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 à partir du 1er janvier 2015

Etat: 1er Janvier 2017

318.106.09 f SAC

12.16

Avant-propos

Conformément à l'article 50b al.2 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.

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.

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.

Table des matières

Abréviations

AF	Allocations familiales
AFA	Allocations familiales dans l'agriculture
ALPS	Applicable Legislation Portal Switzerland
AVS	Assurance-vieillesse et survivants
CdC	Centrale de compensation
GECA	Centre de gestion centralisée des accès de la CdC
ICA	Instance de coordination et d'autorisation
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
RAC	Responsable d'application commune
RAVS	Règlement sur l'assurance-vieillesse et survivants
RIO	Registration Identification Officer
UPIC	Unité de pilotage informatique de la Confédération

Liste des documents valables en complément à ces directives

[1] Liste des applications communes
[2] Formulaire " Annonce de personne de confiance"
[3] Formulaire "Annonce de Registration Identification Officer (RIO)"
[4] Formulaire "Moyens d'authentification"
[5] Formulaire "Demande à l'ICA"
[6] Formulaire "Demande d'accès d'un administrateur ALPS CC"
[7] Formulaire "Demande d'accès d'un administrateur ALPS entreprise"

Les listes et formulaires valables sont disponibles à l'adresse www.bsv.admin.ch (rubrique pratique > exécution > eGov)

Chapitre I

1. Champ d’application et définitions

1.1 Champ d’application

1101 En vertu des articles 50b al.2, 59 al.1, 63 al.3 de la Loi fédérale sur l'assurance-vieillesse et survivants (LAVS RS 831.10) ainsi que de l’article 176, paragraphe 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) [1] est publiée par l’OFAS.

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.

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.

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 :* support physique remis à un(-e) utilisateur(-trice), permettant d'effectuer une authentification à deux facteurs. L'UPIC 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. L'UPIC 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 l'organe central des moyens d'authentification et pour l'attribution, resp. révocation d'un moyen d'authentification à un(-e) utilisateur(-trice).

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.

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 aussi le rôle de RAC pour les applications communes de la CdC.

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.

Chapitre II

2. Accès individuels

2.1 Principe

2.1.1 Utilisateurs(-trices)

2101 La liste des applications communes [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 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" [5].

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)" [3] 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" [5].

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)" [3].

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 [6]. Les deux parties signent le formulaire [6] 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.

2304 Le moyen d’authentification ne doit pas être emmené dans un pays étranger.

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 le 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.

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), les désactive et informe la personne de confiance de cette restitution. Les moyens d’authentification desactivés peuvent à nouveau être attribués.

2326 Il signale toute perte ou toute défectuosité d’un moyen d’authentification à l’OCMA au moyen du formulaire "Moyens d’authentification" [4].

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" [4].

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 se font par le réseau AVS/AI et en respect des directives sur le raccordement au réseau (DRR).

3103 Pour l'authentification machine, 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 [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 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 le 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.

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, le GECA gère la liste des personnes de confiance des organes d’exécution pour toutes les applications communes de la liste [1].

4202 Le rôle de GECA est exercé par la CdC (access-center@zas.admin.ch).

4.4.2. Tâches

4421 Le GECA gère la liste des personnes de confiance des organes d’exécution.

4422 Le GECA reçoit toutes les demandes d’accès aux applications communes de la liste [1].

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

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

5. Entrée en vigueur

5001 Les présentes directives entrent en vigueur le 1er janvier 2017.