen ihre Applikation an den Identitätsprovider von Google anschliessen könnten.

9 Supportorganisation für End-User

End-User wollen auf eine behördliche Applikation zugreifen. Gelingt ihnen dies nicht, sollen sie sich primär an die applikationseignende Behörde wenden. Trotzdem muss es einen AGOV-Support geben. Der AGOV-End-User-Support hat das Potential, Vorläuferstruktur des E-ID-Supports zu sein. Das AGOV-Supportkonzept orientiert sich am Supportkonzept von Apple.

1. Es gibt eine AGOV-Support-Internetseite.
2. Die AGOV-Support-Internetseite beinhaltet Anleitungen, FAQ und einen Wizard. Das Zentrum ist der Wizard.
3. Der Wizard stellt dem End-User Fragen zum Problem und unterbreitet Lösungsvorschläge.
4. Kommt der End-User zu keiner Lösung, bietet der Wizard einen Rückruf durch einen menschlichen Agenten an.
5. In dem Sinne kann der User an dieser Stelle selber ein Ticket erstellen, wobei seine E-Mailadresse und ggf. zusätzlich seine Telefonnummer validiert werden (technische Missbrauchsmassnahmen).
6. Es resultiert nun ein Supportgespräch ohne Warteschlange und auf bereits erhöhtem Niveau, da der ganze Wizardweg des End-Users automatisch im Ticket enthalten ist.

Die Anforderungen an den End-User sind somit Internetkonnektivität, E-Mail, telefonische Erreichbarkeit und die dafür notwendigen Skills. Da diese nicht über die Grundanforderungen für die AGOV-Nutzung an sich heraus gehen, sind sie als adäquat anzusehen.

Auf der AGOV-Support-Internetseite gibt es einen Zugang für Behörden zwecks Ticketeröffnung in ihrem Namen.

Der AGOV-Support-Wizard ist ein Frage-Antwort-Verzweigungssystem ohne künstliche Intelligenz. KI-Einsatz, wenn reif, ist zu einem späteren Zeitpunkt denkbar.

10 AGOV - logische Komponenten

Semantisch ist AGOV ein Identitätsprovider und ein Identitätsverbund. AGOV ist – rein morphologisch – aus End-User- und Behördensicht monolithisch. Effektiv ergeben sich jedoch folgende logischen Komponenten, die miteinander operieren:

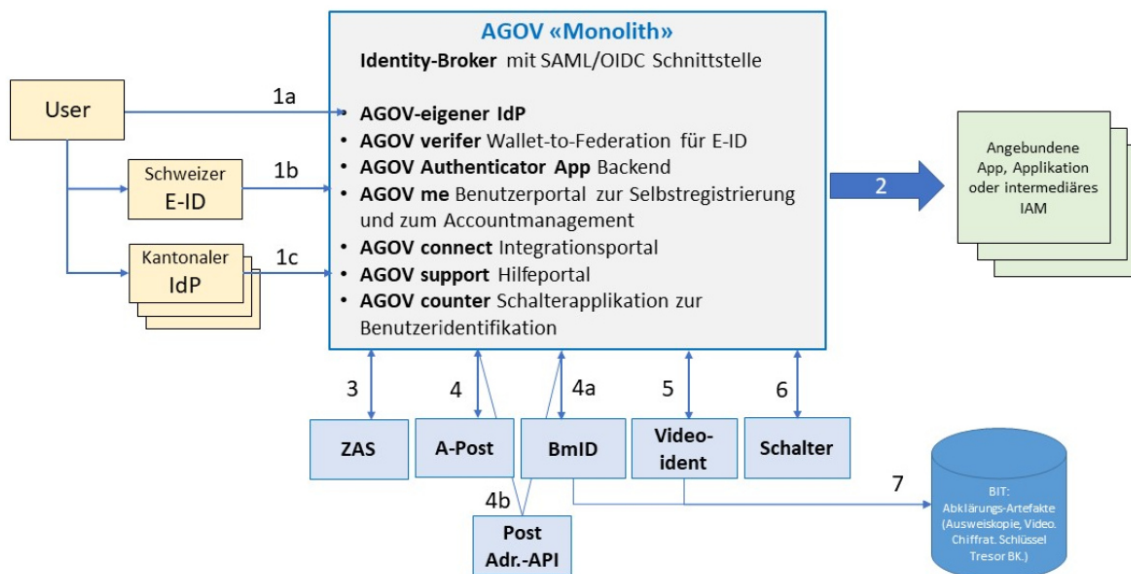
- End-User-Portal
 - o Selbstregistrierung (Eröffnung eines AGOV-Logins)
 - o Registrierung von Loginfaktoren (Credentials)
 - o Deklaration und Prüfung der AHV-Nummer
 - o Identitätsabklärung (z. B. Briefversand, Videoidentifikation, ...)
 - o Recovery
- AGOV-Authenticator-App und Backend dazu
 - o iOS- und Android-App zwecks passwordless Login via AGOV
- Identitätsmanagementsystem (IdM) und Identitätsprovider (IdP)

