

MINISTÈRE DE L'INTÉRIEUR,
DE L'OUTRE-MER,
DES COLLECTIVITÉS TERRITORIALES
ET DE L'IMMIGRATION

—
Secrétariat général
haut fonctionnaire de défense

—
Service du fonctionnaire de défense
—

**Circulaire du 9 mai 2012 relative à la sécurisation du cycle de vie
de la carte agent ministérielle**

NOR : IOCK1207281C

Pièces jointes :

- Glossaire;
- Imprimé de création, suppression et modification d'autorités d'AEL et ADR;
- Liste des visuels de la carte agent ministérielle;
- Document de référence technique de la puce sans contact RFID;
- Modèle de procès-verbal de destruction;
- Modèles d'organigramme fonctionnel type;
- Schémas des changements de situation d'agent.

Le préfet, secrétaire général, haut fonctionnaire de défense, aux destinataires in fine.

Dans le cadre du développement de l'administration électronique, le ministère de l'intérieur a décidé de doter l'ensemble de ses agents, administratifs et policiers, d'une carte professionnelle sécurisée.

Cette carte d'identité professionnelle aura aussi pour usage l'identification et l'authentification de l'agent pour les accès aux applications informatiques ainsi que de permettre le contrôle des accès aux bâtiments et sites. Elle permettra, à terme, de signer électroniquement un courrier et de chiffrer la transmission d'un message.

Elle inclut des possibilités d'utilisation particulière, par exemple en matière de paiement dans un restaurant administratif.

La gouvernance de ce dispositif nécessite une organisation et une gestion rigoureuses.

L'objectif de cette circulaire est de vous préciser les conditions de mise en œuvre de cette gouvernance et les responsabilités qui en découlent tout au long du cycle de vie de la carte agent.

MICHEL BART

DESTINATAIRES

Monsieur le directeur de cabinet du ministre de l'intérieur, à l'attention de :

Monsieur le chef du bureau du cabinet du ministre chargé de l'outre-mer;

Monsieur le chef du bureau des cabinets;

Monsieur le préfet, secrétaire général, haut fonctionnaire de défense, à l'attention de :

Monsieur le directeur de la modernisation et de l'action territoriale;

Monsieur le directeur des ressources humaines;

Monsieur le directeur de l'évaluation, de la performance et des affaires financières et immobilières;

Monsieur le directeur des systèmes d'information et de communication;

Monsieur le délégué à l'information et la communication;

Monsieur le chef du service de l'inspection générale de l'administration;

Monsieur le directeur général de la police nationale;

Monsieur le secrétaire général à l'immigration et à l'intégration;

Monsieur le directeur général des collectivités locales;

Monsieur le directeur général de la sécurité civile et de la gestion des crises;

Monsieur le directeur des libertés publiques et des affaires juridiques;

Monsieur le préfet de police, préfet de la zone de défense de Paris;

Monsieur le délégué général à l'outre-mer;

Mesdames et messieurs les préfets de zone de défense (métropole et DOM);

Mesdames et messieurs les préfets délégués pour la sécurité et la défense;
Mesdames et messieurs les préfets de région (métropole, et DOM);
Mesdames et messieurs les préfets de département (métropole et DOM).

POUR INFORMATION

Monsieur le directeur général de la gendarmerie nationale.

SOMMAIRE

I. – LA CARTE AGENT MINISTÉRIELLE

- A. – UNE CARTE PROFESSIONNELLE MULTISERVICES
- B. – UNE CARTE PROFESSIONNELLE SÉCURISÉE INSCRITE DANS UN CORPUS RÉGLEMENTAIRE ET NORMALISÉ
- C. – LES CARACTÉRISTIQUES TECHNIQUES DE LA CARTE AGENT
- D. – LES CERTIFICATS ÉLECTRONIQUES
- E. – LES USAGES LIÉS À LA CARTE AGENT MINISTÉRIELLE

II. – LES MODALITÉS D'ATTRIBUTION DE LA CARTE AGENT MINISTÉRIELLE

- A. – LES CATÉGORIES D'AGENTS CONCERNÉS
- B. – LES SOURCES D'INFORMATION, DIALOGUE -ARPEGE, À CONSULTER POUR L'ATTRIBUTION DE LA CARTE AGENT
- C. – LES CARTES AGENT DÉLIVRÉES
 - a) Les types de carte agent
 - b) Les différents visuels attachés à la carte agent

III. – LA GOUVERNANCE GÉNÉRALE DU DISPOSITIF CARTE AGENT MINISTÉRIELLE

- A. – L'ADMINISTRATION GÉNÉRALE DU SYSTÈME À L'ÉCHELON NATIONAL
- B. – LES ENTITÉS FONCTIONNELLES
 - a) Les autorités d'enregistrement (AEL)
 - b) Les autorités de délivrance (ADR)
 - c) Les dispositions communes aux autorités d'enregistrement et de délivrance
- C. – L'ORGANISATION DE LA GOUVERNANCE POUR CHAQUE ENTITÉ ADMINISTRATIVE
 - a) Les entités administratives responsables
 - b) L'organigramme fonctionnel
 - c) Le règlement d'application de l'entité

