Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement des Innern EDI
Bundesamt für Sozialversicherungen BSV

Weisungen über die Sicherheit der gemeinsamen Anwendungen (SGA) in den Bereichen AHV/IV/EO/EL/FamZLw/FamZ

Gültig ab 1. Januar 2015

Stand: 1. Januar 2026

318.106.09 d SGA

01.26

Vorwort

Gemäss Art. 49e und 50b Abs. 1 AHVG regelt der Bundesrat den Zugriff auf das zentrale Register der Versicherten und der laufenden Leistungen, insbesondere in Bezug auf die Datensicherheit. Am 4. Juni 2010 beschloss der Bundesrat eine Reihe von Massnahmen für einen sicheren Zugang zum Datennetz des Bundes.

Gemäss Art. 63 Abs. 3 AHVG sorgt das Bundesamt für Sozialversicherungen (BSV) insbesondere für einen zweckmässigen Einsatz technischer Einrichtungen zur Vernetzung der Durchführungsstellen der ersten Säule und der Familienausgleichskassen mit der Zentralen Ausgleichsstelle (ZAS).

Gemäss Art. 176 Abs. 4 AHVV regelt das Bundesamt für Sozialversicherungen (BSV) die Zusammenarbeit zwischen den Durchführungsstellen der ersten Säule, der Familienausgleichskassen und der Zentralen Ausgleichsstelle (ZAS).

Darauf gestützt legt die vorliegende Version der vom BSV in Auftrag gegebenen Weisungen die allgemeinen Grundsätze für die Sicherheit der gemeinsamen, allen Durchführungsstellen zur Verfügung stehenden Anwendungen fest.

Die Initialversion der Weisungen fokussiert auf die Sicherheit der Zugriffe auf die gemeinsamen Anwendungen.

Vorbemerkung zur Fassung vom 1. Januar 2026
(aufgeführt werden nur wesentliche Änderungen)

Die Zwei-Faktor-Authentifizierung wird schrittweise auf das Behörden-Login «AGOV» umgestellt, wozu ein neues Kapitel 5 aufgenommen wurde.

Von dieser Anpassung ist gegenwärtig lediglich ein begrenzter Benutzerkreis betroffen, der Anwendungen nutzt, die über das CH-Login in Kombination mit einem Vasco-Token betrieben werden.

Der grosse Benutzerkreis, jener von Telezas3, wird voraussichtlich im Jahr 2027 auf «AGOV» umgestellt.

Vorbemerkung zur Fassung vom 1. Juli 2020
(aufgeführt werden nur wesentliche Änderungen)

Gestützt auf die Erfahrungen und Entwicklungen des Betriebs der gemeinsamen Anwendungen in den Bereichen AHV/IV/EO/EL/FamZlw/FamZ wurden gegenüber der Fassung vom 1.Januar 2017 die folgenden Änderungen vorgenommen:

– Rz 1213 (neu):
  Definition «Verwaltungsplattform für Authentisierungsmittel» aufgenommen.

– Rz 2313 (Anpassung):
  Präzisierung, dass die Vertrauensperson den RIO über die Löschung einer Zuweisung eines Authentisierungsmittels informieren muss.

– Rz 2325 (Anpassung):
  Präzisierung, dass bei der Rücknahme eines Authentisierungsmittels (Abgang oder Rollenwechsel) die Zuweisung zum Benutzer bzw. Benutzerin gelöscht werden muss.

– Rz. 3102 (Anpassung):
  Es ist möglich, die URL-Adressen der ZAS-Webdienste im Internet zu veröffentlichen. Der Zugang zu diesen ZAS WEB-Diensten ausserhalb des AHV/IV-Netzes wird möglich.

– Rz. 3103 (Anpassung):
  Der Zugang zu den WEB-Diensten der ZAS über das Internet erfordert eine maschinelle Authentifizierung (sedex-Zertifikat).

– Rz 4215 (neu):
  Die ZAMS prüft regelmässig die Zuweisung von Authentisierungsmittel bei gelöschten Benutzernamen und wird ermächtigt, wo nötig, Zuweisungen selber zu löschen.

Vorwort zum Nachtrag 2, gültig ab 1. Januar 2017

Die Weisungen wurden im Anschluss an die Inbetriebnahme der ALPS-Anwendung (Applicable Legislation Portal Switzerland) angepasst. Die zentrale Stelle der ZAS für die Zugriffsverwaltung auf gemeinsame Anwendungen (GECA) führt eine Liste der Vertrauenspersonen für alle gemeinsamen Anwendungen.

