Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Directives relatives au raccordement des caisses de compensation AVS et des offices AI au réseau AVS/AI (DRR)

Valable à partir du 1er juillet 2006

Etat: 1er janvier 2016

318.106.05 f DRR

01.16

Avant-propos

Conformément au mandat légal (art. 176, al. 4, RAVS), l'Office fédéral des assurances sociales (OFAS) veille à l'utilisation rationnelle des installations techniques destinées aux différents organes d'exécution AVS/AI, la Centrale de compensation (CdC) et d'autres institutions chargées de l'exécution des assurances.

L'utilisation des technologies de l'information et de la communication ne cesse de se développer au sein des organes d'exécution AVS/AI. Or les différents réseaux de télécommunication et le réseau TELEZAS 2, par lequel sont transmises toutes les données et informations des caisses de compensation et des offices AI (procédure ARC, consultation du registre central des assurés / des rentes, connexion Intranet, comptes individuels: transmission ou inscription) ont vieilli. Le projet de mettre sur pied un réseau commun pour les organes d'exécution du 1er pilier s'est alors imposé.
Ce réseau de transmission de données relie les organes d'exécution AVS/AI entre eux ainsi qu'avec les centres de calcul centraux et d'autres réseaux et sources de données.

Le réseau AVS/AI répond en outre à toutes les exigences en matière de sécurité des données, facilite la communication électronique et reste ouvert aux développements futurs.

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

Les modifications proposées visent à clarifier la question particulière du télétravail au cm 3010.

Les annexes 3 et 4 qui sont obsolètes ont été supprimées. Les chiffres marginaux 3004, 3005, 3006, 4018, 4019, 4020 ont été modifiés.

Le formulaire de demande se trouve sous :
www.bsv.admin.ch > Pratique> Exécution > eGov> Formulaires

Table des matières

Abréviations 7

Chapitre I 8

1. Généralités 8

2. Champ d'application et base juridique 8

Chapitre II 8

3. Réseau AVS/AI 8
   - 3.1 But 8
   - 3.2 Caractéristiques techniques 8
   - 3.3 Réglementations concernant le raccordement 9

Chapitre III 11

4. Définitions 11
   - 4.1 Organisation et structure 11
   - 4.2 Exploitant du réseau 11
     - 4.2.1 Définition 11
     - 4.2.2 Obligations et tâches 11
   - 4.3 Fournisseur du réseau 12
     - 4.3.1 Définitions 12
     - 4.3.2 Obligations et tâches 13
   - 4.4 Utilisateurs du réseau 13
     - 4.4.1 Définitions 13
     - 4.4.2 Obligations et tâches 14

Chapitre IV 15

5. Instance de coordination et d'autorisation (ICA) 15
   - 5.1 Bases 15
   - 5.2 Tâches 16

Chapitre V 16

6. Exigences en matière de sécurité et prescriptions relatives à la protection des données 16
   - 6.1 Principes de protection et de sécurité des données 16
   - 6.2 Mesures en cas de non-respect 17

Chapitre VI 18

7. Entrée en vigueur 18

Annexe 1 19

Réseau AVS/AI 19

Réglementation de domaine 19

1. Généralités 21
   - 1.1 Bases 21
   - 1.2 Points essentiels de la réglementation du domaine réseau AVS/AI 21
   - 1.3 Principes de protection et de sécurité des données 21

2 Modèle de domaines 22
   - 2.1 Modèle de domaines 22
   - 2.2 Domaine réseau AVS/AI 22
   - 2.3 Autres domaines 23
   - 2.4 Exigences en matière de domaines partenaires 24

3 Besoin de protection 25
   - 3.1 Besoin de protection du domaine réseau AVS/AI 25
   - 3.2 Besoin de protection des domaines partenaires 26

4 Ponts de réseaux 26
   - 4.1 Types de ponts 26
     - 4.1.1 Raccordement simple 26
     - 4.1.2 Pare-feu à états 27
   - 4.2 Ponts du réseau AVS/AI 27
     - 4.2.1 Vue d'ensemble 27
     - 4.2.2 Ponts décentralisés 28
     - 4.2.3 Ponts centraux 29
     - 4.2.4 Ponts des domaines partenaires 29
   - 4.3 Ponts spéciaux 30
     - 4.3.1 CC faisant partie d'une entreprise ou d'une association 30
     - 4.3.2 CC/OAI faisant partie d'un réseau cantonal 31
     - 4.3.3 Connexions à Internet pour les applications B2B32
     - 4.3.4 Accès via Internet RPV ou à distance 32

5 Voies de communication 33

6 Organisation..... 34

Annexe 2 35

Instance de coordination et d'autorisation (ICA) 35

Abréviations

ANS	Accord de niveau de service
AVS	Assurance-vieillesse et survivants
CC	Caisse de compensation AVS
CCa	Centre de calcul
ICA	Instance de coordination et d'autorisation
OAI	Office AI
OFAS	Office fédéral des assurances sociales
OFIT	Office fédéral de l'informatique et de la télécommunication
RAVS	Règlement sur l'AVS
RPV	Réseau privé virtuel
SAP	Service Access Point (Point d'accès au service)
WIsB	Directives du CF concernant la sécurité des TIC dans l'administration fédérale

Chapitre I

1. Généralités

1001 Les présentes directives régissent les conditions générales du raccordement des organes d'exécution AVS/AI et de tiers désignés par ces derniers au réseau AVS/AI, sur la base indiquée au ch. marg. 2001.

2. Champ d'application et base juridique

2001 Ces directives se fondent sur l'art. 176, al. 4, du règlement sur l'assurance-vieillesse et survivants (RAVS).

Chapitre II

3. Réseau AVS/AI

3.1 But

3001 Le réseau AVS/AI se compose de plusieurs réseaux logiques qui reposent sur l'infrastructure de transmission de l'administration fédérale. Il relie les organes d'exécution AVS/AI entre eux et garantit l'accès aux principales applications de la CdC, notamment au registre central.
Il facilite la communication entre les différentes institutions raccordées et peut s'adapter aux évolutions futures.
Les frais d'exploitation pour les prestations de base sont pris en charge par les assurances.

3.2 Caractéristiques techniques

3002 Les caractéristiques techniques du réseau AVS/AI sont fixées comme suit:

- différents réseaux logiques reposant sur l'infrastructure de transmission de l'administration fédérale;

- pare-feu central qui isole les différents réseaux logiques entre eux, et également par rapport aux autres réseaux de l'administration fédérale et à ceux qui y sont raccordés;
- accès central à Internet et connexion aux passerelles de messagerie de l'administration fédérale intégrant un filtre standard contre les mailware et les spams.