IV. – LES 6 ÉTAPES DU CYCLE DE VIE DE LA CARTE AGENT MINISTÉRIELLE

- A. – LA COMMANDE DE CARTE AGENT MINISTÉRIELLE
- B. – L'ACHEMINEMENT DE LA CARTE AGENT MINISTÉRIELLE
- C. – LA DÉLIVRANCE DE LA CARTE AGENT MINISTÉRIELLE
- D. – LES PROCÉDURES DE RENOUVELLEMENT
- E. – LE RETRAIT DE LA CARTE AGENT MINISTÉRIELLE
- F. – LA PERTE OU LE VOL DE LA CARTE AGENT MINISTÉRIELLE

V. – LA GESTION DES AUTORISATIONS LIÉE AUX MOUVEMENTS DES AGENTS

- A. – LA MOBILITÉ INTERNE À UNE DIRECTION OU SERVICE
- B. – LA MOBILITÉ ENTRE DIRECTIONS OU SERVICES DE L'ADMINISTRATION CENTRALE
- C. – LES MOBILITÉS ENTRE ADMINISTRATION CENTRALE ET DÉCONCENTRÉE

VI. – LA CHAÎNE DE SOUTIEN UTILISATEURS

ANNEXES

- Annexe I . – Glossaire
- Annexe II . – Imprimé de création, suppression et modification d'autorités d'AEL et ADR
- Annexe III . – Liste des visuels de la carte agent ministérielle
- Annexe IV . – Document de référence technique de la puce sans contact RFID
- Annexe V . – Modèle de procès-verbal de destruction
- Annexe VI . – Modèle d'organigramme fonctionnel type en administration centrale
- Annexe VII . – Modèle d'organigramme fonctionnel type en administration territoriale
- Annexe VIII . – Modèle d'organigramme fonctionnel type en direction de police (DDSP)
- Annexe IX . – Schéma de changement de situation sans renouvellement de carte agent
- Annexe X . – Schéma de changement de situation avec renouvellement de carte agent
- Annexe XI . – Schéma de changement de situation avec retrait de la carte agent

I. – LA CARTE AGENT MINISTÉRIELLE

A. – UNE CARTE PROFESSIONNELLE MULTISERVICES

À la fois carte professionnelle sécurisée, carte d'accès aux applications informatiques, carte d'accès aux bâtiments et aux sites et carte permettant la gestion de services rendus (restauration collective), la carte agent constitue un outil majeur de la sécurité des systèmes d'information.

La carte agent ministérielle est conçue comme un instrument d'identification et d'authentification de l'agent.

Les personnels de la gendarmerie nationale disposent, déjà, d'une carte professionnelle de même type, qui est totalement compatible et interopérable avec la carte agent ministérielle et les nouveaux systèmes d'information du ministère.

B. – UNE CARTE PROFESSIONNELLE SÉCURISÉE INSCRITE DANS UN CORPUS RÉGLEMENTAIRE ET NORMALISÉ

La carte agent ministérielle s'inscrit dans le contexte réglementaire du référentiel général de sécurité (RGS) dont les modalités sont fixées par le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 8, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Le référentiel général de sécurité (RGS) fixe les règles à respecter pour assurer la sécurité des informations échangées par voie électronique.

Il fonde les contraintes attachées à la demande, à la délivrance et à l'usage de la carte agent ministérielle.

C. – LES CARACTÉRISTIQUES TECHNIQUES DE LA CARTE AGENT

Afin de réduire la contrefaçon, la carte agent est composée de plusieurs éléments résultant d'un processus complexe de fabrication :

- Une puce à contact: assimilable à un coffre-fort contenant les certificats personnels d'authentification, de signature et de confidentialité. La lecture de la puce à contact de la carte agent ne peut s'opérer que par l'utilisation du lecteur «Xiring» validé par l'administration, à partir d'une station de travail.
- Une puce sans contact: permettant la gestion des accès aux bâtiments et aux sites.
- Une bande magnétique: permettant la gestion de services rendus (restauration collective...).
- Des sécurités sur la valeur faciale: dispositions s'inscrivant dans la lutte contre la fraude documentaire.

D. – LES CERTIFICATS ÉLECTRONIQUES

Les certificats électroniques contenus dans la carte agent sont des fichiers numériques permettant de valider le lien entre une signature électronique et son signataire.

Les certificats électroniques permettent l'identification et l'authentification du porteur de la carte agent.

Les certificats électroniques permettent d'instaurer la confiance dans les échanges électroniques, grâce à :

- l'identification formelle d'un utilisateur (authentification);
- l'assurance de l'identité de l'émetteur d'un message électronique (signature);
- la protection de la confidentialité des informations échangées (chiffrement);
- un renforcement de l'imputabilité des actions effectuées et l'accroissement de la traçabilité des accès aux applications les plus sensibles.