Vorwort zum Nachtrag 1, gültig ab 1. Januar 2016

Die Aufgaben der Zentralen Authentisierungsmittelstelle wurden der Zentralen Ausgleichsstelle abgetreten. Die Formulare, die mit den Weisungen SGA zusammenhängen, wurden angepasst und vereinfacht.

Inhaltsverzeichnis

Abkürzungen

AGOV	«Authentifizierung» und «Government»
AHV	Alters- und Hinterlassenenversicherung
AHVG	Bundesgesetz über die AHV
AHVV	Verordnung über die AHV
ALPS	Applicable Legislation Portal Switzerland
BK-DTI	Bundeskanzlei, Bereich Digitale Transformation und IKT-Lenkung
BSV	Bundesamt für Sozialversicherungen
DS	Durchführungsstelle
ESP	EESSI Swiss Plattform (vormals RINA)
FamZLw	Familienzulagen in der Landwirtschaft
FamZ	Familienzulagen
FIDO	Fast Identity Online
GAIME	Gestion Electronique des Documents de la CdC et de l'OAIE
GAV	Gemeinsame Anwendung Verantwortlicher
GECA	Zentrale Stelle der ZAS für die Zugriffsverwaltung auf gemeinsame Anwendungen
GUI	Graphical User Interface
JiveX	Anwendung für die Verwaltung von Röntgenbildern, Filmen (VIDAR-Scanner) oder CD's bei den IV-Stellen
KBI	Koordinations- und Bewilligungsinstanz

KSVRIV	Kreisschreiben zur Verwaltungsrechnung der IV-Stellen
QoA	Qualität der Authentifizierung
RINA	Reference Implementation for a National Application
RIO	Registration Identification Officer
sedex	sedex steht für «secure data exchange» und ist eine zentrale Kommunikationsplattform für die asynchrone Datenübermittlung zwischen Fachapplikationen von Organisationseinheiten der öffentlichen Verwaltung.
TEDAI	Traitement Electronique des Dossiers AI
WBG	Weisungen über Buchführung und Geldverkehr der Ausgleichskassen
ZAMS	Zentrale Authentisierungsmittelstelle
ZAS	Zentrale Ausgleichsstelle

Liste der mitgeltenden Dokumente zu diesen Weisungen

[1] Formular „Meldung Vertrauensperson“
[2] Formular „Meldung Registration Identification Officer (RIO)“
[3] Formular „Authentisierungsmittel“
[4] Formular „Antrag KBI“
[5] Formular "Zugriffsantrag/Nutzungsbedingungen ALPS Administrator AK"[1]

Die gültigen Listen und Formulare sind auf BSV Internet Webseite zu finden (Rubrik Vollzug/eGov/Formulare)

[1] In ALPS direkt verfügbar oder bei alps@bsv.admin.ch verlangen

Kapitel I

1. Geltungsbereich und Definitionen

1.1 Geltungsbereich

1101 Gestützt auf Art. 49e, 50b Abs. 1, Art. 59 Abs. 1 sowie Art. 63 Abs. 3 des Bundesgesetzes über die Alters- und Hinterlassenenversicherung (AHVG, SR 831.10), auf Art. 176 Abs. 4 der Verordnung über die Alters- und Hinterlassenenversicherung (AHVV, SR 831.101), auf Art. 66 des Bundesgesetzes über die Invalidenversicherung (IVG, SR 831.20) sowie auf den Bundesratsbeschluss vom 4. Juni 2010 (Zwei-Faktor-Authentisierung) legen die vorliegenden Weisungen die Rahmenbedingungen für die Sicherheit der gemeinsamen Anwendungen in den Bereichen AHV/IV/EO/ EL/ FamZLw/ FamZ fest.

1102 Gemeinsame Anwendungen stehen allen Durchführungsstellen zur Verfügung. Die Liste der gemeinsamen Anwendungen (z.B. ALPS) ist im Anhang 1.

1103 Diese Weisungen richten sich nicht an Mitarbeitern/innen des Bundes, die bereits mit einem Zwei-Faktor Authentifizierungsmittel ausgerüstet sind.

1104 Für Anwendungen, welche AGOV verwenden, sind die Bestimmungen gemäss Kapitel V beizuziehen.

1.2 Definitionen

1201 *Zwei-Faktor-Authentisierung für Personen*: besteht einerseits aus einem Zugang über ein technisches Hilfsmittel (Faktor Haben), das den Zugriff auf das Netzwerk des Bundes sicherstellt, und andererseits aus einem Benutzernamen und einem Kennwort (Faktor Wissen), mit dem der Zugriff auf die Anwendungen erfolgt.

