Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI
Office fédéral des assurances sociales OFAS

Directives sur la sécurité des applications communes (SAC) dans les domaines de l'AVS/AI/APG/PC/AFA/AF

Valables dès le 1er janvier 2015

Etat: 1er janvier 2026

318.106.09 f SAC

01.26

Avant-propos

Conformément aux articles 49*e* et 50*b,* al. 1, LAVS, l'accès aux registres centraux des assurés et des prestations, notamment en ce qui concerne la sécurité, relève du Conseil fédéral. Le 4 juin 2010, le Conseil Fédéral a décidé une série de mesures dans le but de sécuriser les accès au réseau de la Confédération.

Conformément à l'article 63 al.3 LAVS, l'Office fédéral des assurances sociales (OFAS) veille notamment à l'utilisation rationnelle des installations techniques reliant les organes d'exécution du premier pilier, les caisses d'allocations familiales et la Centrale de compensation (CdC).

Conformément à l'article 176 al. 4 RAVS, l'Office fédéral des assurances sociales (OFAS) règle la collaboration entre les organes d'exécution du premier pilier, les caisses d'allocations familiales et la Centrale de compensation (CdC).

En vertu des éléments ci-dessus, les présentes directives arrêtent les principes généraux en matière de sécurité des applications communes qui bénéficient à l'ensemble des organes et qui sont mandatées par l'OFAS.

Cette première version des directives se concentre sur les accès aux applications communes.

Remarque préalable à la version du 1er janvier 2026
(Seules les modifications essentielles sont mentionnées.)

L'authentification à deux facteurs sera progressivement mise en place pour la connexion des autorités « AGOV », ce qui a donné lieu à l'ajout d'un nouveau chaptire 5.

Pour l'instant, cette modification ne concerne qu'un nombre limité d'utilisateurs qui utilisent des applications fonctionnant avec CH-Login en combinaison avec un Vasco-Token.

Le grand groupe d'utilisateurs, celui de Telezas3, devrait passe à « AGOV » en 2027.

Remarque préalable à la version du 1er juillet 2020
(Seules les modifications essentielles sont mentionnées.)

Sur la base de l'expérience et de l'évolution de l'exploitation des applications communes dans les domaines de l'AVS/AI/APG/PC/AFA/AF, les modifications suivantes ont été apportées par rapport à la version du 1er janvier 2017 :

– Cm. 1213 (nouveau):
  Reprise de la définition « plateforme de gestion des moyens d'authentification».

– Cm. 2313 (adaptation):
  Précision que les personnes de confiance doivent informer le RIO de la suppression de l'attribution d'un moyen d'authentification.

– Cm. 2325 (adaptation):
  Précision que la reprise d'un moyen d'authentification (départ d'un collaborateur ou changement de rôle), l'attribution à un utilisateur ou à une utilisatrice doit être supprimée.

– Cm. 3102 (adaptation):
  Il est possible de publier les adresses URL des services Web de la CdC sur Internet. Les accès à ces services WEB hors du réseau AVS/AI devient de ce fait possible.

– Cm. 3103 (adaptation):
  L'accès aux services WEB de la CdC à travers Internet nécessite une authentification machine (certificat sedex).

– Cm. 4215 (nouveau):
  L'OCMA vérifie régulièrement l'attribution des moyens d'authentification pour les noms d'utilisateurs supprimés et est autorisé à supprimer lui-même les attributions si nécessaires.

Avant-propos au supplément 2, valable dès le 1er janvier 2017

Les directives ont été adaptées suite à la mise en service de l'application ALPS (Applicable Legislation Portal Switzerland).
Le centre de gestion centralisée des accès de la CdC (GECA) gère la liste des personnes de confiance pour toutes les applications communes.

Avant-propos au supplément 1, valable dès le 1er janvier 2016

L’organe central des moyens d’authentification a été remis à la Centrale de compensation. Les formulaires liés aux tâches des directives SAC ont été revus et simplifiés.