E. – LES USAGES LIÉS À LA CARTE AGENT

La carte agent peut être utilisée, dès à présent, pour contrôler les accès aux bâtiments ou aux sites équipés d'un système compatible.

Elle est également destinée à permettre l'accès aux applications informatiques :

- elle est déjà opérationnelle pour l'application du procès verbal électronique (PVe), de celle du plan de vidéo-protection de Paris (PVPP) et de l'application Chorus;
- à court terme de futures applications, en cours de développement, seront accessibles à partir de la carte agent: FAETON, AGDREF, AG1 bio;
- elle permettra également la signature électronique et le chiffrement de la transmission des données;
- son usage pourra être étendu à la gestion de services rendus, telle la restauration collective.

II. – LES MODALITÉS D'ATTRIBUTION DE LA CARTE AGENT MINISTÉRIELLE

L'attribution d'une carte agent ministérielle nécessite que la personne concernée soit identifiée comme disposant d'un statut ouvrant droit à sa délivrance.

Il est impératif de vérifier que l'agent ou la personne identifiée peut bénéficier d'une carte agent, comme carte professionnelle pour les agents du ministère, comme carte d'identification et d'authentification pour les autres.

Pour tous les agents, l'ensemble des informations indispensables à la vérification de leur statut en vue de la délivrance d'une carte agent, (état-civil, situation administrative ou statutaire, grade, affectation, statutaire, adresse du service), sont détenues dans un référentiel unique ministériel: le référentiel des identités et des organisations (RIO).

Cette vérification incombe, sur instruction de sa hiérarchie, au responsable RH.

A. – LES CATÉGORIES D'AGENTS CONCERNÉS

La carte agent ministérielle est attribuée à tout agent du ministère, ou personne collaborant aux missions du ministère, qui ont le statut requis pour cette délivrance:

- Les agents appartenant au ministère;
- Les agents en mobilité au ministère;
- La carte agent pourra être délivrée à des personnes identifiées comme collaborateurs occasionnels;
- Les personnels attachés fonctionnellement au ministère (notamment les sapeurs-pompiers de la DGSCGC, de la BSPP, les marins-pompiers de Marseille). Pour cette catégorie, la carte agent leur sera attribuée chaque fois que l'autorité hiérarchique dont ils dépendent juge indispensable la délivrance d'une carte agent pour l'exercice de leurs missions;
- Tout agent n'appartenant pas à un corps géré par le ministère mais employé et rémunéré par le ministère de l'intérieur, qu'il appartienne à la fonction publique d'État, territoriale, hospitalière ou de la ville de Paris;
- Les personnels de la réserve civile de la DGPN (population non fonctionnaire de la police).

B. – LES SOURCES D'INFORMATION À CONSULTER, DIALOGUE – ARPÈGE POUR L'ATTRIBUTION DE LA CARTE AGENT MINISTÉRIELLE

Le référentiel des identités et des organisations (RIO): ce dernier est alimenté automatiquement par deux systèmes d'information: Dialogue et Arpège.

En conséquence, les deux systèmes d'information Dialogue et Arpège doivent être impérativement actualisés en temps réel par les gestionnaires RH.

Le RIO n'est pas un système d'information de ressources humaines: il n'est pas autorisé de créer un dossier dans le RIO pour pallier le retard d'un dossier Dialogue ou Arpège.

Tout agent appartenant au ministère ou employé et rémunéré par le ministère de l'intérieur, qu'il appartienne à la fonction publique d'État, territoriale, hospitalière ou de la ville de Paris, doit faire l'objet d'un dossier dans un des deux systèmes d'information (Dialogue ou Arpège).

C'est le bureau de gestion RH de l'agent qui crée de toute pièce le dossier d'un nouvel arrivant ou qui en prend la gestion dans l'hypothèse de l'arrivée d'un agent en mobilité, dans Dialogue ou Arpège.

C. – LES CARTES AGENT DÉLIVRÉES

a) Les types de carte agent

- La carte permanente destinée aux personnels œuvrant au sein du ministère pour une période supérieure à six mois, et disposant d'un statut leur ouvrant droit à cette délivrance.
- La carte temporaire destinée:
 - Aux personnels travaillant au sein du ministère pour une courte durée.
 - Aux personnels du ministère ayant un besoin impératif de disposer d'une carte pour leur travail quotidien et ne disposant pas d'une carte permanente pour l'une des deux raisons suivantes: attente d'une carte permanente commandée ou carte invalidée.
 - Aux personnels permanents du ministère quittant le ministère dans un délai de six mois.

Les certificats électroniques de la carte temporaire sont valables pour une durée de 3 mois et pourront être renouvelés autant de fois que nécessaire.

Nota. – La carte temporaire ne peut pallier l'oubli par un agent de sa carte permanente à son domicile.

b) Les différents visuels attachés à la carte agent

Des dispositions ont trait aux règles concernant la personnalisation des cartes.