1201.1 Bei AGOV hingegen ersetzen spezielle Apps[2] auf dem Smartphone oder Sicherheitsschlüssel (umgangssprachlich «FIDO-Stick») den bislang üblichen Benutzernamen und das Passwort inklusive Zweitfaktoren.

1202 *Rechner-Authentisierung:* erfolgt durch Maschinenzertifikate sowie Netzwerkkomponenten, welche die Sicherheit des Datenzugriffs erhöhen. Die Rechner-Authentisierung erfordert ein sedex-Zertifikat.

1203 *Authentisierungsmittel[3]:* Benutzer erhalten für die Zwei-Faktor-Authentisierung ein Authentisierungsmittel in Form eines physischen Datenträgers. Die BK-DTI definiert das zugelassene Authentisierungsmittel entsprechend der Vertraulichkeitseinstufung der Anwendungsdaten.

1204 *Identifikationsmittel*: Ausweisdokument, welches die zuständige Behörde ausstellt und welches die Identifikation einer Person ermöglicht. Die BK-DTI definiert die zugelassenen Identifikationsmittel.

1205 *Durchführungsstelle (DS)*: Durchführungsstelle von AHV/IV/EO/EL/ FamZLw/FamZ.

1206 *Vertrauensperson:* Rolle, die eine Mitarbeiterin oder ein Mitarbeiter der Durchführungsstelle wahrnimmt. Sie ist Ansprechstelle der Benutzer einer Durchführungsstelle und leitet deren Anträge (Zugriffe, Mutationen etc.) der Zentralen Stelle der ZAS für die Zugriffsverwaltung auf gemeinsame Anwendungen weiter.

1207 *Registration Information Officer (RIO):* Rolle, die eine Mitarbeiterin oder ein Mitarbeiter der Durchführungsstelle wahrnimmt. Er ist für die Verwaltung der Authentisierungsmittel zuständig, d.h. für die Bestellung der Authentisierungsmittel bei der Zentralen Authentisierungsmittelstelle und für

[2] swiyu-App mit der Schweizer e-ID und/oder AGOV access App
[3] Das in diesem Dokument verwendete Wort «Authentisierungsmittel» bezieht sich immer auf einen VASCO-Token (Hardwaregerät, welches zeitbasierte Einmalcodes wiedergibt)

die Erteilung bzw. Entfernung der Zuweisung eines Authentisierungsmittels zu einem Benutzer. Für die Anwendungen, welche auf AGOV umgestellt haben, wird die Rolle RIO nicht mehr benötigt.

1208 Gemeinsame Anwendung Verantwortlicher (*GAV)*: Verwaltet die Zugriffe auf die gemeinsamen Anwendungen in dessen Zuständigkeitsbereich.

1209 *Zentrale Authentisierungsmittelstelle (ZAMS)*: nimmt die Verwaltung der Authentisierungsanträge und die Zuteilung der RIO vor. Sie organisiert den zentralen Support. Sobald sämtliche Anwendungen auf AGOV umgestellt haben, wird die ZAMS nicht mehr benötigt.

1210 *Koordinations- und Bewilligungsinstanz (KBI)*: löst bzw. regelt die Ausnahmen, Unklarheiten und die nicht definierten Fälle aus diesen Weisungen.

1211 Zentrale Stelle der ZAS für die Zugriffsverwaltung auf gemeinsame Anwendungen (GECA): verwaltet die Liste der Vertrauenspersonen, nimmt die Rolle des GAV für die gemeinsamen Anwendungen bei der ZAS wahr und organisiert den zentralen AGOV-Support.

1212 ALPS Administrator AK: verwaltet die Zuteilung der Zugriffsrechte auf ALPS, organisiert die Zugriffe auf ALPS und ist der Ansprechpartner der Benutzer für die ALPS Anwendung.

1213 *Verwaltungsplattform für die Authentisierungsmittel*: Verwaltungsplattform, womit die RIO's die Authentisierungsmittel einem Benutzer bzw. einer Benutzerin zuweisen, sperren oder deren Zuweisung bei einem Abgang oder Rollenwechsel löschen können.

1214 *Authentisierung*: ist der Nachweis der Identität.

1215 *Authentifizierung*: ist die Prüfung der Identität durch das IT-System.