- Datenbankbasiertes Produkt als Persistenz-, Integritäts- und Managementlayer für die elektronischen Identitäten
- Broker
 - Ausstellung von OIDC- und SAML-Tokens zuhanden der Zielapplikationen
 - Entgegennahme von OIDC- und SAML-Tokens von an AGOV angeschlossenen (vor allem kantonalen) Identitäts Providern (Identitätsverbund)
 - Nutzung der Schweizer E-ID als Credential (Mittel zum Einloggen)
- Integrationsportal
 - Anschluss von Zielapplikationen (Webapplikationen und nativen Mobile Apps) mittels OIDC und SAML an AGOV im Self-Service durch die Behörden respektive deren IKT-Dienstleister.
 - Das BIT berechtigt für das Integrationsportal eine kleine Anzahl kantonalen Administratoren, welche weitere Personen berechtigen können.
- AGOV-Support-Internetseite
 - Gemäss Kapitel 9. Diese ist nicht integraler Bestandteil des End-User-Portals, sondern autonom.
- Nicht föderative Schnittstellen zu Drittsystemen
 - Kommunikation mit der ZAS zwecks Prüfung der AHV-Nummer
 - Kommunikation mit einem Druckstrassenanbieter zwecks Briefversand
 - Ggf. Kommunikation mit einem Videoidentifikationsserviceanbieter
 - Ggf. Kommunikation zu Behördensystemen oder dediziertes Web-GUI, für Identitätsabklärungen am Schalter der Behörde

AGOV bietet kein Accessmanagement, die Vergabe von Rechten, z. B. in Form von Rollen, ist Sache der Zielapplikationen oder intermediären IAM-Systemen bei der Zielbehörde.

11 Monolithische Sicht auf AGOV und die effektiv nicht monolithische Architektur darin

Die blauen Pfeile zeigen die exemplarischen Datenflüsse. Der grosse blaue Pfeil ist die einzige Schnittstelle zu den mit Authentifizierungen zu versorgenden Zielen, sprich SAML- und OIDC-Tokens enthaltend immer das ganze Attributset).



Legende der Datenflüsse:

1a	Benutzer verwendet zum Login direkt eine native AGOV-Identität.
1b	Auslieferung des «Verifiable Credentials» der CH E-ID an AGOV, falls ein Benutzer mit dieser einloggen will und die Pushnachricht entsprechend akzeptiert hat.
1c	SAML- und OIDC-Föderationen zwischen IdPs und AGOV.
2	SAML- und OIDC-Föderationen zwischen AGOV und authentifizierungskonsumierenden Zielsystemen. Aus Sicht Kantone ist Pfeil 2 die einzige AGOV-Fassade d.h. der alleinige Berührungspunkt.
3	Schnittstelle AGOV <-> ZAS, über welche geprüft wird, ob die behauptete AHV-Nummer zu den geprüften Attributen Namen, Vornamen und Geburtsdatum passen.
4	Schnittstelle, über welche A-Postbriefe durch AGOV an eine Druckstrasse übergeben werden.
4a	Schnittstelle, über welche BmID-Postbriefe durch AGOV an eine Druckstrasse übergeben werden. inkl. Datenrückfluss nach AGOV.
4b	Adressüberprüfungs-API der Post, damit vor dem Initieren eines Briefes (4 und 4a) die Adresse vorgeprüft werden kann (Verringerung der Fehlversände).
5	Schnittstelle, über welche AGOV den Benutzer zum Videoidentifikationsprozess führt (inkl. Bezahlungsfunktion und Datenrückfluss nach AGOV).
6	Anbindung der Schalterapplikation. In dieser können kantonale Mitarbeiter die Vorort Überprüfung von AGOV-Benutzer am Schalter abwickeln.
7	Abklärungsartefakte (z. B. Videoaufzeichnung) des Abklärungsprozesses und Ablage.

Die detaillierten Datenflüsse werden im separaten Dokument "AGOV-Datenflüsse" unter <https://work.agov.ch?c=agovstudie> beschrieben.

12 Loginfaktoren (Credentials)

Die für AGOV verwendete Basistechnologie ist vom CH-LOGIN der Bundesverwaltung abgeleitet und unterstützt eine Vielzahl von Loginfaktoren (Credentials) und Loginfaktorkombinationen wie klassische Passwörter kombiniert mit SMS-mTAN und moderneren, sichereren Lösungen.

Das Projekt AGOV verfolgt jedoch das Ziel, wenig sichere und veraltete Loginfaktoren von Anfang an nicht mehr anzubieten. Dieses Gebot der Zeitgemässheit lässt somit folgendes wegfallen: Passwörter, SMS mTAN, Sicherheitsfragen, Streichlisten und unspezifische Authenticator Apps z. B. von Google und Microsoft (diese Technologie stellt ein spezifisches Sicherheitsrisiko dar, weil Nachahmungen dieser Apps mit Schadcode im Umlauf sind).