Table des matières

Abréviations

AF	Allocations familiales
AFA	Allocations familiales dans l'agriculture
AGOV	« Authentification » et « Government »
ALPS	Applicable Legislation Portal Switzerland
AVS	Assurance-vieillesse et survivants
CCAOAI	Circulaire sur le compte d'administration des offices AI
CdC	Centrale de compensation
ChF TNI	Chancellerie fédérale, Secteur Transformation numérique et gouvernance de l'informatique
DCMF	Directives sur la comptabilité et les mouvements de fonds des caisses de compensation
ESP	EESSI Swiss Plattform (auparavant RINA)
FIDO	Fast Identity Online
GAIME	Gestion Electronique des Documents de la CdC et de l'OAIE
GECA	Centre de gestion centralisée des accès de la CdC
GUI	Graphical User Interface
ICA	Instance de coordination et d'autorisation
JiveX	Application pour la gestion des radiographies, films (scanners VIDAR) ou CD par les offices AI
LAVS	Loi fédérale sur l'AVS
OE	Organe d'exécution

OCMA	Organe central de gestion des moyens d’authentification
OFAS	Office fédéral des assurances sociales
QoA	Qualité de l'authentification
RAC	Responsable d’application commune
RAVS	Règlement sur l’assurance-vieillesse et survivants
RINA	Reference Implementation for a National Application
RIO	Registration Identification Officer
sedex	sedex signifie « secure data exchange » ; il s’agit d’une plateforme de communication centrale pour la transmission asynchrone de données entre les applications métier des unités d’organisation de l’administration publique.
TEDAI	Traitement Electronique des Dossiers AI
UPIC	Unité de pilotage informatique de la Confédération

Liste des documents valables en complément à ces directives

[1] Formulaire « Annonce de personne de confiance »
[2] Formulaire « Annonce de Registration Identification Officer (RIO) »
[3] Formulaire « Moyens d'authentification »
[4] Formulaire « Demande à l'ICA »
[5] Formulaire « Demande d'accès d'un administrateur ALPS CC »[1]

Les listes et formulaires valables sont disponibles sur le site Internet de l'OFAS (rubrique Application/eGov/Formulaires)

[1] Directement disponible dans l'application ALPS ou peut être demandé à cette adresse e-mail : alps@bsv.admin.ch

Chapitre I

1. Champ d'application et définitions

1.1 Champ d'application

1101 En vertu des articles 49*e*, *50b*, al. 1, 59, al.1, et 63, al. 3, de la loi fédérale sur l'assurance-vieillesse et survivants (LAVS RS 831.10) ainsi que de l'article 176, al. 4, du règlement du 31 octobre 1947 sur l'assurance-vieillesse et survivants (RAVS, RS 831.101), de l'article 66 de la loi sur l'assurance-invalidité (LAI, RS 831.20) et de la décision du Conseil fédéral du 4 juin 2010 (authentification à deux facteurs), les présentes directives règlent les conditions-cadres pour la sécurité des applications communes dans les domaines de l'AVS/AI/APG/PC/AFA/AF.

1102 Les applications communes sont à disposition de l'ensemble des organes d'exécution. La liste des applications communes (p.ex. ALPS) se trouve à l'annexe 1.

1103 Ces directives ne s'appliquent pas aux collaboratrices et collaborateurs de l'administration fédérale qui disposent déjà d'un autre moyen d'authentification à deux facteurs.

1104 Les dispositions du chapitre V s'appliquent aux applications qui utilisent AGOV.

1.2 Définitions

1201 *Authentification à deux facteurs pour les personnes* : se compose, d'une part, d'un accès au moyen d'un support physique -ce que l'on détient- permettant d'accéder au réseau de la Confédération et, d'autre part, d'un nom d'utilisateur et d'un mot de passe -ce que l'on connaît- permettant d'accéder à une application.

1201.1 En revanche, avec AGOV, des applications spécifiques[2] sur le smartphone ou la clé de sécurité (communément appelée « clé FIDO ») remplacent le nom d'utilisateur et le mot de passe usuels, y compris l'authentification à deux facteurs.

1202 *Authentification machine :* réalisée par certificats pour machines ainsi que par composants, permettant d'augmenter la sécurité des accès aux données. Pour l'authentification machine un certificat sedex est nécessaire.

1203 *Moyen d'authentification[3] :* support physique remis à un(-e) utilisateur(-trice), permettant d'effectuer une authentification à deux facteurs. Le ChF TNI définit le moyen d'authentification autorisé en fonction de la classification du degré de confidentialité des données d'applications.