1216 *Autorisierung*: ist die Zuweisung von Rechten aufgrund einer nachgewiesenen Identität.

1217 *Fast Identity Online (FIDO)*: ist ein Protokoll, das eine sicherere und benutzerfreundlichere Alternative zum traditionellen Login mit Benutzername und Passwort bereitstellt.

1218 *Passkeys*: sind kryptografische FIDO-Anmeldedaten, die mit dem Konto eines Benutzenden auf einer Website oder in einer Anwendung verknüpft sind. Benutzernamen und Passwörter sind überflüssig. Stattdessen genehmigt ein Benutzer die Anmeldung mit demselben Verfahren, das er zum Entsperren seines Geräts verwendet (z. B. biometrische Daten, PIN, Muster).

Kapitel II

2. Persönlicher Zugriff

2.1 Grundsatz

2.1.1 Benutzer

2101 Die Anwendungen, welche eine Zwei-Faktor-Authentisierung benötigen und diejenigen die dies nicht benötigen (z.B. ALPS) befinden sich auf der Liste der gemeinsamen Anwendungen (siehe Anhang 1).

2102 Die Benutzer fordern über ihre Vertrauensperson den Zugriff auf einzelne gemeinsame Anwendungen, welche eine Zwei-Faktor-Authentisierung benötigen, an. Sie erhalten über ihre Vertrauensperson einen Benutzernamen und ein Kennwort oder einen Einladungslink für den persönlichen Zugriff auf die gemeinsamen Anwendungen.

2103 Nachdem die Benutzer durch den RIO identifiziert wurden, erhalten sie ihr Authentisierungsmittel.

2.1.2 Vertrauensperson

2111 Jede Durchführungsstelle (DS) bezeichnet im Rahmen der in Artikel 59 Absatz 1 AHVG garantierten Selbstverwaltung mindestens zwei und maximal zehn Vertrauenspersonen. Die Erreichbarkeit der Vertrauensperson muss während der üblichen Bürozeiten gewährleistet sein.

2112 Jede Vertrauensperson muss bei einer Durchführungsstelle unter Vertrag stehen. Die Vertrauensperson wird von der DS-Leitung ernannt. Beide Parteien müssen ein für diesen Zweck vorgesehenes Formular unterzeichnen und der GECA übermitteln.

2113 Jede Mutation betreffend einer Vertrauensperson ist der GECA zu melden.

2.1.3 Registration Identification Officer (RIO)

2121 Jede Durchführungsstelle bezeichnet im Rahmen der in Artikel 59 Absatz 1 AHVG garantierten Selbstverwaltung mindestens zwei und maximal zehn Registration Identification Officers (RIO). Die Erreichbarkeit der RIO während den üblichen Bürozeiten muss gewährleistet sein.

2122 Sind mehrere Durchführungsstellen (DS) der gleichen Leitung unterstellt, kann diese RIO bestimmen, die für alle angegliederten Stellen zuständig sind. Die Gruppierung von Stellen ist der KBI mittels Formulars „Antrag KBI“ [4] zu melden.

2123 Jeder/jede RIO muss bei einer Durchführungsstelle (DS) unter Vertrag stehen. Der/die RIO wird von der DS-Leitung identifiziert und ernannt. Beide Parteien müssen ein dafür vorgesehenes Formular „Meldung Registration Identification Officer (RIO)“ [2] unterzeichnen und der ZAMS übermitteln.

2124 Die Durchführungsstelle kann die Verantwortung ihrer RIO auf Drittstellen (z.B. Leistungserbringer) ausdehnen. Die

Ausdehnung der Verantwortung muss mittels Formulars „Antrag KBI“ [4] bei der KBI beantragt werden.

2125 Jeder Antrag betreffend Zuteilung, Mutation oder Aufhebung einer RIO-Rolle ist der ZAMS mittels Formulars „Meldung Registration Identification Officer RIO“ [2] zu melden.

2.1.4 ALPS Administrator AK

2131 Jede AHV Ausgleichskasse bezeichnet im Rahmen der in Artikel 59 Absatz 1 AHVG garantierten Selbstverwaltung mindestens zwei und maximal zehn ALPS Administratoren AK.

2132 Die Rolle ALPS Administrator AK ist erstmalig durch die Vertrauensperson zu beantragen (Rz 2102).

2133 Der Administrator ALPS AK und die Vertrauensperson unterschreiben die Allgemeinen Nutzungsbedingungen die im Formular [5] beinhaltet sind. Dafür unterschreiben beide Rollen das Formular [5] und senden es an die GECA.