3.3 Réglementations concernant le raccordement

3003 S'agissant du raccordement des utilisateurs (pour la définition cf. ch. marg. 4015 ss) au réseau AVS/AI, les points suivants sont réglementés:
- le raccordement des organes d'exécution AVS/AI (ch. marg. 3004);
- le raccordement des centres de calcul (ch. marg. 3005);
- le raccordement de tiers (partenaires des organes d'exécution AVS/AI) et de réseaux extérieurs (ch. marg. 3006);
- le point d'accès au service (Service Access Point) du réseau AVS/AI (ch. marg. 3007);
- l'utilisation de l'accès central à Internet et de la passerelle de messagerie (ch. marg. 3008).

3004 1/16 Les organes d'exécution AVS/AI sont raccordés au réseau AVS/AI au moyen d'une connexion unique et d'une prestation de base selon les conditions fixées par l'OFAS.
Si un organe d'exécution nécessite plus d'un accès, une connexion supplémentaire peut être autorisée selon le ch. marg. 3009.
D'autres variantes de raccordement, par exemple un niveau de service plus élevé en raison d'un nombre très important d'utilisateurs, peuvent être envisagées à titre exceptionnel selon le ch. marg. 3009.

3005 1/16 Les centres de calcul, les centres de sauvegarde et centres d'impressions qui exploitent les applications informatiques et données au profit des organes d'exécution AVS/AI dans leurs propres locaux, sont raccordés au réseau AVS/AI sur demande à l'OFAS.
Les organes AVS/AI indiquent les centres de calcul qui doivent être raccordés au réseau en tant que tels. Le nombre de

connexions est fonction des besoins des organes d'exécution AVS/AI.
Le raccordement de centres de calcul doit être autorisé selon les conditions mentionnées au ch. marg. 3009.

3006 1/16 Le raccordement de tiers ou de réseaux externes au réseau AVS est possible selon les critères énoncés ci-dessous.
Le raccordement de tiers au réseau AVS/AI est obligatoirement soumis à une autorisation selon le ch. marg. 3009.
Les critères pour le raccordement de tiers au réseau AVS/AI sont les suivants:

- Ledit tiers fournit, à un ou plusieurs organes d'exécution AVS/AI, une prestation qui ne peut être apportée de manière efficiente qu'au travers d'un raccordement au réseau AVS/AI et qui est étroitement liée à l'exécution de l'AVS et de l'AI.
- Ledit tiers participe, avec un ou plusieurs organes d'exécution AVS/AI, à un échange de données (les transfère ou les reçoit) dans le cadre de l'exécution de l'AVS et de l'AI, qui ne pourrait être réalisé de manière efficiente sans un raccordement direct du tiers au réseau AVS/AI.

3007 Le point de raccordement au réseau AVS/AI se trouve obligatoirement dans les locaux de l'utilisateur. L'interface avec le réseau local (LAN) de(s) appareil(s) de raccordement (routeur) située dans les locaux de l'utilisateur est considérée comme étant le point d'accès au service (service access point, SAP).
La responsabilité du fournisseur du réseau cesse au point d'accès au service.

3008 Les utilisateurs raccordés au réseau AVS/AI utilisent obligatoirement l'accès Internet central et la passerelle de messagerie de l'administration fédérale.
Des exceptions peuvent être admises par l'instance de coordination et d'autorisation (ch. marg. 5001 ss) dans les cas fondés.

3009 Des modifications concernant les prestations du réseau, en particulier le débit et les prestations décrites à l'annexe 2

(partie «Autorisation»), doivent être demandées par le biais d'une procédure d'autorisation (ICA) puis approuvées.

3010 1/16 Pour le cas particulier du télétravail à l'intérieur du Pays, les documents suivants doivent être rassemblés et mis à disposition, sur demande du réviseur ou de l'auditeur :

- Règlement interne concernant le télétravail
- Directives ou police sur l'utilisation sécurisée des données en dehors du lieu de travail avec un schéma technique contenant les différents composants qui permettent le télétravail

Chapitre III

4. Définitions

4.1 Organisation et structure

4001 Le réseau AVS/AI est structuré comme suit:

- exploitant du réseau
- fournisseur du réseau
- utilisateurs du réseau

Le fournisseur du réseau est également l'instance de coordination et d'autorisation (ICA) au sens du ch. marg. 5001.

4.2 Exploitant du réseau

4.2.1 Définition

4002 Le réseau AVS/AI est exploité par l'Office fédéral de l'informatique et de la télécommunication (OFIT) sur mandat de l'Office fédéral des assurances sociales (OFAS). L'OFIT est donc l'exploitant du réseau AVS/AI.

4.2.2 Obligations et tâches

4003 L'exploitant du réseau fournit aux utilisateurs du réseau les prestations de télécommunications listées au ch. marg. 3002.

4004 L’exploitant du réseau assure, par une gestion efficace, l’exploitation du réseau AVS/AI jusqu’au point d’accès au service (SAP) inclus situé chez l’utilisateur, conformément au ch. marg. 3007.

4005 Les augmentations de débit, demandées par les utilisateurs, sont soumises à l’autorisation du fournisseur du réseau et effectuées par l’exploitant. L’exploitant du réseau veille à procéder rapidement à cette augmentation.

4006 L’exploitant du réseau veille au respect des directives relatives à la sécurité des données (ch. marg. 6002) au sein du réseau AVS/AI.

4007 L’exploitant du réseau offre un soutien technique aux organes d’exécution et met en place un service d’assistance central.

4.3 Fournisseur du réseau

4.3.1 Définitions

4008 Conformément au mandat légal (art. 176, al. 4, RAVS), l’Office fédéral des assurances sociales (OFAS) veille notamment à l’utilisation rationnelle des installations techniques destinées aux divers contacts entre les différents organes d’exécution AVS/AI, la Centrale de compensation (CdC) et d’autres institutions chargées de l’exécution des assurances.

4009 En tant que fournisseur du réseau, l’OFAS représente l’AVS et l’AI. En cette qualité, il est l’instance de coordination et d’autorisation (ICA) chargée de la gestion des nouveaux raccordements ainsi que des questions de coûts et de sécurité. L’ICA est présentée en détails dans l’annexe 2.

4010 Le fournisseur du réseau AVS/AI est partenaire contractuel de l’OFIT, exploitant de ce réseau, dans le cadre de l’accord

de niveau de service et de la convention de prise en charge des coûts.

4011 Le fournisseur du réseau AVS/AI est dépositaire de la réglementation de domaine de ce réseau et, partant, responsable de son application auprès des utilisateurs et de l'exploitant du réseau.