Ziel ist, dass AGOV genau zwei Loginfaktoren anbietet (je einzeln und unabhängig funktionierend), beide sind sogenannten passwordless, der eine Loginfaktor benötigt ein nicht veraltetes, unkompromittiertes Smartphone als Funktionsgrundlage, der zweite nicht.

Die AGOV-Authenticator-App (iOS und Android) kann von den End-Usern weltweit kostenlos aus den entsprechenden offiziellen Online-Stores heruntergeladen und im AGOV-End-User-Portal registriert werden. Es handelt sich um eine AGOV-gebrandete Gehärtete Authenticator-App, welche auch im Polizeiwesen und im militärischen Umfeld der Schweiz für hohe Authentifizierungsqualitäten eingesetzt wird. Die AGOV-Authenticator-App funktioniert im Push-Challengeverfahren passwordless. Die AGOV-Authenticator-App funktioniert nicht auf Smartphone-Emulatoren und veralteten oder kompromittierten Smartphones.

FIDO-Tokens. FIDO-Tokens sind kleine Hardwareelemente z. B. in Form eines USB-Sticks oder NFC-Sticks mit kryptografischem Chipsatz. Diese können im Elektronikhandel erworben und im AGOV-End-User-Portal registriert werden. Das AGOV-End-User-Portal kontrolliert zur Laufzeit die White-Liste der FIDO-Alliance, um nicht zugelassene, veraltete oder kompromittierte FIDO-Tokens abzulehnen.

Dank der Akzeptanz von FIDO-Tokens in AGOV besteht kein Smartphone-Zwang. Personen ohne Smartphones oder mit nicht zugelassenen Smartphones oder in Settings, wo der Smartphone-Einsatz nicht möglich oder nicht erwünscht ist, können so adäquat bedient werden.

Der Idealfall ist, dass Benutzer die AGOV-Authenticator-App UND einen FIDO-Token in AGOV registrieren, damit bei Verlust des einen Loginfaktors (Credentials) auf den anderen zurückgegriffen werden kann.

Die Kantone können für ihre Bürgerinnen und Bürger selber ein FIDO-Token-Angebot aufbauen, im Grosseinkauf sind diese sehr günstig und Branding ist möglich. Die Beschaffung von FIDO-Tokens kann (wie die Beschaffung der Smartphones) jedoch auch direkt den End-Usern überlassen werden.

Die AGOV-Authenticator-App kann spezifisch nur für AGOV verwendet werden und ist gegen Nachahmung geschützt. Die FIDO-Tokens sind nicht AGOV-spezifisch und können in allen Systemen genutzt werden, die FIDO-Tokens unterstützen. FIDO-Tokens sind gegen Nachahmung geschützt.

13 Authentifizierungsqualität und Credentials

Die Authentifizierungsqualität setzt sich aus drei Dimensionen zusammen:

1. Verwendete(s) Credential(s) (Loginfaktoren)
2. Abklärung der effektiven Identität der Person
3. Kopplung des Abklärungsprozesses mit den Credentials

Die Permutation von Einsatzmöglichkeiten dieser drei Dimensionen kann zu einer Vielfalt von Authentifizierungsqualitäten führen, was für die End-User nicht einfach zu verstehen ist. Deshalb werden in AGOV die Dimension 1 und 3 wie folgt fixiert:

- ➔ Die verwendbaren Credentials sind FIDO-Lösungen entweder in App- oder Hardware-Ausprägung (auch die verwendete Gehärtete Authenticator-App gebrandet als AGOV-Authenticator-App ist eine FIDO-Lösung). Es gibt also nur eine Credentialqualität, nämlich eine sehr hohe.
- ➔ Die Identitätsabklärung ist immer stark zum Credential gekoppelt, auch wenn Sie über einen Brief mit Einmalcode als Zwischenschritt erfolgt, denn der Brief wird unter Verwendung des Credentials bestellt und der Einmalcode kann nur genau wieder mit diesem Credential einmalig eingelöst werden.

Somit gibt es nur bei der Dimension Nummer 2 Flexibilität, in AGOV ist dies die Ausprägung «ungeprüft» (in einer Ausprägung) versus die Ausprägung «geprüft», (in mehreren Ausprägungen) wobei die verwendeten Identitätsabklärungsverfahren unterschiedliche Wertigkeit haben können.

Für AGOV sind fünf Authentifizierungsqualitäten geplant, die sich nur in der Abklärungsqualität unterscheiden, nämlich ungeprüft, zustellbarkeitsgeprüft (per Briefzustellung, z. B. A-Post wie beim BE-Login), stark identitätsgeprüft (per Ausweiskontrolle inkl. Ausweisspeicherung; dafür kommen die Verfahren BmID der Schweizer Post, Videoidentifikation und Schalterbesuch in Frage) und als fünfte und höchste Stufe «LOA3» das Level of Assurance LOA3 gemäss eCH0170 V2, diese Leistung wird von der zukünftigen Schweizer E-ID, direkt nutzbar in AGOV, erwartet. AGOVs Authentifizierungsqualitäten sind im Anhang 23.3 tabellarisch aufgeführt.