2.1.5 Rollenbesetzung

2141 Die Rollen Vertrauensperson, ALPS Administrator AK und RIO können der gleichen Mitarbeiterin oder dem gleichen Mitarbeiter zugewiesen werden.

2.2 Identifikationsregeln

2201 Die RIO identifizieren Benutzer, die ihrer Durchführungsstelle oder einer Drittstelle (Rz 2124) angegliedert sind, anhand eines amtlichen, zum Zeitpunkt der Identifikation nicht abgelaufenen Lichtbild-Ausweises, d. h. anhand eines Reisepasses oder einer Identitätskarte. Eine Fotokopie oder eine elektronische Speicherung des Identifizierungs-Dokuments wird aufbewahrt. Dieses beinhaltet Vorname, Name, Foto und das Geburtsdatum sowie die Ausweis-Nummer und das Gültigkeitsdatum des Ausweises. Die Kopie oder die elektronische Speicherung wird bis zur Vernichtung des Personaldossiers aufbewahrt.

2202 Falls ein Benutzer/eine Benutzerin über kein gültiges amtliches Dokument verfügt, handelt es sich um einen Sonderfall, der über ein Ausnahmeverfahren durch die KBI zu genehmigen ist.

2203 Bei jeder Abgabe eines Authentisierungsmittels ist der/die RIO verpflichtet, die Identifikation des Benutzers/der Benutzerin vorzunehmen.

2.3 Aufgaben und Verpflichtungen

2.3.1 Aufgaben und Verpflichtungen der Benutzer

2301 Folgende Aufgaben und Verpflichtungen richten sich an gemeinsame Anwendungen, welche eine Zwei-Faktor-Authentisierung benötigen.

2302 Die Benutzer aktivieren das persönliche Authentisierungsmittel mit einem Link, den sie zuvor per E-Mail erhalten haben.

2.3.2 Aufgaben und Verpflichtungen der Vertrauensperson

2311 Die Vertrauensperson ist als einzige Rolle berechtigt, bei der GECA einen Antrag einzureichen. Sie spezifiziert, welchem Benutzer welche Zugriffsberechtigungen auf welche gemeinsame Anwendung erteilt werden sollen und informiert den/die RIO über die Zuweisung der Zugriffsrechte, wenn eine Zwei-Faktor-Authentisierung nötig ist.

2312 Der Zugriff wird mit den von der GECA zur Verfügung gestellten Formularen beantragt.

2313 Bei einer Neuzuweisung, einem Abgang oder Rollenwechsel eines Benutzers oder einer Benutzerin, muss die Vertrauensperson die vorzunehmende Mutation der GECA melden und den RIO innert 15 Tagen über die Mutation informieren, wenn eine Zwei-Faktor-Authentisierung nötig ist oder die Zuweisung eines Authentisierungsmittels gelöscht werden muss.

2.3.3 Aufgaben und Verpflichtungen des/der RIO

2321 Der/die RIO ist verantwortlich für die Identifizierung der Benutzer, welchen er/sie ein Authentisierungsmittel übergibt und zuweist. Diesbezüglich gelten die Identifikationsregeln (Rz 2201-2203).

2322 Der/die RIO erfasst und speichert die Identifikationsnummer und die Art des Ausweises auf der Verwaltungsplattform für die Authentisierungsmittel.

2323 Der/die RIO (auf Personenebene) führt eine Liste der zugewiesenen, der inaktiven (d. h. noch nicht zugewiesenen), der deaktivierten, der defekten und der verlorenen Authentisierungsmittel.

2324 Der/die RIO weist den Benutzern deren Authentisierungsmittel zu.

2325 Der/die RIO nimmt Authentisierungsmittel, die nicht mehr benötigt werden (Abgang oder Rollenwechsel) zurück, löscht in der Verwaltungsplattform für die Authentisierungsmittel die Zuweisung vom Authentisierungsmittel zum Benutzer bzw. Benutzerin und informiert die Vertrauensperson über die Rücknahme. Authentisierungsmittel, welchen die Zuweisung zu einem Benutzer oder einer Benutzerin gelöscht wurde, können weiterverwendet werden und im Rahmen der Zwei-Faktor-Authentisierung einem anderen Benutzer bzw. Benutzerin zugewiesen werden.

2326 Der/die RIO meldet Verluste oder defekte Authentisierungsmittel der ZAMS mittels Formulars „Authentisierungsmittel“ [3].