4.3.2 Obligations et tâches

4012 Le fournisseur du réseau est responsable de l'application des présentes directives auprès des utilisateurs et de l'exploitant du réseau.

4013 Le fournisseur du réseau conclut, pour le réseau AVS/AI, un accord de niveau de service avec l'exploitant, réglementant les prestations que doit fournir l'exploitant, les obligations et les droits réciproques des parties, de même que les aspects financiers.

4014 En tant que fournisseur du réseau, l'OFAS représente les intérêts des utilisateurs du réseau vis-à-vis de l'exploitant.

4.4 Utilisateurs du réseau

4.4.1 Définitions

4015 Par principe, tout organe relié au réseau AVS/AI est un utilisateur du réseau. Conformément au ch. marg. 3003, les utilisateurs peuvent être:

- des organes d'exécution AVS/AI (caisses de compensation AVS et offices AI);
- des centres de calcul;
- des tiers (partenaires des organes d'exécution AVS/AI).

4016 Les organes d'exécution AVS/AI peuvent se rassembler dans un pool. Dans ce cas, ils délèguent leurs droits et leurs obligations en tant qu'utilisateurs du réseau à ce pool. Ce dernier est alors chargé, en qualité de représentant de ses membres,

de respecter les directives relatives au réseau AVS/AI en vigueur.

4.4.2 Obligations et tâches

4017 Les utilisateurs du réseau sont responsables de la protection de leurs données, y compris celles se trouvant dans les centres de calcul (CCa). A cette fin, ils doivent mettre en œuvre des mesures adaptées. Cf. ch. marg. 6001 ss sur la protection des données.

4018 1/16 Chaque utilisateur du réseau dispose d'au moins un interlocuteur par emplacement raccordé, qui doit pouvoir donner des renseignements par téléphone en cas d'incidents techniques et être en mesure d'exécuter des manipulations simples (sur le routeur ou le modem) en suivant des instructions. Cette personne ou ce groupe de personnes doit être joignable durant les heures de service.
En outre, les utilisateurs mettent en place un service (service d'assistance, super user) qui, en temps normal, communique les annonces faisant état d'incidents techniques au centre d'appels de l'exploitant du réseau.

4019 1/16 L'utilisateur du réseau est responsable de la protection contre les accès non autorisés ou les interventions sur l'infrastructure de l'exploitant du réseau (OFIT). Il lui appartient également de veiller à ce que l'équipement de l'exploitant du réseau soit placé dans des locaux appropriés répondant aux exigences suivantes de sécurité :

Les locaux abritant la connexion au réseau AVS/AI doivent pouvoir être fermés à clé et ne pas se trouver dans une zone accessible à la clientèle.
L'accès aux appareils de raccordement au réseau doit être réservé aux personnes autorisées : p. ex. le personnel de maintenance sera toujours accompagné par un utilisateur du réseau et les interventions sur les composantes du réseau ne se feront que selon les instructions de l'exploitant du réseau.

4020 1/16 L'utilisateur du réseau garantit comme suit l'accès au site qui sera nécessaire en cas d'annonce d'incidents techniques:

- pendant les heures de bureau (du lundi au vendredi entre 7 h 30 et 17 h) pour les sites avec le niveau de service «critique»;
- 7 jours sur 7 et 24 heures sur 24 pour les sites avec un niveau de service «hautement disponible».

4021 Responsable de la sécurité informatique pour les utilisateurs du réseau

- Chaque utilisateur du réseau désigne une personne responsable de la sécurité informatique.
- Celle-ci a la responsabilité d'établir et de mettre à jour la réglementation de domaine de l'utilisateur du réseau.
- Elle communique à l'exploitant du réseau les adresses IP autorisées du sous-réseau pour un «raccordement simple».
- Elle définit, dans la réglementation de pare-feu, les règles applicables aux ponts centraux du réseau qui concernent l'utilisateur.
- Elle est l'interlocutrice de l'exploitant et du fournisseur du réseau pour tout événement ayant trait à la sécurité informatique.

Une CC ou un OAI peut confier la tâche de responsable de la sécurité informatique à un pool.

Chapitre IV

5. Instance de coordination et d'autorisation (ICA)

5.1 Bases

5001 La fonction d'instance de coordination et d'autorisation (ICA), qui fait office d'organe reliant le fournisseur et l'exploitant du réseau, est assurée par l'OFAS. En cette qualité, elle veille à répondre aux interrogations matérielles concrètes des utilisateurs concernant le réseau AVS/AI.

5002 L'ICA est ainsi responsable des tâches et des domaines suivants:

- coordination
- autorisation
- planification et direction
- contrôle
- direction de l'accord de niveau de service (ANS)
- gestion de la sécurité
- médiation
- administration

5.2 Tâches

5003 Les tâches précitées sont décrites en détails dans l'annexe 2.

Chapitre V

6. Exigences en matière de sécurité et prescriptions relatives à la protection des données

6.1 Principes de protection et de sécurité des données

6001 La sécurité du réseau se fonde sur les directives du CF concernant la sécurité informatique dans l'administration fédérale et sur la réglementation de domaine du réseau AVS/AI.

6002 La protection et la sécurité des données sont régies par les principes suivants:

- Les organes d'exécution raccordés au réseau AVS/AI garantissent le strict respect de la protection et de la sécurité des données en mettant en œuvre des mesures adaptées;
- Cette protection inclut également les centres de calcul (CCa) auprès desquels les caisses de compensation et les offices AI ont, le cas échéant, enregistré leurs données;
- Les données sont codées lors de leur transmission via le réseau AVS/AI. Conformément au ch. marg. 3007, le point d'accès au service du réseau AVS/AI est à chaque fois le point à partir duquel le codage intervient ou prend fin;

- La Centrale de compensation (CdC) est soumise aux dispositions de sécurité de l'administration fédérale. Elle demeure responsable de la protection des registres centraux.

6003 Principes régissant le raccordement de réseaux tiers:
- Les tiers sont raccordés en premier lieu via le réseau AVS/AI, qui garantit un contrôle simple de l'accès.
- L'annexe 1, ch. 4.2.4, énumère les conditions auxquelles des (domaines) tiers peuvent être raccordés directement à un organe

6004 Réglementation de domaine des organes raccordés
- Chaque CC/OAI établit sa propre réglementation de domaine pour ses systèmes et ses données, conformément aux prescriptions de l'annexe 1, ch. 4.2.

6.2 Mesures en cas de non-respect

6005 Lorsque l'exploitant du réseau (OFIT) constate des insuffisances ou des incidents en matière de sécurité ou de protection des données, il détermine, d'entente avec le fournisseur du réseau (OFAS), les mesures à prendre.