13.1 Die AGOV-Authentifizierungsqualität (AGOVaq) «ungeprüft»

Numerisch repräsentiert mit dem Wert 100. Ungeprüft in AGOV bedeutet, dass alle Angaben zur Person durch den End-User selbst deklariert sind und in keiner Weise überprüft wurden und somit keine Verlässlichkeit haben, sondern frei erfunden sein könnten. Es wird auch kein Registerabgleich gemacht. Die Authentifizierungsqualität ist vergleichbar mit einem Google-Login, wobei AGOV die robusteren Credentials (AGOV-Authenticator-App und FIDO-Tokens) einsetzt. In der Bundesverwaltung findet der Grossteil der E-Government-Geschäfte mit solchen ungeprüften elektronischen Identitäten statt (dazu mit schlechteren Credentials als in AGOV). Es soll einer der ersten Aufträge an den Fachausschuss sein, abzuklären, wie dies in der Bundesverwaltung rechtlich-organisatorisch ermöglicht wird. In der Bundesverwaltung wird diese Authentifizierungsqualität offiziell mit QoA30 beschrieben und ugs. als LOA2, welche allerdings wegen des fehlenden Registerbezugs im Sinne von eCH-0170 nicht effektiv erreicht wird.

13.2 Die AGOV-Authentifizierungsqualität (AGOVaq) «zustellbarkeitsgeprüft»

Numerisch repräsentiert mit dem Wert 200. Die AGOVaq «zustellbarkeitsgeprüft» von AGOV basiert auf dem Versand eines einmaligen Onboarding-Codes per Briefpost. Obwohl daraus keine verlässlichen Aussagen zur effektiven Identität der Zielperson abgeleitet werden können, hat sich dieses Verfahren im E-Government bewährt (vgl. BE-Login).

13.3 Die AGOV-Authentifizierungsqualität (AGOVaq) «stark identitätsgeprüft»

Numerisch repräsentiert mit dem Wert 300, wenn keine AHV-Nummer assoziiert ist, Wert 400 mit AHV-Nummer (geprüft über die ZAS-Schnittstelle). Die AGOVaq «stark identitätsgeprüft» von AGOV ist eine sehr hohe Authentifizierungsqualität. Obwohl in den Dimensionen «verwendete Credentials» und «Identitätsabklärungsverfahren» und «Kopplung» Verfahren angewendet werden, welche den Weg zu einem LOA3 nach eCH-0170 V2 eröffnen könnten, will AGOV dieses LOA3 per Definition nicht erreichen, weil die den drei Dimensionen vor- und nachgelagerten Auflagen zu erfüllen den Rahmen von AGOV sprengen würde und der resultierende Mehrwert für E-Government-Transaktionen in einem schlechten Verhältnis zum Aufwand läge. Ugs. wird bei der resultierenden Authentifizierungsqualität von AGOV von einem LOA2,5 gesprochen, was umschrieben werden kann als Einsatz hochkarätiger Credentials mit einer sehr starken Kopplung zu verlässlichen Identitätsabklärungsverfahren. AGOV wird voraussichtlich unter der Verwendung der zukünftigen staatlichen Schweizer E-ID Authentifizierungen auf LOA3 leisten.

13.4 Die AGOV-Authentifizierungsqualität (AGOVaq) «LOA3»

Die AGOVaq «LOA3» entspricht den Festlegungen im Standard eCH0170 V2 und ist durch die zukünftige staatliche Schweizer E-ID zu leisten.

14 Identitätsabklärungsverfahren

Nebst dem schwachen zustellbarkeitsgeprüften Verfahren A-Post-Brief, werden für AGOV folgende vier starken Identitätsgeprüften Verfahren diskutiert:

Brief BmID der Schweizer Post (Übergabe mit Ausweiskontrolle und Ausweiserfassung)

Dies ist die präferierte Variante der Bundeskanzlei. Ein End-User bestellt im AGOV-End-User-Portal den Brief, dies unter Verwendung der in Kapitel 12 ausgeführten Credentials. Der Brief wird nur in der Schweiz zugestellt, ausschliesslich an private Adressen und ausschliesslich persönlich übergeben (sogenannt eigenhändig), dies mit Kontrolle eines amtlichen Lichtbildausweises, Erfassung dessen und Datenrückfluss nach AGOV. Der Einmalcode ist unter Verwendung desselben Credentials einzulösen wie bei der Briefbestellung. Die Adresse für den Briefversand ist selbstdeklariert und hat keinen Registerbezug. Für dieses Identitätsabklärungsverfahren kann ein Onlinebezahlportal für Selbstzahler und/oder kantonal ausgegebene Voucher zwischengeschaltet werden.