1204 *Moyen d'identification :* document d'identité délivré par l'autorité compétente, permettant d'identifier une personne. Le ChF TNI définit les moyens d'identification autorisés.

1205 *Organe d'exécution (OE)* : organe d'exécution des assurances AVS, AI, APG, PC, AFA et AF.

1206 *Personne de confiance* : rôle d'une collaboratrice ou d'un collaborateur de l'organe d'exécution. Elle est le point de contact des utilisateurs(-trices) d'un organe d'exécution et transmet les demandes (accès, mutations, etc.) au centre de gestion centralisée des accès de la CdC (GECA).

1207 *Registration Information Officer (RIO)* : rôle d'une collaboratrice ou d'un collaborateur de l'organe d'exécution. Il ou elle est chargé(-e) de la gestion des moyens d'authentification à deux facteurs, i.e. de la commande de moyens d'authentification auprès de

[2] L'application swiyu avec l'e-ID suisse et/ou l'application AGOV access
[3] Le terme « moyen d'authentification » utilisé dans ce document se réfère toujours à une clé VASCO (appareil qui transmet des codes uniques à durée de validité limitée)

l’organe central des moyens d’authentification et pour l’attribution, resp. révocation d’un moyen d’authentification à un(-e) utilisateur(-trice). Le rôle RIO n’est plus nécessaire pour les applications qui sont passées à AGOV.

1208 *Responsable d’application commune* (RAC): gère les demandes d’accès et mutations à l’application commune dont il est en charge.

1209 *Organe central des moyens d’authentification (OCMA)* : gère les demandes d’autorisations et les attributions des RIO. Il organise le support centralisé. Dès que toutes les applications sont passées à AGOV, l’OCMA n’est plus nécessaire.

1210 *Instance de coordination et d’autorisation (ICA)* : résout, resp. règle les exceptions, les ambiguïtés et les cas non définis dans ces directives.

1211 *Centre de gestion centralisée des accès de la CdC (GECA)* : gère une liste de personnes de confiance, assume le rôle de RAC pour les applications communes de la CdC et organise le support central d'AGOV.

1212 *Administrateur ALPS* : gère l'attribution des accès ALPS, l'organisation de la gestion des accès et est l'interlocuteur des utilisateurs pour l'application ALPS.

1213 *Plateforme de gestion des moyens d'authentification :* Plateforme de gestion, avec laquelle les RIO peuvent attribuer ou bloquer les moyens d'authentification à un utilisateur ou à une utilisatrice ou supprimer leur attribution en cas de départ ou de changement de rôle.

1214 *Authenticité* : preuve d'identité

1215 *Authentification* : contrôle de l'identité par un système informatique.

1216 *Autorisation* : attribution de droits sur la base d'une identité vérifiée.

1217 *Fast Identity Online (FIDO) : protocole proposant une alternative sécurisée et conviviale au login traditionnel, avec nom d'utilisateur et mot de passe.*

1218 *Passkeys* : données de connexion cryptographiques FIDO qui sont liées au compte d'un utilisateur sur un site web ou dans une application. Les noms d'utilisateurs et les mots de passe deviennent inutiles. En lieu et place, l'utilisateur approuve la connexion en utilisant la même procédure que pour déverrouiller son appareil (par ex. données biométriques, PIN, dispositif de verrouillage).

Chapitre II

2. Accès individuels

2.1 Principe

2.1.1 Utilisateurs(-trices)

2101 La liste des applications communes (voir annexe 1) renseigne sur les applications qui nécessitent une authentification à deux facteurs et sur celles qui n'en nécessitent pas (p.ex. ALPS).

2102 Pour les applications nécessitant une authentification à deux facteurs, les utilisateurs(-trices) font une demande auprès de leur personne de confiance pour accéder aux différentes applications communes. Ils reçoivent un nom d'utilisateur(-trice) et un mot de passe ou un lien d'invitation transmis par la personne de confiance pour l'accès individuel aux applications communes.