6006 L'exploitant du réseau peut, sans consulter préalablement le fournisseur, prendre immédiatement certaines mesures – p. ex. verrouiller un accès au réseau (SAP) – s'il estime qu'elles sont nécessaires pour garantir la sécurité du réseau.

6007 Une telle mesure se justifie notamment lorsque l'incident est dû à un non-respect de la réglementation de domaine ou qu'il est de nature à porter atteinte à l'ensemble du réseau AVS/AI.

Chapitre VI

7. Entrée en vigueur

7001 Les présentes directives entrent en vigueur le 1er juillet 2006

Annexe 1

Bundesamt für Informatik und Telekommunikation BIT
Office fédéral de l'informatique et de la télécommunication OFIT
Ufficio federale dell'informatica e della telecomunicazione UFIT
Uffizi federal d'informatica e telecommunicaziun UFIT

BSV / OFAS / UFAS /

Réseau AVS/AI

Réglementation de domaine

Etat du 1er juillet 2006

Table des matières

1. Généralités 21
1.1 Bases 21
1.2 Points essentiels de la réglementation du domaine réseau AVS/AI 21
1.3 Principes de protection et de sécurité des données 21

2 Modèle de domaines 22
2.1 Modèle de domaines 22
2.2 Domaine réseau AVS/AI 22
2.3 Autres domaines 23
2.4 Exigences en matière de domaines partenaires 24

3 Besoin de protection 25
3.1 Besoin de protection du domaine réseau AVS/AI 25
3.2 Besoin de protection des domaines partenaires 26

4 Ponts de réseaux 26
4.1 Types de ponts 26
4.1.1 Raccordement simple 26
4.1.2 Pare-feu à états 27
4.2 Ponts du réseau AVS/AI 27
4.2.1 Vue d'ensemble 27
4.2.2 Ponts décentralisés 28
4.2.3 Ponts centraux 29
4.2.4 Ponts des domaines partenaires 29
4.3 Ponts spéciaux 30
4.3.1 CC faisant partie d'une entreprise ou d'une association 30
4.3.2 CC/OAI faisant partie d'un réseau cantonal 31
4.3.3 Connexions à Internet pour les applications B2B32
4.3.4 Accès via Internet RPV ou à distance 32

5 Voies de communication 33

6 Organisation 34

1. Généralités

1.1 Bases

A. Directives relatives au raccordement des caisses de compensation AVS et des offices AI au réseau AVS/AI (DRR)
B. Directives du CF concernant la sécurité informatique dans l'administration fédérale (WIsB), ainsi que ses annexes 1 (Exigences de sécurité minimales et responsabilités relatives au besoin général de protection) et 2 (Définitions et directives concernant la sécurité des réseaux).

1.2 Points essentiels de la réglementation du domaine réseau AVS/AI

Les exigences de sécurité minimales citées dans WIsB portent sur

- l'organisation de la sécurité,
- le traitement des informations et des données,
- la sécurité physique,
- la gestion de réseaux et de systèmes,
- le contrôle d'accès,
- le développement et l'entretien des systèmes,
- le traitement des pannes et des urgences.

Se fondant sur ces bases, la réglementation du domaine réseau AVS/AI définit les exigences de sécurité plus étendues pour ce réseau.

1.3 Principes de protection et de sécurité des données

Les principes applicables en matière de protection et de sécurité des données dans le réseau AVS/AI sont définis dans DRR (chapitre V, chiffre 6.1).

2 Modèle de domaines

2.1 Modèle de domaines

La présente réglementation distingue les domaines suivants:

- le domaine réseau AVS/AI
- les domaines partenaires
- les domaines tiers

Les domaines sont reliés entre eux par des ponts de réseaux.

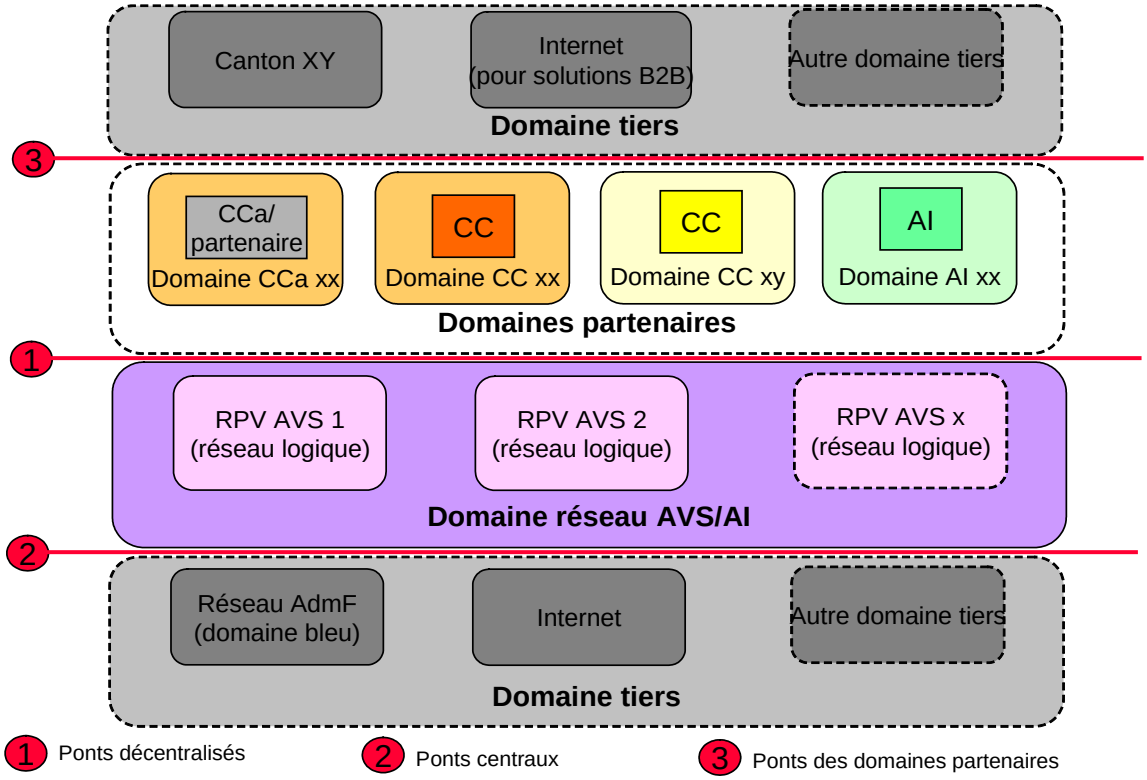


Figure 1: modèle de domaine réseau AVS/AI

2.2 Domaine réseau AVS/AI

Description

- Le domaine réseau AVS/AI est le réseau commun auquel sont raccordés tous les organes d'exécution de l'AVS/AI, leurs centres de calcul et des tiers (partenaires desdits organes).