Onze visuels différents ont été définis pour figurer sur la valeur faciale de la carte agent.

A: police nationale: policier actif

B: police nationale: adjoint de sécurité

D: agent des administrations parisiennes: préfecture de police

K: agent de surveillance de Paris: préfecture de police

L'attribution de ces quatre visuels à la carte agent des personnels concernés est faite de manière automatique, en fonction des informations statutaires contenues dans le RIO et provenant pour la plupart des porteurs de Dialogue et d'Arpège. Pour les personnels techniques et scientifiques de la police, le choix du visuel B est fait manuellement par l'AEL.

F: corps préfectoral

I: hauts fonctionnaires

Seule l'AEL du bureau de gestion du corps préfectoral et des administrateurs civils (DMAT) peut attribuer ces deux visuels.

J: cabinet du ministre

Attribution réservée aux seules AEL des bureaux des cabinets des ministres.

G: inspection générale de l'administration

Attribution réservée à la seule AEL de l'IGA.

C: personnel administratif et technique

E: personnel temporaire

H: externe

Ces trois derniers visuels sont attribués par les AEL de chaque entité administrative concernée.

III. – LA GOUVERNANCE GÉNÉRALE DU DISPOSITIF CARTE AGENT MINISTÉRIELLE

A. – L'ADMINISTRATION GÉNÉRALE DU SYSTÈME À L'ÉCHELON NATIONAL

La sécurité globale du dispositif incombe au service du haut fonctionnaire de défense (SHFD).

Conformément au référentiel général de sécurité (RGS), l'initialisation du système à l'échelon central nécessite la mise en place de «secrets» qui ont été confiés à des porteurs. Ces «secrets» constituent des éléments clés de la sécurité du dispositif.

La section des réseaux sécurisés du SHFD assure la gestion nationale de ces «secrets».

Les agents à qui ont été confiés ces «secrets» doivent les conserver en lieu sûr dans une armoire forte et s'assurer régulièrement de leur présence. En cas de disparition, il y a lieu d'aviser sans délai le SHFD.

Annuellement, une revue de la présence de ces «secrets» sera organisée par le SHFD.

En cas de départ (mutation, retraite, départ du ministère, etc.), le porteur de «secret» (ou son responsable hiérarchique) doit aviser le SHFD au plus tôt, et le cas échéant, lui remettre ce «secret».

B. – LES ENTITÉS FONCTIONNELLES

Il existe des entités fonctionnelles:

– Autorité d'enregistrement nationale (AEN) et autorité d'enregistrement locale (AEL);

– Autorité de délivrance nationale (ADN) et autorité de délivrance de rattachement (ADR).

Sous l'appellation «autorité» d'enregistrement ou de délivrance on désigne une fonction. Les agents qui assurent cette fonction sont dénommés «opérateurs». On emploie indifféremment la terminologie AEL ou opérateur, et la terminologie ADR ou opérateur.

a) L'autorité d'enregistrement (AEL)

L'autorité d'enregistrement (AE) procède à la commande de la carte agent.

Il existe deux types d'AE:

– l'autorité d'enregistrement nationale ayant un périmètre de responsabilité général sur tout le ministère;

– l'autorité d'enregistrement locale (AEL) ayant un périmètre de responsabilité limité à quelques services, qui a pour principale mission de commander les cartes des agents qui font partie de son périmètre de responsabilité.

L'autorité d'enregistrement local (AEL) dispose d'un périmètre de responsabilité, une adresse mail en « nom-du-service-ael@interieur.gouv.fr » et procède à la commande des cartes.

Pour exécuter ses commandes de cartes agent, l'opérateur d'autorité d'enregistrement local se repose sur :

DIALOGUE : données d'organisation et données personnelles ;

RIO : référentiel des identités et de l'organisation.

Il doit en outre procéder à la vérification des points essentiels suivants :

- Fiabilité des informations dans Dialogue : conformité des informations essentielles ;
 - État civil ;
 - Grade/corps ;
 - Affectation en service d'affectation administrative (SAA) ou service d'affectation opérationnelle (SAO) ;
 - Adresse des unités : livraison des cartes – courrier code ;
 - Adresse mail en « prénom.nom@interieur.gouv.fr » ;
- Vérification dans le RIO : insertion de la photographie de l'agent.

b) L'autorité de délivrance

L'autorité de délivrance (AD) procède à la remise de la carte agent.

Il existe deux types d'AD :

- l'autorité de délivrance nationale ayant un périmètre de responsabilité général sur tout le ministère ;
- l'autorité de délivrance de rattachement (ADR) ayant un périmètre de responsabilité limité à quelques services et qui a pour principale mission de délivrer les cartes aux agents qui sont dans son périmètre de responsabilité.

L'autorité de délivrance de rattachement (ADR) dispose d'un périmètre de responsabilité défini, d'une adresse mail en « nom-du-service-adr@interieur.gouv.fr », et procède à la délivrance des cartes agent.