Videoidentifikation

Die Bundesverwaltung setzt – ausserhalb des Vorhabens AGOV – Videoidentifikation mit menschlichem Agenten über die Firma Intrum ein. Dieses Identitätsabklärungsverfahren ist nicht unumstritten (Sicherheit, Usability, Kosten). Sollte es für AGOV eingesetzt werden, könnte ein Beschaffungsgeschäft – ggf. beim betroffenen Kanton - notwendig werden. Für dieses Identitätsabklärungsverfahren kann ein Onlinebezahlportal für Selbstzahler und/oder kantonal

ausgegebene Voucher zwischengeschaltet werden. Die Bundeskanzlei fokussiert für AGOV auf die briefliche Abklärung (und die Schalterabklärung).

Schalter Kantone / Gemeinden

Sollen Identitätsabklärungen an Schaltern von Kantonen und Gemeinden stattfinden, muss AGOV ein Benutzerinterface und ein Berechtigungssystem anbieten, dank denen die Kantons- und Gemeindemitarbeitenden die Abklärungsergebnisse eintragen. Herausfordernd ist die Qualitätssicherung des Abklärungsprozesses vor Ort und das darauf abstellende gegenseitige, schweizweite Vertrauen.

Pass-Chip auslesen durch End-User in einem Onlineprozess

Mangels PIN auf dem Schweizer Pass-Chip nicht allein stehend einsatzmöglich (dem Haben-Wissen-Paar fehlt der Teil Wissen als Credential). Nur in Kombination mit der Videoidentifikation. Viele Personen haben keinen Pass.

15 AHV-Nummer

AGOV End-User können Ihre AHV-Nummer hinterlegen und über die ZAS-Schnittstelle bestätigen lassen. Die AHV-Nummer wird in den OIDC- und SAML-Tokens an die Zielapplikationen mitgegeben.

16 Resultierendes Attribut-Set

1. Name*(n)**
2. Vorname*(n)**
3. Geburtsdatum*
4. Geschlecht*
5. Geburtsort***
6. Nationalität*
7. AHVN13***
8. Datum der Abklärung AGOV
9. Art der Abklärung AGOV
10. Ablaufdatum der Abklärung AGOV (= Datum der Abklärung plus 5 Jahre)M
11. Verifizierte**** E-Mail-Adresse (verwendet als Username)
12. AGOV-Authentifizierungsqualität AGOVaq (100,200,300,400,500)
13. AGOV-ID (technischer Identifikator, enumeriert)
14. Quell-IdP

*ab AGOVaq 300 in der von den Abklärungsdienstleistern erbrachten Symmetrie zu den Ausweisdaten

**ab AGOVaq 300 in der von den Abklärungsdienstleistern erbrachten Symmetrie zu Mehrfachnamen in den Ausweisdaten

***nur bei AGOVaq 400. AGOVaq 500 je nach Datensatz in E-ID.

****Bei der Erstregistrierung durch Code-Loop-Back auf Zustellbarkeit verifiziert

Jede AGOV-Kontoeröffnung beginnt mit der Selbstregistrierung durch den End-User im Self-Service. Dabei können beliebig viele Daten abgefragt werden, soweit es der rechtliche Rahmen zulässt. Grundsätzlich verfolgt AGOV das Gebot der Datensparsamkeit. Alle so erhobenen Daten sind selbstdeklariert. Ein Teil dieser Daten können in einem Abklärungsprozess geprüft werden, insbesondere sind dies Namen, Vornamen, Geburtsdatum. Die AHV-Nummer wird durch zwei Schritte verlässlich gemacht, siehe Kapitel 17.1, dabei ist eine Ergänzung mit dem Geburtsort möglich (geliefert über die ZAS-Schnittstelle). Die Abklärungsverfahren unterscheiden sich in Qualität und Attribut-Set. Während bei der Zustellung eines Einschreibens mit eigenhändiger Übergabe die Wohnadresse implizit geprüft wird (Zustellbarkeit), ist nicht gewährleistet, dass die Postangestellten die Korrektheit des Geburtsdatums überprüfen. Bei der Videoidentifikation sind Name, Vorname und Geburtsdatum gesichert, es gibt aber gar keinen Bezug zu einer Wohnadresse. Die resultierenden Attribut-Lücken sind durch nachgelagerte Registerabfragen im kantonalen IKT-Ökosystem durch die kantonalen Systeme selber zu füllen, wobei die AHV-Nummer als Identifikator hilfreich ist. Deshalb ist zu prüfen, wie AGOV-End-Benutzer zur Eingabe der AHV-Nummer bewogen werden können. Eine Obligatorisch-Erklärung könnte End-User ausschliessen.