- Le réseau AVS/AI est, un peu comme le réseau KOMBV-KTV[1], un simple réseau de transport.
- Le réseau AVS/AI est composé de plusieurs réseaux logiques et utilise l'infrastructure de transmission du réseau porteur Confédération.

Limite de domaine

- La limite de domaine se situe au point d'accès au service (SAP) du réseau AVS/AI (cf. DRR, ch. marg. 3007).
- Les ponts de réseaux centraux et décentralisés sont des éléments du domaine réseau AVS/AI.
- Les réseaux locaux (LAN) ainsi que les systèmes locaux des CC/OAI, de leurs centres de calcul et de leurs partenaires se trouvent à l'extérieur du domaine réseau AVS/AI. Ils sont connectés à celui-ci par des ponts de réseaux.
- Les systèmes de la CdC se trouvent à l'extérieur du domaine réseau AVS/AI[2]. Un pont de réseau permet d'avoir accès à ces systèmes depuis le réseau AVS/AI.

Exigences en matière de systèmes dans le domaine réseau AVS/AI

- Le domaine réseau AVS/AI sert exclusivement au transport de données et ne contient pas de systèmes au sens WIsB.
- Il n'est donc pas nécessaire de poser des exigences en matière de systèmes.

Propriétaire du domaine

- L'Office fédéral des assurances sociales (OFAS) est propriétaire du domaine réseau AVS/AI.

2.3 Autres domaines

Domaines partenaires

Sont considérés comme domaines partenaires du domaine réseau AVS/AI (énumération exhaustive):

[1] Réseau de communication qui relie tous les cantons de Suisse entre eux et avec les organes de la Confédération. Le réseau KOMBV-KTV est exploité, tout comme le réseau AVS/AI, sur la base du réseau porteur Confédération.

[2] Ils se trouvent dans le «domaine bleu» de l'administration fédérale.

- les organes d'exécution de l'AVS/AI (caisses de compensation et offices AI);
- le centre de calcul qui utilise des applications ou des systèmes pour un organe d'exécution;
- le partenaire d'un organe d'exécution qui fournit à l'AVS/AI des prestations de développement ou d'assistance dans le domaine informatique.

Un domaine partenaire est toujours directement connecté au domaine réseau AVS/AI, sans passer par un domaine intermédiaire

Domaines tiers

- Sont dénommés domaines tiers tous les réseaux tiers atteignables via les ponts centraux du domaine réseau AVS/AI ou connectés à un domaine partenaire par un pont.
- Exemples (énumération non exhaustive):
  – réseau de l'administration fédérale
  – réseau cantonal
  – Internet

2.4 Exigences en matière de domaines partenaires

Réglementation de domaine propre

- Chaque domaine partenaire établit, pour ses systèmes et ses données, sa propre réglementation de domaine[3], qui doit satisfaire aux exigences WIsB.

Simplification pour les membres d'un pool

- Les organes d'exécution de l'AVS/AI regroupés dans un pool peuvent établir une réglementation de domaine commune à tous les membres du pool.

Intégration de centres de calcul et de tiers

- Les centres de calcul et les tiers (partenaires des organes d'exécution de l'AVS/AI) doivent être intégrés dans la ré-

[3] Par réglementation de domaine, il faut en fait entendre une stratégie de sécurité informatique qui règle au moins les points exigés WIsB.

glementation de domaine d'un organe d'exécution ou d'un pool s'ils soient raccordés au réseau AVS/AI.

3 Besoin de protection

3.1 Besoin de protection du domaine réseau AVS/AI

Le besoin de protection du domaine réseau AVS/AI porte sur les éléments suivants:

- la confidentialité des données transmises;
- l'intégrité des données transmises;
- le contrôle de l'accès au domaine réseau AVS/AI;
- la disponibilité du réseau AVS/AI.

Confidentialité des données transmises

- Pour leur transmission via le réseau AVS/AI, les données doivent être codées par des procédés de cryptographie. Le point à partir duquel le codage intervient ou prend fin est toujours le point d'accès au service du réseau AVS/AI (cf. DRR ch. marg. 6002).

Intégrité des données transmises

- L'intégrité des données durant leur transmission via le réseau AVS/AI doit être garantie au moyen de fonctions de hachage cryptographique. Le point à partir duquel le codage intervient ou prend fin est, comme pour le codage, le point d'accès au service du réseau AVS/AI.

Contrôle de l'accès au domaine réseau AVS/AI

- Le réseau AVS/AI offre une protection de base aux organes raccordés par le fait qu'il n'admet que les ponts autorisés par l'OFAS.
- Aux ponts décentralisés et centraux, l'accès au réseau doit être limité aux adresses IP autorisées.
- Il n'y a pas d'authentification des utilisateurs à la limite du domaine réseau AVS/AI.

Disponibilité du réseau AVS/AI

- La disponibilité du réseau AVS/AI ne fait pas partie de la réglementation du domaine réseau AVS/AI; elle est décrite dans l'accord de niveau de service (ANS) concernant ce réseau. L'ANS fait partie du contrat entre le fournisseur (OFAS) et l'exploitant (OFIT) du réseau.

3.2 Besoin de protection des domaines partenaires

Les domaines partenaires déterminent eux-mêmes leur besoin de protection, en tenant compte des exigences du chapitre 2.4 les concernant.

Recommandation:
Il est recommandé aux domaines partenaires raccordés au réseau AVS/AI de prendre des mesures supplémentaires de protection de leur propres données contre les virus, le piratage, etc.

4 Ponts de réseaux

4.1 Types de ponts

4.1.1 Raccordement simple

Caractéristiques

- filtre de paquets,
- autorisation d'une communication au moyen d'adresses IP sources et cibles,
- physiquement, en général, un routeur.

Règles pour un raccordement simple

- Du domaine partenaire vers le réseau AVS/AI (entrée): la communication est en principe ouverte aux adresses IP autorisées du sous-réseau d'un domaine partenaire par les adresses cibles des registres centraux.

- D’autres voies de communication sont ouvertes aux adresses IP autorisées du sous-réseau avec l’autorisation préalable de l’exploitant du réseau.

Liste des adresses IP autorisées du sous-réseau

- Pour chaque raccordement simple, l’exploitant du réseau tient une liste des adresses IP autorisées du sous-réseau.

4.1.2 Pare-feu à états

Caractéristiques

- autorisation d’une communication basée sur des adresses IP source et cible et de l’adresse de port TCP ou UDP ainsi que sur les paquets antérieurs (pare-feu à états);
- physiquement, un pare-feu.