2103 Après avoir été identifiés par le RIO, les utilisateurs(-trices) reçoivent leur moyen d'authentification.

2.1.2 Personne de confiance

2111 Chaque organe d'exécution (OE) désigne au moins deux et au maximum dix personnes de confiance, conformément à l'autonomie garantie par l'article 59 al.1 LAVS. Une permanence pendant les heures usuelles de travail doit être assurée.

2112 Chaque personne de confiance doit être sous contrat d'un organe d'exécution. La personne de confiance est désignée par la direction de l'OE. Les deux parties signent le formulaire et le transmettent au GECA.

2113 Tout changement concernant une personne de confiance doit être communiqué au GECA.

2.1.3 Registration Identification Officer (RIO)

2121 Chaque organe d'exécution désigne au moins deux et au maximum dix Registration Identification Officers (RIO) conformément à l'autonomie garantie par l'article 59 al.1 LAVS. Une permanence pendant les heures usuelles de travail doit être assurée.

2122 Lorsque la responsabilité de plusieurs organes d'exécution (OE) est portée par une même direction, celle-ci peut nommer des RIO avec une responsabilité portant sur l'ensemble de ses entités. Le groupe d'entités doit être annoncé à l'ICA au moyen du formulaire "Demande à l'ICA" [4].

2123 Chaque RIO doit être sous contrat d'un organe d'exécution (OE). Le RIO est un (-e) utilisateur (-trice) identifié (-e) et désigné (-e) par la direction de l'OE. Les deux parties signent le formulaire "Annonce de Registration Identification Officer (RIO)" [2] et le transmettent à l'OCMA.

2124 L'organe d'exécution peut étendre la responsabilité de son RIO à une entité tierce (p.ex. fournisseur). L'extension de la responsabilité doit être demandée à l'ICA au moyen du formulaire "Demande à l'ICA" [4].

2125 Toute demande concernant une désignation, mutation ou révocation du rôle de RIO doit être communiquée à l'OCMA au moyen du formulaire "Annonce de Registration Identification Officer (RIO)" [2].

2.1.4 Administrateur ALPS

2131 Chaque caisse de compensation AVS désigne au moins deux et au maximum dix Administrateurs ALPS conformément à l'autonomie garantie par l'article 59 al.1 LAVS.

2132 L’attribution du rôle administrateur ALPS est demandée pour la première fois par la personne de confiance (cm 2102).

2133 Chaque administrateur ALPS ainsi qu’une personne de confiance signent les conditions générales d’utilisation intégrées dans le formulaire [5]. Les deux parties signent le formulaire [5] et le transmettent au GECA.

2.1.5 Occupation des rôles

2141 Les rôles de personne de confiance, d’administrateur ALPS et de RIO peuvent être assignés à une même collaboratrice ou à un même collaborateur.

2.2 Règles d’identification

2201 Le RIO identifie les utilisateurs(-trices) de son organe d’exécution ou d’une entité tierce (cm 2124) sur la base d’un document d’identité officiel (passeport ou carte d’identité) non expiré lors de l’identification, assorti d’une photo. Il conserve une photocopie ou un enregistrement électronique du document d’identification. Celui-ci contient le prénom, le nom, la photo et la date de naissance de l’utilisateur(-trice), ainsi que le numéro et la date d’expiration du document d’identité. La photocopie ou l’enregistrement électronique est conservé jusqu’à la destruction du dossier personnel.

2202 Si un(-e) utilisateur(-trice) ne possède pas de document d’identité officiel valable, il s’agit d’un cas particulier qui fait l’objet d’une procédure d’exception à valider par l’ICA.

2203 Lors de chaque réception d’un moyen d’authentification, le RIO doit identifier l’utilisateur(-trice).

2.3 Tâches et obligations

2.3.1 Tâches et obligations des utilisateurs(-trices)

2301 Les tâches et obligations suivantes se réfèrent aux applications communes nécessitant une authentification à deux facteurs.

2302 Les utilisateurs(-trices) activent le moyen d'authentification personnel avec un lien reçu par email.

2303 Le nom d'utilisateur(-trice), le mot de passe et le moyen d'authentification sont personnels et confidentiels.

2.3.2 Tâches et obligations de la personne de confiance

2311 La personne de confiance est seule habilitée à déposer une demande d'accès auprès du GECA. Elle spécifie les droits d'accès des utilisateurs(-trices) aux applications communes et informe le RIO de l'attribution de droits d'accès lorsque l'authentification à deux facteurs est requise.