L'opérateur d'autorité de délivrance de rattachement (ADR) :

- Réceptionne les colis de cartes ;
- Réceptionne les cartes dans l'application CARTES ;
- Initialise dans la puce à contact les certificats personnels de l'agent ;
- Présente les certificats à l'agent ;
- Imprime et signe le récépissé de délivrance ;
- Fait saisir les questions/réponses secrètes par le porteur de la carte.

c) Dispositions communes aux autorités d'enregistrement et de délivrance

Les décisions de création, suppression et modification d'autorités (AEL ou ADR), ainsi que les décisions de désignation ou de cessation de fonction d'opérateur d'autorités seront portées sans délai à la connaissance des services du SHFD (voir imprimé joint en annexe).

Il en est de même de leur périmètre de responsabilité. Ces informations sont transmises aux services du haut fonctionnaire de défense qui assurent sur les applications RIO et CARTES la gestion des autorités et des opérateurs. Cette information sera transmise dans un premier temps par mail (à l'adresse : deploiement-carte-agents@interieur.gouv.fr), confirmé par courrier en utilisant l'imprimé joint en annexe.

Chaque autorité (AE/AD) disposera d'une adresse mail « correspondant carte agent ministérielle » (de type nom-du-service-ael/adr@interieur.gouv.fr) accessible à chaque opérateur RIO pour recevoir les messages émis automatiquement par l'application.

La gestion nationale des autorités et des opérateurs est effectuée, par mesure de sécurité, par des personnels différents. Fin 2012, un outil informatique de gestion automatique des AEL, ADR et des opérateurs sera mis à la disposition des directions et services.

Les AE et AD ne doivent pas, conformément aux annexes du référentiel général de sécurité approuvé par l'arrêté du Premier ministre du 6 mai 2010 (JO du 18 mai 2010), avoir de condamnation de justice en contradiction avec leurs attributions. Ces informations pourront être contrôlées par les services du haut fonctionnaire de défense ou des personnes dûment mandatées par le SHFD.

Préalablement à l'exercice des fonctions d'AEL ou d'ADR, l'opérateur devra avoir reçu une formation organisée soit par la DRF Paris – Île de France ou le SERFOR pour la préfecture de police, la DRCPN pour la DGPN ou la SDRF pour tous les autres agents du ministère. Ce n'est qu'au terme de cette formation que le périmètre de chaque autorité sera arrêté et ouvert par le SHFD en conformité du périmètre défini par le service demandeur.

Même si une documentation est en ligne sur le portail carte agent, des sessions de formation devront obligatoirement être organisées et suivies afin de respecter les prescriptions du RGS. Il appartient à chaque entité administrative, nationale et locale, par la tenue et le suivi d'un tableau de bord, d'anticiper les départs des opérateurs afin d'organiser ces formations en lien avec la DSIC au niveau central.

C. – L'ORGANISATION DE LA GOUVERNANCE POUR CHAQUE ENTITÉ ADMINISTRATIVE

La carte agent sera délivrée à tous les agents du ministère avant la fin de l'année 2013. Les personnes identifiées comme collaborateurs occasionnels pourront aussi en bénéficier dans les conditions rappelées ci-dessus. Toutes les entités administratives au sein du ministère sont impliquées dans le dispositif carte agent.

a) Les entités administratives responsables

Ces entités sont définies par les responsables des différentes grandes missions du ministère, administration centrale, administration territoriale, police nationale, sécurité civile et en fonction de leurs instructions.

Est considérée comme périmètre d'autorité, soit pour la commande ou la délivrance de la carte agent ministérielle «une entité administrative homogène».

Par exemple, il peut s'agir d'une direction d'administration centrale, d'une préfecture, d'une sous-préfecture, d'une direction locale de police (DDSP, DDPAF), d'un SGAP, d'un service, de la préfecture de police, d'une agence du ministère, etc.

Ces entités administratives responsables identifiées sont en charge de la gouvernance locale du dispositif de commande et délivrance de la carte agent et de la gestion de son cycle de vie.

b) L'organigramme fonctionnel

Il doit être impérativement élaboré, par chaque entité administrative, un organigramme fonctionnel détaillant la chaîne des procédures de délivrance, retrait et de gestion des cartes agent.

Il identifiera nominativement les autorités qui seront en charge de la mise en œuvre du dispositif pour cette entité.

L'implication de tout acteur au sein d'une chaîne organisationnelle au sein de l'entité administrative doit être construite dans le détail tenant compte des spécificités propres à chaque entité administrative et en respectant les lignes directrices fixées dans la présente circulaire.

c) Le règlement d'application de l'entité

Dans le règlement d'application pour l'entité, sera décrit le rôle des autorités responsables des diverses autorisations (commande, délivrance, accès aux applications et bâtiments, gestion du cycle de vie de la carte). Ces dispositions sont indispensables pour prévenir tout usage frauduleux de la carte agent susceptible d'entraîner des procédures disciplinaires, contentieuses ou, le cas échéant, pénales.