2327 Der/die RIO sorgt für eine umweltgerechte Entsorgung defekter Authentisierungsmittel (Batteriesammelstelle).

2328 Weitere Fälle und Ausnahmen werden durch die KBI geregelt.

2329 Der/die RIO bestellt die Authentisierungsmittel mittels Formulars „Authentisierungsmittel“ [3] bei der ZAMS.

2330 Der/die RIO bestätigt der ZAMS mittels Formulars „Authentisierungsmittel“ [3] den Erhalt der Authentisierungsmittel.

2.3.4 Aufgaben und Verpflichtungen des/der ALPS Administrator AK

2341 Der/die ALPS Administrator AK eröffnet ALPS Benutzernamen, verwaltet und löscht sie, falls nötig. Er/sie informiert die Vertrauensperson über Benutzerabgänge.

2342 Der/die ALPS Administrator AK informiert seine Benutzer über die allgemeinen Nutzungsbedingungen, die er selber unterschrieben hat (Rz 2133).

3. Rechner-Authentisierung

3.1 Grundsatz

3101 Der Zugriff eines Rechners auf gemeinsame Anwendungen erfordert keine Zwei-Faktor-Authentisierung.

3102 Zugriffe auf Applikationen erfolgen entweder über das Internet oder über das AHV/IV-Netz (folgen den Weisungen über den Anschluss ans Netzwerk (WAN)).

3103 Für die Rechner-Authentisierung (WEB Services) wird das sedex-Zertifikat verwendet.

Kapitel III

4. Zentrale Stellen

4.1 Gemeinsame Anwendung Verantwortlicher (GAV)

4.1.1 Grundsatz

4101 Jeder/jede GAV ist die Kontaktstelle zwischen einer bestimmten gemeinsamen Anwendung und den Vertrauenspersonen.

4102 Er/sie ist die Ansprechstelle der Vertrauenspersonen.

4103 Ein/eine GAV wird für jede gemeinsame Anwendung gemäss „Liste der gemeinsamen Anwendungen“ (siehe Anhang 1) durch die zuständige Stelle ernannt und dem KBI gemeldet.

4104 Jeder/jede GAV stellt die erforderlichen Formulare zur Verfügung. Jede Änderung in der Struktur der Formulare muss dem KBI unterbreitet werden.

4.1.2 Aufgaben und Verpflichtungen

4111 Der GAV verwaltet Zugriffs- und Benutzerberechtigungen für eine bestimmte gemeinsame Anwendung. Der Antrag wird durch die Vertrauensperson gestellt.

4112 Der/die GAV stellt eine Supportorganisation sicher, welche vom KBI genehmigt wird.

4113 Die GECA überprüft alle 6 Monate sämtliche Benutzernamen. Benutzernamen, welche seit mehr als 12 Monaten inaktiv sind, werden gelöscht.

4.2 Zentrale Authentisierungsmittelstelle (ZAMS)

4.2.1 Grundsatz

4201 Die Zentrale Authentisierungsmittelstelle ist die Koordinationsstelle zwischen den RIO und dem Lieferanten der Authentisierungsmittel.

4202 Die Rolle der ZAMS ist durch die ZAS wahrgenommen.

4.2.2 Aufgaben und Verpflichtungen

4211 Die ZAMS validiert die RIO, indem sie diese in der Verwaltungsplattform für die Authentisierungsmittel innert einem Arbeitstag nach Eintreffen des Formulars aktiviert und deaktiviert.

4212 Die ZAMS stellt sicher, dass die bestellten Authentisierungsmittel den Durchführungsstellen (DS) zugestellt werden.

4213 Die ZAMS führt das Inventar der verteilten Authentisierungsmittel, auf Ebene DS oder Gruppierung von Stellen.

4214 Die ZAMS stellt eine Supportorganisation sicher, welche vom KBI genehmigt wird.

4215 Die ZAMS überprüft alle 6 Monate bei den gelöschten Benutzernamen, ob noch ein Authentisierungsmittel zugewiesen ist. Ist dies der Fall, fordert die ZAMS den zuständigen RIO auf, die Löschung der Zuweisung des Authentisierungsmittels gemäss Rz. 2325 zu vollziehen. Die ZAMS ist ermächtigt, bei gelöschten Benutzernamen die Löschung von zugewiesenen Authentisierungsmitteln selber zu vollziehen.