2312 Les demandes d'accès sont à effectuer au moyen des formulaires mis à disposition par la GECA.

2313 En cas de nouvelle attribution, de départ de l'utilisateur(-trice) ou en cas de changement de rôle, la personne de confiance doit annoncer la mutation au GECA et la communiquer au RIO dans les 15 jours lorsque l'authentification à deux facteurs est requise ou si l'attribution du moyen d'authentification doit être supprimée.

2.3.3 Tâches et obligations du RIO

2321 Le RIO est responsable de l'identification des utilisateurs(-trices) auxquels il remet un moyen d'authentification. Pour cela, il applique les règles d'identification (cm 2201-2203).

2322 Il enregistre le numéro de la pièce d’identité ainsi que son type dans l’application de gestion des moyens d’authentification.

2323 Il gère une liste (au niveau des utilisateurs(-trices)) des moyens d’authentification attribués, inactifs (non-attribués), desactivés, défectueux et perdus.

2324 Il attribue les moyens d’authentification aux utilisateurs(-trices).

2325 Il récupère les moyens d’authentification qui ne sont plus attribués à un(-e) utilisateur(-trice) (départ ou changement de rôle), supprime sur la plateforme de gestion des moyens d’authentification l’attribution du moyen d’authentification à l’utilisateur ou l’utilisatrice et informe la personne de confiance de cette restitution. Les moyens d’authentification dont l’attribution à un utilisateur ou à une utilisatrice a été supprimé, peuvent à nouveau être attribués dans le cadre d’une authentification à double-facteur à d’autres utilisateurs.

2326 Il signale toute perte ou toute défectuosité d’un moyen d’authentification à l’OCMA au moyen du formulaire "Moyens d’authentification" [3].

2327 Il veille à une destruction écologique (point de collecte des piles) des moyens d'authentification défectueux dans les 90 jours.

2328 Les autres cas et exceptions sont réglés par l'ICA.

2329 Le RIO commande des moyens d'authentification auprès de l'OCMA au moyen du formulaire "Moyens d'authentification" [4].

2330 Le RIO confirme à l'OCMA la réception des moyens d'authentification au moyen du formulaire "Moyens d'authentification" [3].

2.3.4 Tâches et obligations de l'administrateur ALPS

2341 L'administrateur ALPS gère les comptes utilisateurs ALPS, les ouvre, les clôture et les modifie lorsque cela est nécessaire. Il informe la personne de confiance de tout changement concernant les comptes utilisateurs.

2342 L'administrateur ALPS informe les utilisateurs de l'application ALPS dont il est responsable des conditions générales d'utilisation à respecter et qu'il a lui-même acceptées et signées (cm 2133).

3. Authentification machine

3.1 Principe

3101 Les accès machines aux applications communes ne nécessitent pas d'authentification à deux facteurs.

3102 Les accès aux applications communes peuvent se faire soit par le réseau Internet soit par le réseau AVS/AI (en respect des directives sur le raccordement au réseau (DRR)).

3103 Pour l'authentification machine (services WEB), le certificat sedex est utilisé.

Chapitre III

4. Organe centraux

4.1 Responsable d'application commune (RAC)

4.1.1 Principe

4101 Chaque RAC est l'organe de contact entre une application commune particulière et les personnes de confiance.

4102 Il est l'interlocuteur des personnes de confiance.

4103 Pour chaque application commune selon la liste en annexe 1, un RAC doit être défini par l'organe responsable et annoncé à l'ICA.

4104 Chaque RAC met à disposition les formulaires nécessaires. Toute modification de structure de formulaire doit être soumise à la validation de l'ICA.

4.1.2 Tâches et obligations

4111 Le RAC gère les droits d'accès d'utilisateurs (-trices) à une application commune particulière. La demande est déposée par la personne de confiance.

4112 Le RAC met en place une organisation de support, à valider par l'ICA.

4113 Le RAC contrôle au moins tous les six mois les accès de tous les utilisateurs de l'application commune dont il est responsable. Les accès utilisateurs inactifs depuis plus de 12 mois seront effacés par la GECA sur demande de la personne de confiance.

