



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 1^{er} janvier 2015

Etat: 1^{er} janvier 2016

318.106.09 f SAC

12.15

Avant-propos au supplément 1, valable dès le 1^{er} 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.....	5
Chapitre I	7
1. Champ d'application et définitions	7
1.1 Champ d'application	7
1.2 Définitions.....	7
Chapitre II.....	9
2. Accès individuels	9
2.1 Principe.....	9
2.1.1 Utilisateurs(-trices)	9
2.1.2 Personne de confiance.....	9
2.1.3 Registration Identification Officer (RIO)	10
2.1.4 Occupation des rôles.....	10
2.2 Règles d'identification	11
2.3 Tâches et obligations	11
2.3.1 Tâches et obligations des utilisateurs(-trices).....	11
2.3.2 Tâches et obligations de la personne de confiance	11
2.3.3 Tâches et obligations du RIO	12
3. Authentification machine.....	13
3.1 Principe.....	13
Chapitre III.....	13
4. Organe centraux	13
4.1 Bureau d'autorisation de l'application commune.....	13
4.1.1 Principe	13
4.1.2 Tâches et obligations	14
4.2 Organe central des moyens d'authentification (OCMA)	14
4.2.1 Principe	14
4.2.2 Tâches	14
4.3 Instance de coordination et d'autorisation (ICA)	15
4.3.1 Principe	15
4.3.2 Tâches	15
5. Entrée en vigueur.....	16

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 [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.

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 Tout 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 Occupation des rôles

- 2131 Les rôles de personne de confiance et de RIO peuvent être assignés à une même collaboratrice ou un même collaborateur.
- 2132 Une personne de confiance peut être en charge de plusieurs bureaux d'autorisation.