4.3 Koordinations- und Bewilligungsinstanz (KBI)

4.3.1 Grundsatz

4301 Die Funktion Koordinations- und Bewilligungsinstanz (KBI) wird durch das BSV wahrgenommen (egov@bsv.admin.ch).

4302 Die KBI kann Ihre Aufgaben delegieren.

4.3.2 Aufgaben und Verpflichtungen

4311 Die KBI genehmigt die Anträge der GAV, der Zentralen Authentisierungsmittelstelle (ZAMS) und der Durchführungsstellen gemäss vorliegenden Weisungen.

4312 Die KBI regelt Sonderfälle auf Anfrage.

4313 Die KBI überprüft bei den Durchführungsstellen (DS) mindestens:

- die Anzahl RIO
- die Liste der berechtigten Benutzer
- die Ausweiskopien der berechtigten Benutzer
- die Liste der aktiven und inaktiven Authentisierungsmittel.

4314 Die KBI überprüft bei der GECA mindestens:

- die Liste der Vertrauenspersonen
- die Verwaltung der Mutationen der Vertrauenspersonen.

4315 Die KBI überprüft bei der Zentralen Authentisierungsmittelstelle (ZAMS) mindestens:

- die Liste der RIO
- die Verwaltung der Mutationen der RIOs
- das Inventar der Bestellungen der Authentisierungsmittel.

4316 Die KBI kann weitere Aspekte der Überprüfung definieren.

4.4. Zentrale Stelle der ZAS für die Zugriffsverwaltung auf gemeinsame Anwendungen (GECA)

4.4.1. Grundsatz

4411 Die GECA nimmt die Rolle der GAV für gemeinsame Anwendungen der ZAS und den AGOV-Support wahr. Zusätzlich verwaltet GECA die Liste der Vertrauenspersonen der Durchführungsstellen für alle gemeinsamen Anwendungen gemäss der Liste (siehe Anhang 1).

4412 Die Rolle GECA wird durch die ZAS wahrgenommen (access-center@zas.admin.ch).

4.4.2. Aufgaben und Verpflichtungen

4421 Die GECA verwaltet die Liste der Vertrauenspersonen der Durchführungsstellen.

4422 Die GECA sammelt sämtliche Zugriffsanträge auf gemeinsame Anwendungen.

4423 Die GECA prüft, dass die Zugriffsanträge durch eine Vertrauensperson beantragt werden.

4424 Die GECA leitet die Zugriffsanträge, falls die gemeinsame Anwendung nicht unter ihre Verantwortung steht, an der/die zuständige GAV weiter.

4425 Die GECA organisiert den zentralen AGOV-Support.

Kapitel V (AGOV)

5. Persönlicher Zugriff

5.1 Grundsatz

5101 Die Benutzer fordern über ihre Vertrauensperson den Zugriff auf eine gemeinsame Anwendung an.

5102 Beim Zugriff auf eine Anwendung, die mindestens AGOVaq300[4] erfordert, muss eine Videoidentifikation, welche kostenpflichtig ist, durchgeführt werden.

5103 Die Kosten für eine Videoidentifikation müssen vor Beginn der Videoidentifikation mit einem gängigen Online-Zahlungsmittel bezahlt werden. Die Organisation der Bezahlung und des Zahlungsmittels ist Aufgabe der DS.

5104 Falls kein Smartphone zur Anwendung kommt, erhält der/die BenutzerIn von der DS einen FIDO-Stick formlos-ausgehändigt.

5105 Die DS besorgen sich die FIDO-Sticks gemäss den Beschaffungsvorgaben (Kapitel 5.3.3) selber.

5.2 Videoidentifikationsregeln

5201 Die Identitätsprüfung eines Benutzers wird mittels Videoidentifikation durchgeführt. AGOV stellt dazu die Lösung «IDnow»[5] zur Verfügung.

5202 Die Voraussetzungen einer Videoidentifikation sind die folgenden:

[4] Schutzniveau der Bundesverwaltung: https://www.eiam.swiss/?c=eiam!qoa&l=de
[5] https://help.agov.ch/?c=videoident&l=de

- Die Videoidentifikation kann von Privatpersonen mit Schweizer oder ausländischer Wohnadresse genutzt werden.
- Die Identitätsprüfung ist 5 Jahre gültig.
- Für die Videoidentifikation werden folgende Ausweisdokumente akzeptiert:
    - Personalausweise und Reisepässe gemäss Länderliste.
    - Schweizer Aufenthaltsbewilligungen werden **nicht akzeptiert**.
    - Andere Ausweispapiere wie Führerschein, Swiss Pass, Studenten-Legis etc. werden **nicht akzeptiert**.
    - AGOV-Kontoinhaber/innen müssen persönlich zur Videoidentifikation erscheinen. Stellvertretungen sind **nicht möglich**.