Règles pour un pare-feu à états

- Du réseau AVS/AI vers un domaine tiers (entrée):
  la communication est en principe ouverte aux adresses IP autorisées du sous-réseau d’un domaine partenaire par les adresses cibles des registres centraux.
- D’autres voies de communication sont définies dans une réglementation de pare-feu.

Réglementation de pare-feu

- Chaque pare-feu nécessite une réglementation et un programme d’exploitation qui décrivent au moins les points exigés WIsB.
- Il incombe à l’exploitant du réseau (et du pare-feu) d’établir cette réglementation et ce programme.

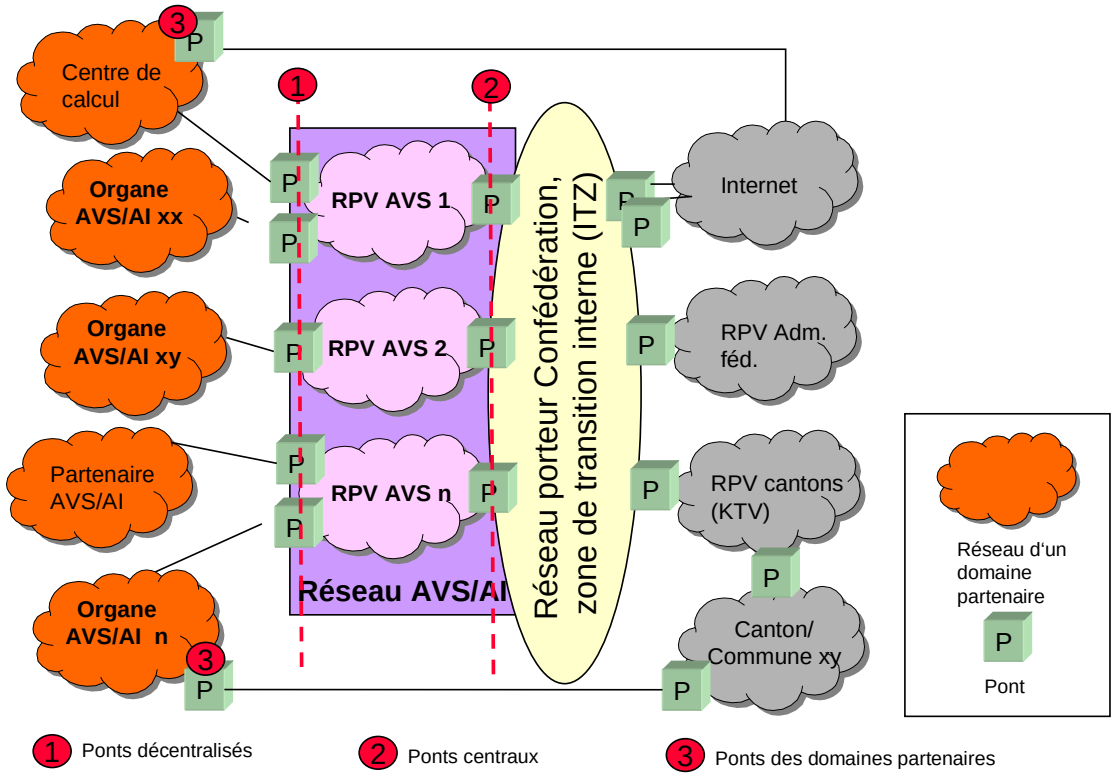
4.2 Ponts du réseau AVS/AI

4.2.1 Vue d’ensemble

Un pont connecte deux réseaux de manière à permettre une communication (un échange de paquets de données limité dans le temps) entre les deux.

Le réseau AVS/AI fait une distinction entre

- les ponts décentralisés,
- les ponts centraux et
- les ponts des domaines partenaires.



l'exploitation de tels ponts selon la présente réglementation de domaine (cf. ch. 4.2.4).

4.2.3 Ponts centraux

Chaque réseau logique du domaine réseau AVS/AI dispose d'un pont central qui le connecte à la «zone de transition interne» du réseau porteur de la Confédération.
Les ponts centraux sont toujours munis d'un pare-feu à états. Ils permettent l'accès aux réseaux suivants (énumération non exhaustive):

- d'autres réseaux logiques du domaine réseau AVS/AI,
- les registres centraux de la CdC dans le réseau de l'administration fédérale,
- Internet par l'accès Internet de l'administration fédérale,
- les réseaux cantonaux via KOMBV-KTV.

4.2.4 Ponts des domaines partenaires

Exigences minimales
Les domaines peuvent exploiter leur propre pont vers un domaine tiers aux conditions suivantes:

- L'OFAS a connaissance du pont vers le domaine tiers et l'a approuvé.
- La réglementation du domaine partenaire est approuvée par l'OFAS et respecte les prescriptions WIsB.
- Le pont vers le domaine tiers est décrit dans la réglementation du domaine partenaire.
- Le domaine partenaire veille à ce que l'accès au domaine tiers soit effectivement contrôlé au pont de réseau.
- Un pont vers Internet n'est autorisé qu'exceptionnellement et doit aussi être approuvé par l'OFAS.
- L'OFAS peut en tout temps effectuer ou faire effectuer par des tiers un audit portant sur la sécurité du domaine partenaire, y compris celle du pont vers le domaine tiers.

Exemples de ponts de domaines partenaires

- pont vers un réseau cantonal,
- pont vers Internet dans un centre de calcul qui exploite des applications B2B pour un organe d'exécution,
- pont vers le réseau étendu (WAN) d'une caisse de compensation reliant entre elles plusieurs de ses agences,
- pont vers un service médical régional (SMR).

4.3 Ponts spéciaux

4.3.1 CC faisant partie d'une entreprise ou d'une association

Quelques caisses de compensation sont, pour ce qui est du réseau, complètement intégrées dans une entreprise ou une association. C'est le cas des CC de Coop ou de Migros.
Le pont relie donc en fait le domaine réseau AVS/AI au réseau d'une entreprise ou d'une association. La CC n'est qu'une partie de ce réseau.
Seule la partie du réseau qui concerne la caisse de compensation constitue le domaine partenaire.

Réalisation du pont

Pour l'instant, un tel pont est toujours réalisé de manière décentralisée par un «raccordement simple» pour les raisons suivantes:

- Ce type de raccordement a également été toléré pour le réseau TeleZAS, précurseur du réseau AVS/AI.
- On utilise le même type de raccordement que pour un domaine partenaire, afin de garantir la même fonctionnalité.
- Il n'existe qu'un petit nombre d'organes d'exécution de ce type (cas spéciaux).

Ces raccordements simples constituent une exception à la règle selon laquelle les domaines partenaires doivent être raccordés au réseau AVS/AI sans passer par des domaines tiers.