17 End-User-Flow

17.1 Registrierung

1. AGOV-End-User-Portal aufrufen
2. AGOV-Konto eröffnen unter Angabe von Namen, Vornamen, Geburtsdatum und E-Mailadresse (ggf. weitere Daten, wenn erwünscht, notwendig und erlaubt)
3. Bestätigungscode eingeben, der per E-Mail versendet wurde
4. Loginfaktor (Credential) registrieren. Das ist die AGOV-Authenticator App oder ein FIDO-Token, vgl. Kapitel 12.
5. Optional: AHV-Nummer erfassen (Selbstdeklaration mit ZAS-Abgleich).
 - a. Es erfolgt eine Abfrage der ZAS-Schnittstelle. Wenn Namen, Vornamen, Geburtsdatum und AHV-Nummer zusammenpassen, wird dieses Datenset in AGOV eingefroren (oder der End-User entfernt die AHV-Nummer wieder). Wenn negativ, kann die AHV-Nummer nicht gespeichert werden. Dies ist keine Abklärung der Daten, sondern nur ein Einfrieren eines effektiv bei der ZAS existierenden Datensets.
6. Optional: Identitätsabklärungsverfahren durchführen (vgl. Kapitel 14)

17.2 Login

1. Zielapplikation aufrufen. Diese leitet automatisch an AGOV weiter
2. Loginfaktor (Credential) einsetzen. Das ist die AGOV-Authenticator App oder ein FIDO-Token, vgl. Kapitel 12.

18 Kompatibilität mit Identitätsprovider Dritter (Identitätsverbund)

Identitätsprovider Dritter können über SAML und OIDC an AGOV angeschlossen werden. Somit können Logins über Identitätsprovider Dritter ausgeführt werden, die Zielapplikation erhält dann trotzdem eine AGOV-Identität. AGOV bietet Step-Ups an, welche allfällige Lücken des Drittproviders schliessen, z. B. Abklärung, starker Loginfaktor, AHV-Nummer. Ein zu definierendes AGOV-Gremium muss die Aufnahmebedingungen für Identitätsprovider Dritter definieren sowie, ob hohen Authentifizierungsqualitäten Dritter im Verbund AGOV vertraut wird und diese darin weitergegeben werden sollen.

19 Kompatibilität mit der staatlichen Schweizer E-ID

Die zukünftige staatliche Schweizer E-ID wird via AGOV direkt als Loginfaktor (Credential) einsetzbar sein. Der Registrierungsprozess nach Kapitel 17.1. entfällt, ebenso entfallen Abklärungsprozess und Registrierung/Nutzung anderer Credentials (AGOV-Authenticator-App / FIDO-Tokens). Der Wechsel vom klassischen AGOV-Konto zur E-ID-Nutzung kann auf zwei Arten erfolgen, automatisiert über das gemeinsame Merkmal AHV-Nummer oder manuell durch einmaliges Doppellogin (Migrationswizard).

20 Sondernutzungen

20.1 Qualifizierte elektronische Signaturen

Authentifizierungen über AGOV können erst unter Nutzung der zukünftigen staatlichen Schweizer E-ID qualifizierte elektronische Signaturen auslösen, vorausgesetzt, die E-ID erreicht die angestrebte Qualität.

20.2 Elektronisches Patientendossier

Authentifizierungen über AGOV haben das Potential, für Zugriffe auf das elektronische Patientendossier eingesetzt zu werden. Es muss hierbei definiert und verbrieft werden, dass die von AGOV angebotene Authentifizierungsqualität – ugs. bewertet als LOA2,5 – dafür genügt. Eine allfällige Zertifizierung überprüft die Einhaltung der vorerwähnten zu verbriefenden Definition. Der Einsatz der zukünftigen staatlichen Schweizer E-ID via AGOV wird für den Zugriff auf elektronische Patientendossiers genügen, vorausgesetzt, die E-ID erreicht die angestrebte Qualität.

21 Schnitt des PoC per August 2023

Per August 2023 wird AGOV als funktionaler PoC erstellt. In diesem können die in Kapitel 17 beschriebenen Flows «Registrierung» und «Login» effektiv durchgeführt werden, inklusive der optionalen Schritte. Die Abklärungsprozesse werden im Mock-Modus mit Option zur Scharfschaltung (Details siehe Anhang Kapitel 27.2) angeboten, damit beim Ausprobieren keine Kosten entstehen und auch keine Wartezeiten (Briefversand).

22 Gouvernanz

Die Gouvernanz ist im Kapitel 18 erwähnten AGOV-Gremium festzulegen. Bis dahin wird auf die IKT-Vorgaben der Bundesverwaltung abgestellt. Übergeordnet gelten die Rechtsgrundlagen gemäss Kapitel 6.

23 Weitere Prozesse

Weitere Prozesse wie Recovery, Sperrung etc. sind im separaten Dokument «AGOV-Prozesse» unter <https://work.agov.ch?c=agovstudie> beschrieben.

24 Produktkatalog (Basisangebot und Zusatzangebote)

Der Produktkatalog ist ein separates Dokument, siehe <https://work.agov.ch?c=agovstudie> beschrieben.