4.2 Organe central des moyens d'authentification (OCMA)

4.2.1 Principe

4201 L'organe central des moyens d'authentification assume la fonction d'organe de coordination entre le fournisseur de moyens d'authentification et les RIO.

4202 Le rôle de l'OCMA est exercé par la CdC

4.2.2 Tâches

4211 L'OCMA valide les RIO en les activant et les désactivant dans l'application de gestion des moyens d'authentification dans un délai d'un jour ouvrable après réception de la demande.

4212 Il s'assure que les moyens d'authentification commandés sont remis aux organes d'exécution (OE).

4213 Il gère un inventaire des moyens d'authentification remis au niveau des OE et des groupes d'entités.

4214 Il met en place une organisation de support, à valider par l'ICA.

4215 L'OCMA vérifie tous les 6 mois si un moyen d'authentification est toujours attribué aux noms d'utilisateur supprimés. Si tel est le cas, l'OCMA demande au RIO responsable de supprimer l'attribution du moyen d'authentification conformément au Cm. 2325. L'OCMA est autorisé à supprimer les attributions des moyens d'authentification à des noms d'utilisateur supprimés.

4.3 Instance de coordination et d'autorisation (ICA)

4.3.1 Principe

4301 Le rôle d'instance de coordination et d'autorisation (ICA) est exercé par l'OFAS (egov@bsv.admin.ch).

4302 Elle peut déléguer ses tâches.

4.3.2 Tâches

4311 Elle valide les demandes des RAC, de GECA, de l'OCMA et des organes d'exécution conformément à ces directives.

4312 Sur demande, elle règle les cas particuliers.

4313 L'ICA contrôle au moins auprès des organes d'exécution (OE) :

- Le nombre de RIO
- La liste des utilisateurs (-trices) autorisés
- Les copies des pièces d'identité des utilisateurs (-trices) autorisés
- La liste des moyens d'authentification activés et inactivés

4314 L'ICA contrôle au moins auprès de GECA:

- La liste des personnes de confiance
- La gestion des mutations des personnes de confiances

4315 L'ICA contrôle au moins auprès de l'organe central des moyens d'authentification (OCMA) :

- La liste des RIO
- La gestion des mutations des RIO
- L'inventaire des commandes des moyens d'authentification

4316 L'ICA peut définir d'autres aspects à contrôler.

4.4. Centre de gestion centralisée des accès (GECA)

4.4.1. Principe

4411 En plus de ses tâches de RAC pour les applications communes de la CdC et le support d'AGOV, la GECA gère la liste des personnes de confiance des organes d'exécution pour toutes les applications communes de la liste en annexe 1.

4412 Le rôle de GECA est exercé par la CdC (access-center@zas.admin.ch).

4.4.2. Tâches

4421 La GECA gère la liste des personnes de confiance des organes d'exécution.

4422 La GECA reçoit toutes les demandes d'accès aux applications communes de la liste en annexe 1.

4423 La GECA vérifie que la demande d'accès a bien été déposée par une personne de confiance.

4424 La GECA transmet ensuite les demandes d'accès, lorsque l'application commune n'est pas de sa compétence, aux RAC compétents.

4425 La GECA organise le support central d'AGOV.

Chapitre V (AGOV)

5. Accès personnel

5.1 Principe

5101 Les utilisateurs demandent l'accès à une application commune en s'adressant à une personne de confiance.

5102 Lors de l'accès à une application qui requiert au minimum AGOVaq300[4], une vérification (payante) par vidéo doit être réalisée.

5103 Les coûts de la vérification par vidéo doivent être payés avec un moyen de paiement en ligne courant avant le début de la vérification. L'organisation du paiement et ses modalités incombent à l'organe d'exécution (OE).

5104 Si aucun smartphone n'est utilisé, l'utilisateur reçoit une clé FIDO sans formalités particulières de l'OE.

5105 Les OE se procurent eux-mêmes les clés FIDO selon les dispositions d'acquisition (chap. 5.3.3).

5.2 Règles d'identification par vidéo

5201 La vérification d'identité de l'utilisateur est réalisé par vidéo. À cet effet, AGOV met à disposition la solution « IDnow »[5].

5202 Les conditions d'une identification par vidéo sont les suivantes :

- Elle est possible pour les personnes domiciliées en Suisse ou à l'étranger.