Mesures destinées à réduire les risques

Les risques que comporte ce type de raccordement sont les suivants:

- Le réseau de l'entreprise ou de l'association n'a pas les mécanismes du réseau AVS qui garantissent la confidentialité et l'intégrité des données transmises.
- Le contrôle de l'accès au domaine réseau AVS/AI par des adresses IP autorisées est peu efficace, car ces adresses peuvent non seulement correspondre à des collaborateurs de la caisse de compensation, mais aussi cacher d'autres organes de l'entreprise ou de l'association.

Ces risques ne peuvent être réduits qu'en collaboration avec les entreprises ou associations concernées. Pour raccorder une CC faisant partie d'une entreprise ou d'une association, il faut prévoir, d'entente avec les responsables du domaine informatique, les mesures suivantes:

- ne donner l'accès au réseau AVS/AI qu'aux utilisateurs autorisés de la caisse de compensation;
- coder les données AVS/AI transmises par le réseau de l'entreprise ou de l'association par des procédés cryptographiques;
- garantir l'intégrité des données transmises au moyen de fonctions de hachage cryptographique.

4.3.2 CC/OAI faisant partie d'un réseau cantonal

Les caisses de compensation et les offices AI qui sont complètement intégrés dans l'infrastructure informatique d'un organe administratif (cantonal ou communal) constituent un cas spécial.

Dans la mesure du possible, ces organes utilisent l'infrastructure existante du réseau cantonal et ne sont pas raccordés au réseau AVS/AI.

- La Confédération est déjà reliée aux administrations cantonales par le réseau KOMBV-KTV, qui relie les cantons entre eux et avec les services de l'administration fédérale.
- Aujourd'hui déjà, les cantons et les communes utilisent le réseau KOMBV-KTV pour avoir accès aux registres centraux.
- Le réseau KOMBV-KTV est atteignable depuis le réseau AVS/AI par les ponts centraux.

Les organes d'exécution d'un canton reliés au réseau KOMBV-KTV sont, du point de vue du domaine réseau AVS/AI, considérés comme des domaines tiers.

4.3.3 Connexions à Internet pour les applications B2B

La présente réglementation de domaine est applicable par analogie au commerce interentreprise (business to business, B2B), tel qu'il existe par exemple sur la base de e-AVS/AI. Etant donné qu'il s'agit là d'une question d'actualité et souvent posée, elle est traitée explicitement ci-après:

- Un système B2B n'est jamais directement raccordé au domaine réseau AVS/AI.
- Les domaines partenaires raccordés au réseau AVS/AI qui exploitent des systèmes B2B et utilisent à cet effet des ponts vers des domaines tiers (p. ex. Internet) doivent remplir les exigences minimales pour l'exploitation d'un pont de domaine partenaire.
- Une connexion à Internet spécialement exploitée pour une relation B2B n'est pas soumise aux mêmes prescriptions que celles qui sont applicables selon DRR à l'accès à Internet pour les utilisateurs. Elle peut se trouver dans un centre de calcul ou chez un partenaire de l'AVS/AI.

4.3.4 Accès via Internet RPV ou à distance

La présente réglementation de domaine est applicable par analogie aux accès via Internet ou à distance. Etant donné qu'il s'agit là d'une question actuelle et souvent posée, elle est traitée explicitement ci-après.

- L'accès au réseau via Internet ou à distance représente toujours un accès depuis un domaine tiers.
- La réglementation de domaine applicable dépend du type de raccordement du domaine tiers: lorsque celui-ci est raccordé au réseau AVS/AI via un pont central, c'est la réglementation WIsB qui est applicable; lorsqu'il est relié au réseau d'un domaine partenaire, c'est la réglementation de l'organe d'exécution.

5 Voies de communication

Les voies de communication du domaine réseau AVS/AI sont soumises aux règles suivantes:

Communication entre domaines partenaires via le réseau AVS/AI

- Toute voie de communication entre domaines partenaires via le réseau AVS/AI doit d'abord être approuvée réciproquement par ceux-ci et mise en service par l'exploitant du réseau.
- Les responsables de la sécurité informatique des partenaires de communication sont compétents pour l'approbation réciproque.

Communication entre domaines partenaires et domaines tiers

1er cas: le domaine tiers est atteignable via un pont central du réseau AVS/AI:

- Toute voie de communication doit être définie dans le cadre de la réglementation pare-feu. Le responsable de la sécurité informatique du domaine partenaire est compétent pour cette définition.

2e cas: le domaine tiers est atteignable via le réseau AVS/AI via un domaine partenaire:

- La voie de communication doit d'abord être approuvée par les deux domaines partenaires A (souhaitant avoir accès au domaine tiers via B) et B (offrant à A un accès au domaine tiers) et mise en service par l'exploitant du réseau.
- Les responsables de la sécurité informatique des domaines partenaires A et B sont compétents pour l'approbation réciproque.

Communication entre deux domaines tiers via le réseau AVS/AI

- Ce type de communication n'est en principe pas admis.
- L'OFAS peut autoriser des exceptions dans certains cas.

6 Organisation

Se référer à DRR pour la description des différents rôles assumés dans le réseau AVS/AI.

Annexe 2

Instance de coordination et d'autorisation (ICA)

L'Office fédéral des assurances sociales (OFAS), en tant que fournisseur du réseau, assume les tâches de l'instance de coordination et d'autorisation (ICA).