Devront être également précisément identifiées les fonctions de chaque intervenant dans la chaîne organisationnelle définie et mise en place.

d) Dispositions diverses

Chaque entité administrative fixe le périmètre de responsabilité de son AEL et de son ADR. Au sein de chaque périmètre, des agents sont désignés comme opérateur soit pour l'autorité d'enregistrement locale, soit pour l'autorité de délivrance de rattachement. Un opérateur ne peut pas être opérateur de plusieurs autorités.

Chaque entité administrative du ministère (hormis pour l'administration centrale) arrête le nombre d'AEL et d'ADR dont elle souhaite disposer. Le SSMI est ADR pour tous les sites franciliens de l'administration centrale. Il doit être désigné un nombre suffisant d'opérateurs pour assurer la continuité du service public et pallier les éventuelles absences.

Les décisions de création, suppression et modification d'autorités (AEL ou ADR) ainsi que les décisions de désignation ou de cessation de fonction d'opérateur d'autorités seront portées sans délai à la connaissance des services du SHFD. Il en est de même de leur périmètre de responsabilité, cette information sera transmise dans un premier temps par mail (à l'adresse: deploiement-carte-agents@interieur.gouv.fr), confirmé par courrier en utilisant l'imprimé joint en annexe.

IV. – LES 6 ÉTAPES DU CYCLE DE VIE DE LA CARTE AGENT MINISTÉRIELLE

A. – LA COMMANDE DE CARTE AGENT MINISTÉRIELLE

Pour tout personnel déjà affecté ou entrant dans le ministère, la commande sera réalisée par l'opérateur AEL de l'entité administrative, qui vérifiera au préalable les éléments du dossier de l'agent qui doit en bénéficier. L'opérateur AEL devra s'assurer de l'exactitude des données saisies dans Dialogue et présentes dans le RIO.

Dans l'hypothèse d'informations erronées ou insuffisantes interdisant une commande de la carte, l'AEL devra saisir le gestionnaire RH de l'agent pour mise à jour de son dossier dans Dialogue. La mise à jour finale du RIO incombe à l'AEL. En aucun cas il ne pourra être créé ex-nihilo un dossier dans le RIO sans création du dossier Dialogue ou mise à jour des données, sauf des cas particuliers strictement limités, après autorisation de la hiérarchie.

La mise à jour permanente et immédiate de Dialogue et d'Arpège conditionne la commande des cartes. Les gestionnaires RH ont cette responsabilité sous le contrôle de l'autorité autorisant les commandes de cartes.

Une commande de carte ne doit pas intervenir s'il est connu que l'agent est en instance de mutation ou de départ du ministère. L'opérateur AEL doit vérifier ces hypothèses auprès du gestionnaire RH.

Pour les agents disposant d'un dossier dans le RIO, quelques données peuvent être modifiées: il s'agit de la photo, de l'adresse de messagerie (au format « prenom.nom@interieur.gouv.fr » ou « prenom.nom@nomdudépartement.gouv.fr ») et l'affectation RIO.

Pour les personnels présents temporairement au sein du ministère (prestataires extérieurs, vacataires), un opérateur AEL devra créer le dossier dans le RIO sur instruction de sa hiérarchie.

Des informations essentielles sont à vérifier par l'AEL :

- l'état civil de la personne: nom, prénoms, date de naissance qui doivent être conformes à l'état-civil, le système carte agent utilise le nom d'usage;
- le grade et l'adresse de messagerie électronique au format « prenom.nom@interieur.gouv.fr » ou « prenom.nom@nomdudépartement.gouv.fr »; si l'agent n'en possède pas, cette zone ne doit pas être renseignée;
- l'affectation: le système utilisé, le service d'affectation opérationnelle;
- l'adresse du service: elle est utilisée pour l'envoi à l'agent de la lettre contenant son code d'activation.

B. – L'ACHEMINEMENT DE LA CARTE AGENT MINISTÉRIELLE

Dès sa validation, la commande de carte est transmise à l'imprimerie nationale pour être fabriquée et éditée. L'envoi des fichiers de demandes est réalisé tous les lundis et jeudis avant 6 heures du matin. Une fois produites, les cartes sont envoyées au destinataire *via* l'autorité de délivrance de rattachement (ADR) à J + 4 jours, (J étant le jour de réception du fichier).

Les cartes sont livrées aux ADR à J + 5 pour la métropole, à J + 6 pour la Corse et pour les DOM-COM de J + 8 à J + 12.

Les opérateurs ADR ont connaissance par courriel envoyé automatiquement par l'application CARTES de l'expédition d'un colis de cartes à leur attention. Les opérateurs ADR doivent, aussitôt la réception du colis de cartes, vérifier la présence des cartes produites par l'Imprimerie nationale en pratiquant l'opération de « réception » dans l'application CARTES. Toute absence de réception du colis dans un délai de 3 jours après la date de réception du courriel doit être signalée à l'adresse deploiement-carte-agents@interieur.gouv.fr.