25 Roadmap

Februar 2023: Gründung Fachausschuss und Onboarding interessierter Kantone, ggf. auch in den PA

März 2023: Definition des AGOV-Gouvernanz-Gremiums durch DVS.

August 2023: Funktionaler Prototyp steht bereit

Januar 2024: Version 1.0 ZH-ready (auf AZURE) → Pilotbetrieb produktiv

Verlauf 2024: AGOV-Betrieb ins BIT übernommen (PaaS-Readyness) → Produktion

Verlauf 2024: Version 1.1 Go Live mit kantonalen Applikationen nach Inkrafttreten des EMBAG

Verlauf 2024: Anschluss von Identitätsprovider Dritter (vgl. Kapitel 18) und Umsetzung neuer Anforderungen

So bald wie möglich (z. B. 2025): Nutzung der staatlichen Schweizer E-ID als Loginfaktor (Credential)

26 Varianten für die Umsetzung von AGOV

Die Ausgangslage für AGOV ist das CH-LOGIN der Bundesverwaltung, nämlich die Ausdehnung dessen Nutzung auf das E-Government anderer Schweizer Behörden als die Bundesverwaltung.

26.1 Umsetzungsvarianten

Varianten bieten sich für die Umsetzung von AGOV in zwei Dimensionen an:

1. a) Umwandlung des bestehenden CH-LOGIN
versus
b) Entwicklung eines neuen «leeren» Identitätsproviders
und
2. a) Eigenentwicklung
versus
b) Kauf eines IdP-Produktes

In der ersten Dimension wurde lange die Variante a) favorisiert. Nach vertiefter Analyse wurde festgestellt, dass die Gelegenheit genutzt werden sollte, ohne technologische Altlasten des bestehenden CH-LOGIN zu starten, damit die Bundesverwaltung dann das CH-LOGIN (und seine Altlasten) abbauen und auf AGOV setzen kann.

Da das CH-LOGIN eine Eigenentwicklung ist und sein Kern für AGOV übernommen wird, wurde in der zweiten Dimension von Beginn weg die Variante a) favorisiert, dies ist unverändert.

Die Autoren empfehlen somit die Variante «Neuer IdP in Eigenentwicklung» zur Wahl.

	Umwandlung CH-LOGIN	Neuer «leerer» IdP
Eigenentwicklung	-	empfohlen
Kauf eines IdP-Produktes	-	-

26.2 Umsetzungsausführungsvarianten

Bei der Betrachtung der Umsetzungsausführungsvarianten wird von der im vorangegangenen Kapitel empfohlenen Umsetzungsvariante «Neuer IdP in Eigenentwicklung» ausgegangen.

Die Umsetzungsausführung von AGOV gliedert sich in 4 Phasen:

1. Erstellung des Prototyps per August 2023
2. Erstellung der Version 1.0 ZH-ready mit Produktivziel Januar 2024
3. Erstellung der Version 1.1 mit Identitätsverbundsfähigkeit (Anschluss kantonaler IdPs) im Verlauf des Jahres 2024
4. Erstellung der Version 1.2 mit E-ID-Anbindung (Wallet-to-Federation-Service) auf den E-ID-Go-Live-Termin hin, z. B. 2025.

Bezüglich einer Umsetzungsausführungsvariantenwahl sind nur die Phasen 1 und 2 zu betrachten.

Varianten:

1. Gesamtheitliche Umsetzung der Phasen 1 und 2 durch den eIAM ART BIT
2. Umsetzung der Phase 1 extern und der Phase 2 durch den eIAM ART BIT
3. Umsetzung der Phasen 1 und 2 extern

Der Auftraggeber hat sich am 4. Mai 2023 für die Umsetzungsausführungsvariante 3 entschieden.

26.3 Betriebsvarianten

Da AGOV per 1.1.2024 produktiv eingesetzt wird, muss es rund zwei Monate vor diesem Termin betriebsbereit sein, damit bis Ende Jahr die ersten Teilnehmer angeschlossen werden können. Es müssen dabei Betriebsstart und konsolidierter Betrieb unterschieden werden, um Varianten mit unterschiedlichen zeitlichen Herausforderungen vorzulegen.

Varianten:

1. Betriebsstart in externem Rechenzentrum, konsolidierter Betrieb in Bundesrechenzentren.
2. Betriebsstart und konsolidierter Betrieb in Bundesrechenzentren.

Die zeitliche Herausforderung ist bei der Variante 1 kleiner, da die Betriebsumgebung des AGOV-PoC in Azure verwendet werden kann. Auftraggeber und Projektausschussmitglieder favorisieren die Variante 2, da nachhaltiger und politisch opportuner.

Die Stossrichtung per Projektausschusssitzung vom 4. Mai 2023 ist, dass die Vorbereitungen für beide Varianten getroffen werden, wobei der Bund mit Hochdruck auf die Variante 2 zuarbeitet und die Variante 1 als Rückversicherung fungiert, falls der Betrieb in einem Bundesrechenzentrum nicht fristgerecht zur Verfügung steht.