Table des matières

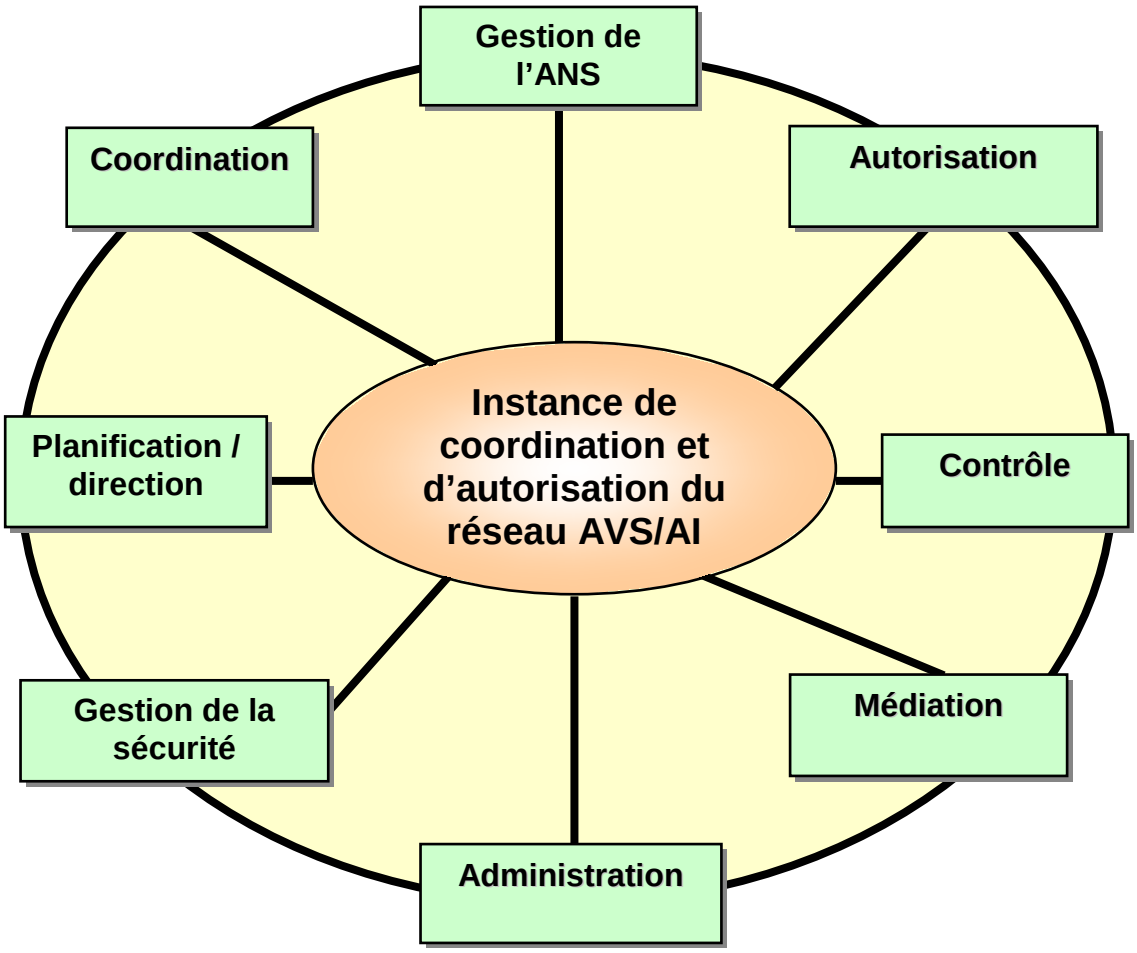
1. Tâches de l'ICA – schéma

2. Tâches de l'ICA –- domaines
   - coordination
   - autorisation
   - planification et direction
   - contrôle
   - direction de l'accord de niveau de service (ANS)
   - gestion de la sécurité
   - médiation
   - administration

3. Formulaire de demande
   - Procédure de contrôle et d'autorisation

1. Tâches de l'ICA – schéma

L'ICA est compétente pour les tâches suivantes:



2. Tâches de l'ICA – domaines

2.1 Coordination

- défense des intérêts des utilisateurs du réseau vis-à-vis de l'exploitant du réseau;
- coordination des modifications/adaptations de la stratégie de sécurité du réseau;
- Informations sur le réseau AVS/AI destinées
  – aux utilisateurs du réseau,
  – à l'exploitant du réseau,

  - aux organes internes à l'OFAS ou à d'autres (p. ex. CdC);
- défense des intérêts du réseau AVS/AI lors du développement ou de l'adaptation d'applications existantes ayant un impact sur le réseau;
- Mise à jour des directives relatives au réseau AVS/AI (DRR).

2.2 Autorisation

- nouveaux raccordements au réseau AVS/AI;
- raccordement de domaines tiers;
- modifications des connexions existantes ayant un impact financier (p. ex. une augmentation du débit, l'introduction d'un système redondant, etc.);
- communications entre domaines tiers via le réseau AVS/AI;
- réglementations de domaine de domaines partenaires s'ils exploitent leurs propres ponts vers des domaines tiers;
- raccordement de centres de calcul;
- raccordements externes à Internet.

2.3 Planification et direction

- planification à moyen terme pour le réseau AVS/AI (planification relative à l'extension du réseau) en collaboration avec l'exploitant;
- planification de nouveaux produits et services en collaboration avec l'exploitant du réseau;
- traitement actif des rapports livrés par l'exploitant du réseau concernant les besoins futurs ou les difficultés prévisibles à moyen terme;
- participation à des réunions de coordination avec l'exploitant du réseau.

2.4 Contrôle

- contrôle de la conformité aux règlements dans l'application de la réglementation de domaine par des utilisateurs du réseau et de son exploitant:
  – prescription d'audits,
  – prescription de mesures techniques et organisationnelles pour corriger les irrégularités en matière de sécurité,
  – surveillance de l'application;
- contrôle de la facture trimestrielle de l'exploitant du réseau;
- contrôle de la qualité et des services fournis par l'exploitant du réseau (selon les accords) sur la base de rapports réguliers.

2.5 Direction de l'accord de niveau de service (ANS)

- communication des contrats conclus à l'exploitant du réseau et surveillance de l'application en matière:
  – de raccordement de nouveaux emplacements,
  – de suppression ou de fusion d'emplacements,
  – d'adaptation d'emplacements existants (p. ex. une augmentation du débit),
  – d'introduction de nouveaux services ou de modification de services existants;

2.6 Gestion de la sécurité

- responsabilité, en tant que dépositaire de la réglementation de domaine, de sa mise à jour, sur proposition du fournisseur du réseau;
- organe de recours en cas d'urgence;
- définition, en collaboration avec l'exploitant du réseau, de scénarios d'urgence et des mesures à mettre en oeuvre;
- définition de mesures de sécurité pour le raccordement de CC/OAI qui, du point de vue du réseau, font partie d'une entreprise ou d'une association;

- réalisation ou commande auprès de tiers d'audits portant sur la sécurité du domaine partenaire;
- archivage de la réglementation de domaine et renforcement éventuel de certains pools à titre individuel.

2.7 Médiation

- organe de recours pour les utilisateurs du réseau et son exploitant en cas de réclamations et de problèmes;
- organe de recours en cas d'imprécisions ou de divergences portant sur l'application des directives relatives au réseau AVS/AI ou de la réglementation de domaine;
- destinataire des retours concernant le réseau AVS/AI.

2.8 Administration

- responsabilité dans l'emploi de systèmes et d'outils d'assistance (p. ex. commandes et mutations pour des raccordements à l'Intranet AVS/AI);
- mise à jour d'offres correspondantes sur l'Intranet AVS/AI;
- mise à disposition trimestrielle des prestations allant au-delà de l'offre de base aux utilisateurs du réseau;
- responsabilité de la traduction des documents importants en français.