Un courrier contenant le code d'activation de la carte est adressé, par courrier postal à l'agent, à l'adresse de son service d'affectation opérationnelle (SAO) à J + 6 jours. Le délai d'acheminement de ce courrier est de 4 à 8 jours, pour la métropole et l'outre-mer.

À l'arrivée de ce courrier au sein du service, il ne doit pas être ouvert par une tierce personne, même par les secrétariats d'autorité. Il doit être remis au plus vite au destinataire et non à un opérateur ADR. En l'absence du destinataire, il est conservé dans un endroit sûr au sein de son service.

Si une carte est livrée dans une unité où le porteur n'est plus présent, les mesures suivantes sont à appliquer :

- l'agent a été muté dans une autre unité du ministère ou en dehors du ministère. Un message est envoyé à l'adresse deploiement-carte-agents@interieur.gouv.fr en précisant les noms, prénoms et numéro RIO de l'agent. En retour, il sera communiqué à l'ADR et à l'AEL les nouvelles coordonnées du porteur pour faire suivre la lettre contenant le code d'activation et les nouvelles coordonnées de l'ADR pour envoyer par pli recommandé la carte de l'agent;
- l'agent a quitté définitivement la fonction publique: la carte est retirée du service par l'ADR, puis détruite.

C. – LA DÉLIVRANCE DE LA CARTE AGENT MINISTÉRIELLE

La délivrance de la carte est effectuée par l'ADR (SSMI pour les directions centrales situées en Île-de-France).

Le titulaire lors de la délivrance de sa carte l'active en saisissant le code d'activation reçu par courrier personnel, puis il la protège en saisissant des codes PIN personnels (PIN global à 4 chiffres et PIN de signature à 6 chiffres).

L'ADR teste aussitôt son bon fonctionnement en utilisant le logiciel dénommé «Middleware IAE ECC» explorateur de carte pour montrer au porteur les certificats insérés dans la puce. Le porteur doit impérativement *in fine* de la procédure de délivrance se connecter au portail agent pour saisir ses questions/réponses secrètes.

Cette dernière opération est obligatoire, car dans l'hypothèse de 3 saisies erronées d'un code PIN, la carte est bloquée et en l'absence de questions/réponses secrètes, il est impossible de la débloquent. La carte est alors inutilisable définitivement et retirée du service.

Le porteur et l'ADR signent à l'issue de cette procédure le récépissé de prise en compte et d'engagement de responsabilité. Un exemplaire est remis au porteur et un autre archivé dans son dossier personnel (transmis au service RH par l'ADR).

Concernant la réserve civile de la DGPN (population non fonctionnaire de la police), la délivrance se fera également dans les mêmes conditions, dans les secrétariats généraux pour l'administration de la police SGAP.

L'autorité de délivrance de rattachement (ADR) doit disposer d'une adresse mail en «nom-du-service-adr@interieur.gouv.fr».

D. – LES PROCÉDURES DE RENOUVELLEMENT

a) Renouvellement de la carte agent

En principe, le remplacement de la carte intervient tous les 6 ans, il est initié par l'AEL, prévenu par l'application.

Le renouvellement a lieu aussi en cas de changement :

- de situation ou affectation qui nécessite une modification du visuel de la carte de l'agent ;
- de l'état civil du porteur ;
- du corps pour tous les agents ;
- de grade pour l'ensemble des fonctionnaires.

La première carte devra être restituée à l'ADR au moment de l'activation de la nouvelle carte. Elle sera détruite par celui-ci en présence du porteur, dans la mesure du possible, avec établissement d'un procès-verbal de destruction classé au dossier RH de l'intéressé (voir modèle de procès-verbal de destruction joint en annexe).

Dans l'hypothèse du renouvellement à échéance des 6 ans, l'opérateur AEL sera avisé par l'application CARTES par la mention : état : carte à renouveler.

Le renouvellement sera aussi effectué sur requête en cas de perte, vol, détérioration de la carte ou d'impossibilité de rechargement des certificats électroniques.

Ces renouvellements permettent d'actualiser, le cas échéant, les données personnelles de l'agent, notamment la photographie.

Dans l'hypothèse du renouvellement sur demande de l'agent par la voie hiérarchique (cas de perte, vol, détérioration ou impossibilité de recharger les certificats électroniques), en ce cas l'opérateur AEL devra s'assurer que tous les éléments du dossier du demandeur sont toujours valides. Il incombe à chaque entité administrative de définir les modalités des pièces à fournir en cas de perte ou de vol.

b) Renouvellement des certificats électroniques

Le renouvellement des certificats électroniques peut intervenir dans trois cas :

- les certificats arrivent en fin de validité (les certificats ont une durée de validité de 3 ans) ;
- mutation du porteur susceptible d'entraîner un changement de l'autorité de certification des certificats. Le ministère met en œuvre trois autorités de certification correspondant à 3 domaines : police nationale, administration centrale et administration territoriale. Une mutation d'un service inclus dans un domaine vers un service d'un autre domaine entraîne un renouvellement de certificat ;
- changement d'adresse mail du porteur.