5203 Falls ein Benutzer/eine Benutzerin über kein gültiges amtliches Dokument verfügt, kann keine Videoidentifikation durchgeführt werden und ein Zugang zur entsprechenden Anwendung ist nicht möglich. Ein Ausnahmeverfahren wie in Rz. 2202 beschrieben, existiert für AGOV nicht.

5.3 Aufgaben und Verpflichtungen

5.3.1 Aufgaben und Verpflichtungen der Benutzer

5311 Ein AGOV-Login ist persönlich. Es ist verboten, ein AGOV-Login zur Nutzung an eine oder mehrere andere Personen weiterzugeben.

5312 AGOV-Login-Konten sind personenbezogen und repräsentieren stets genau eine natürliche Person, unabhängig davon, ob diese via AGOV-Login für sich selbst oder im Auftrag, beispielsweise einer Körperschaft, handelt. Die Verantwortung für die ordnungsgemässe Nutzung der AGOV-Logins, der damit verbundenen Anwendungen und der darin durchgeführten Transaktionen liegt bei dieser natürlichen Person. Das bedeutet, dass die Person auch für die sichere Aufbewahrung und angemessene Verwendung der zugehörigen Loginfaktoren (AGOV access App und/oder Sicherheitsschlüssel) verantwortlich ist.

5.3.2 Aufgaben und Verpflichtungen der DS

5321 Die durch die DS bezahlten Kosten für eine Videoidentifikation oder einen FIDO-Stick können über folgende Verwaltungsrechnungs-Konten über den jeweiligen Fonds abgerechnet werden:

AHV-Ausgleichskassen gemäss WBG[6]:

212.3291 Kosten für Erwerb FIDO-Stick (AGOV Behörden-Login)

212.3292 Kosten für Videoidentifikation (AGOV Behörden-Login)

IV-Stellen gemäss KSVRIV[7]:

380.5391 Kosten für Erwerb FIDO-Stick (AGOV-Behörden-Login)

380.5392 Kosten für Videoidentifikation (AGOV Behörden-Login)

[6] https://sozialversicherungen.admin.ch/de/d/6925
[7] https://sozialversicherungen.admin.ch/de/d/6444

5322 Bei eigenständigen Familienausgleichskassen sind die Kosten für die Durchführung der Videoidentifikation und die Beschaffung der FIDO-Sticks von der jeweiligen Familienausgleichskasse selbst zu tragen.

5.3.3 Beschaffungsvorgaben FIDO-Sticks

5331 Diese Beschaffungsvorgaben gelten nur für jene FIDO-Sticks, bei welchen deren Beschaffungskosten über die Ausgleichsfonds oder GECA zurückgefordert werden.

5332 Der Beschaffungspreis für einen FIDO-Stick beträgt maximal CHF 30.00 (inkl. MWST, exkl. Versandgebühren). Für die Beschaffung eines teureren FIDO-Sticks kann durch die KBI eine Ausnahmebewilligung erteilt werden.

5333 FIDO-Sticks dürfen nur BenutzerInnen einer DS, welche einen Zugang zu einer AGOV-Anwendung benötigen, abgegeben werden. Die Abgabe an Private oder nicht AGOV-BenutzerInnen ist untersagt.

5334 Die Beschaffung und Aufbewahrung (Reserve) ist auf 10% der Anzahl Mitarbeitenden einer DS beschränkt.

5335 Die zurückgeforderten Beschaffungskosten werden durch das BSV kontrolliert. Jede DS muss die zurückgeforderten Beschaffungskosten jederzeit plausibel belegen können.

6. Inkrafttreten

6001 Diese Weisungen treten am 1. Januar 2017 in Kraft.

Anhang 1

Typ	Nom/Name
Fachanwendung ZAS	ACOR
Fachanwendung ZAS	Escal
Fachanwendung ZAS	FamZReg
Fachanwendung ZAS	EL-Register
Fachanwendung ZAS	Sumex
Fachanwendung ZAS	SWAP
Fachanwendung ZAS	NRA
Fachanwendung ZAS	NRR
Fachanwendung ZAS	GAIME
Fachanwendung ZAS	JiveX
Fachanwendung ZAS	TEDAI
Fachanwendung BSV	ALPS
Fachanwendung BSV	eRegress
Fachanwendung BSV	ESP