[4] Niveau de protection de l'administration fédérale : https://www.eiam.swiss/?c=eiam!qoa&l=fr
[5] https://help.agov.ch/?c=videoident&l=fr

- Elle est valable cinq ans.
- Les documents suivants peuvent devoir être présentés lors de la vérification d'identité par vidéo :
    - cartes d'identité et passeports, selon la liste des pays ;
    - **ne sont pas acceptés** : permis de séjour suisses ;
    - **ne sont pas non plus acceptés** : d'autres documents tels que le permis de conduire, le SwissPass, la carte d'étudiant, etc. ;
    - le titulaire de compte AGOV doit procéder en personne à la vérification par vidéo**. Aucune autre personne** ne peut le remplacer lors de cette procédure.

5203 Si un utilisateur ne dispose pas d'un document d'identité officiel valable, la vérification par vidéo ne peut être réalisée et l'accès à l'application correspondante n'est pas possible. Une procédure d'exception, telle que celle décrite au ch. 2202, n'existe pas dans le cas d'AGOV.

5.3 Tâches et obligations

5.3.1 Tâches et obligations des utilisateurs

5311 Un login AGOV est personnel. Il est interdit de le transmettre à une ou plusieurs autres personnes.

5312 Les comptes AGOV sont individuels et représentent une unique personne physique, indépendamment du fait qu'elle agisse pour son propre compte via le login AGOV ou pour le compte, par exemple, d'une personne morale. La responsabilité de la bonne utilisation du login AGOV, des applications liées et des transactions qui y sont effectuées incombe à la personne physique. Autrement dit, cette personne est également tenue de conserver les facteurs de login correspondants (application AGOV access ou clé

de sécurité) en toute sécurité et de les utiliser de manière appropriée.

5.3.2 Tâches de l’organe d’exécution

5321 Les coûts payés par l’OE pour une vérification par vidéo ou une clé FIDO peuvent être comptabilisés sous les comptes d’administration suivants de chacun des fonds concernés :

Caisses de compensation AVS selon les DCMF :

212.3291 Coûts d’acquisition des clés FIDO (login officiel des autorités AGOV)

212.3292 Coûts liés à l’identification vidéo (login officiel des autorités AGOV)

Offices AI selon la CCAOAI :

380.5391 Coûts d’acquisition des clés FIDO (login officiel des autorités AGOV)

380.5392 Coûts liés à l’identification vidéo (login officiel des autorités AGOV)

5322 Dans le cas des caisses d’allocations familiales indépendantes, les coûts liés à la mise en œuvre de la vérification par vidéo et à l’acquisition des clés FIDO sont à la charge de la caisse d’allocations familiales concernée.

5.3.3 Dispositions d’acquisition

5331 Les dispositions d’acquisition ne concernent que les clés FIDO dont les frais d’acquisition sont remboursés par les fonds de compensation ou le GECA.

5332 Le prix d’acquisition d’une clé FIDO s’élève à 30 francs au plus (TVA incluse, hors frais d’envoi). L’ICA peut accorder une autorisation exceptionnelle pour l’acquisition de clés FIDO plus coûteuses.

5333

Les clés FIDO doivent être remises uniquement aux utilisateurs d'un OE ayant besoin d'un accès à une application AGOV. Toute remise d'une clé FIDO à une personne privée ou qui n'utilise pas AGOV est interdite.

5334 L'acquisition et la conservation (réserve) sont limitées à 10 % de l'effectif d'un OE.

5335 Le remboursement des frais d'acquisition est contrôlé par l'OFAS. Chaque OE doit pouvoir prouver en tout temps ses frais d'acquisition.

6. Entrée en vigueur

6001 Les présentes directives entrent en vigueur au 1er janvier 2017.

Annexe 1

Type	Nom
Application CdC	ACOR
Application CdC	Escal
Application CdC	RaFAM
Application CdC	RPC
Application CdC	Sumex
Application CdC	SWAP
Application CdC	NRA
Application CdC	NRR
Application CdC	GAIME
Application CdC	JiveX
Application CdC	TEDAI
Application OFAS	ALPS
Application OFAS	eRegress
Application OFAS	ESP