27 Anhänge

27.1 Änderungsverzeichnis

Version	Datum	Änderung	Autor
0.1-0.6	Januar 2023	Mehrere Initialdokumente	mis
0.7	31.01.2023	Konsolidiert, RC	mis
0.8	02.02.2023	Stakeholder ergänzt	mis
0.8.1	06.02.2023	Anhänge	mis
0.8.2	08.02.2023	Kapitel 3 <i>Anforderungen</i> eingefügt (Quelle Webseite) und Rechtschreibung	gas
0.8.3	16.02.2023	Qualitätsmodell 3-stufig, Aspekt LOA3	mis
0.8.32	17.02.2023	Diverse Änderungen	das/gas/mis
0.8.33	20.02.2023	Kap. 3 Pt1 mut. Pt8 neu, Kap 23.5 neu	mis
0.9	27.03.2023	Neue AGOVAq, Architekturbild und Prozessverweis	mis
0.9.1	06.04.2023	Reformulierung Leistung 5. Verweis auf Produktkatalog	mis
1.0	26.04.2023	Kleinere Text Ergänzungen, neue AGOV Abbildung Kap. 11 und neues Kap. 26 Varianten Freigabeversion	mis,dap
1.1	08.05.2023	Abbildung. Kap. 11, Kap. 26.2 ersetzt und Kap. 26.3 neu	Mis
1.2	13.07.2023	Änderung der Wertebezeichnungen (un)abgeklärt = (un)geprüft schwach abgeklärt = zustellbarkeitsgeprüft stark abgeklärt = stark identitätsgeprüft	gas

27.2 Ausführungen zum Mock-Modus

Die Mock-Modi müssen auch ausgeschaltet werden können, sprich der produktive Modus eingeschaltet werden können. Die Ausprägung des Mock-Modus der Videoidentifikation ist durch den Videoidentifikationsanbieter gegeben. Der Mock-Modus der postalischen Abklärungen soll einen Brief auf dem Bildschirm simulieren, damit der Einmalcode danach effektiv eingegeben werden muss.

27.3 Tabellarische Darstellung von AGOVs Authentifizierungsqualitäten

Basierend auf der Qualität der Identitätsabklärung. Die Credentialqualität ist für AGOV immer hoch (FIDO und FIDO-basierte Authenticator-App).

AGOV-Qualität	Identitätsabklärung	Beurteilung nach eCH0170	Wertigkeit gemäss eIAMs QoA
100 (ungeprüft)	Keine (selbstregistriert, kein Registerabgleich)	LOA1, obwohl verwendete AGOV-Credentials sehr stark	QoA30
200 (zustellbarkeitsgeprüft)	Versand Onboardingcode per A-Post	LOA2 wobei verwendete AGOV-Credentials besser	QoA38 (neu einzuführende Zwischenstufe)
300 (stark identitätsgeprüft ohne AHV-Nr.)	BmID-Brief, Videoident, Schalter	Kurz vor LOA3 (aber keine Zertifizierung)	QoA50
400 (stark identitätsgeprüft mit AHV-Nr.)	BmID-Brief, Videoident, Schalter	Kurz vor LOA3 (aber keine Zertifizierung)	QoA50
500 (LOA3)	CH E-ID oder anderweitig Konform zu eCH0170 V2	LOA3	QoA50

27.4 LOA3 in AGOV

AGOV wird vor der Einführung der staatlichen Schweizer E-ID keine Authentifizierungsleistungen auf Level of Assurance 3 gemäss eCH0170 V2 anbieten, obwohl gewisse Identitätsabklärungsverfahren dafür genügen könnten. Die AGOV-Infrastruktur ist jedoch auf LOA3 auszulegen, damit die für die E-ID anzunehmende LOA3 verlustfrei transportiert werden kann und das Potential für erfolgreiche Zertifizierungen besteht.

27.5 Besonderheiten bezüglich der AHV-Nummer

Bezüglich der AHV-Nummer sind folgende Besonderheiten zu berücksichtigen:

1. Selbstdeklaration der AHV-Nummer mit ZAS-Abgleich gem. Kapitel 15 nach der Identitätsabklärung
 - a. Ohne Veränderung der geprüften Daten (dazu ZAS passend)
 - b. Unter Veränderung der geprüften Daten (da nicht zu ZAS passend → Neuabklärung notwendig)
2. Entscheid, ob AHV-Nummer bei der AGOV-Qualität i alias QoA30 im Token immer unterdrückt werden soll, da keine Identitätsabklärung vorliegt.
3. Ermöglichen eines AuthN-Requests gegenüber AGOV, in welchem das Vorhandensein einer AHV-Nummer (unter Berücksichtigung des obgenannten Punktes 2) verlangt wird; AGOV reagiert mit entsprechendem step-up-artigen Userflow, wenn fehlend.