L'opération est effectuée par l'AEL avisé par l'application CARTES (état : certificats à renouveler).

Le porteur est avisé par courriel s'il dispose d'une adresse de messagerie en «prenom.nom@interieur.gouv.fr» ou «prenom.nom@nomdudepartement.gouv.fr» ou par l'opérateur AEL s'il n'en dispose pas.

Le porteur peut après cette action de l'AEL se connecter au portail agent (<https://portail-agent-cartes.mi/>) pour effectuer le renouvellement de ses certificats. Deux renouvellements successifs de certificats par le portail ne sont pas possibles. Après un renouvellement par le portail, le renouvellement suivant doit être effectué auprès d'une ADR. L'opération est également possible auprès d'une ADR.

c) Dispositions diverses concernant les certificats électroniques

Lorsque le bénéficiaire quitte temporairement son poste au sein du ministère (congé parental ou congé formation de longue durée), les codes et autorisations d'accès aux applications seront désactivés, par l'administrateur des applications, sans invalidation des certificats de la carte.

S'agissant du congé maternité, congé de longue maladie et congé de longue durée, les agents conservent leur carte.

Pour toute durée d'absence supérieure à 6 mois, l'autorité hiérarchique s'assurera de l'invalidation des certificats de la carte.

Nota. – En attendant la mise en œuvre opérationnelle de l'invalidation des certificats, il y a lieu de procéder à la désactivation des autorisations d'accès aux applications.

En cas de détachement ou de mise à disposition sortante, tous les agents conserveront leur carte dans la mesure où elle est une carte professionnelle sécurisée. Les codes et autorisations d'accès aux applications seront désactivés, sans invalidation des certificats de la carte, sur décision de l'autorité hiérarchique.

E. – LE RETRAIT DE LA CARTE AGENT MINISTÉRIELLE

a) Retrait définitif de la carte agent

La carte agent est retirée en cas de départ définitif de l'agent du ministère : démission, exclusion définitive, révocation, retraite, décès. Elle est également retirée en cas de suspension d'activité de l'agent.

Propriété de l'État, elle doit être remise par le titulaire soit à l'autorité hiérarchique, soit à un opérateur AEL ou ADR avant le départ.

Elle devra être immédiatement invalidée par l'ADR et sera détruite avec établissement d'un procès-verbal de destruction qui sera classé au dossier de l'intéressé.

En cas de placement en disponibilité, tous les agents doivent rendre leur carte.

Elle pourra être retirée par l'autorité hiérarchique en cas de sanction disciplinaire le justifiant. Elle sera immédiatement invalidée par l'ADR avant le départ de l'agent, puis remise soit à l'autorité hiérarchique, soit à son AEL ou ADR.

b) Retrait temporaire de la carte agent

La carte agent sera retirée le temps d'une exclusion temporaire prononcée à l'encontre de l'agent ou suite à une suspension de fonction.

Dans le cas d'une exclusion temporaire, les codes et autorisations d'accès aux applications seront désactivés sans invalidation de la carte.

Les réservistes non retraités de la police nationale doivent remettre leur carte à leur service d'emploi entre deux périodes d'emploi. Leurs codes et autorisations d'accès aux applications doivent être désactivés sans invalidation de la carte.

Dans ces deux dernières situations, la carte sera insérée dans une enveloppe scellée, sur laquelle le porteur apposera sa signature de manière à garantir, lors de la récupération de la carte, que celle-ci n'a pas été manipulée à son insu.

Les codes PIN (4 chiffres et 6 chiffres), qui protègent l'utilisation de la carte, sont personnels au bénéficiaire de la carte. Il ne peut pas être exigé du bénéficiaire de la carte que celui-ci dévoile ses codes PIN.

F. – LA PERTE OU LE VOL DE LA CARTE AGENT MINISTÉRIELLE

Une carte perdue ou volée doit être signalée immédiatement à l'autorité hiérarchique, pour être invalidée dans les plus brefs délais :

- en heures et jours ouvrés, le porteur de la carte agent s'adresse en priorité à un opérateur ADR qui informera aussitôt l'AEL et l'autorité hiérarchique. L'opération d'invalidation incombe à l'ADR ;
- en heures et jours non ouvrés, le porteur de la carte agent appellera le centre de service national (CSN), au 0800 20 72 77 ou + 33 800 20 72 77 pour l'outre-mer ;
- le porteur de la carte agent est identifié par le centre de service national (CSN) grâce à la réponse à une des questions secrètes du porteur que celui-ci a formulé lors de l'activation initiale de sa carte ;

- l'opérateur CSN saisit la réponse du porteur de la carte et la valide. La réponse est vérifiée. Si elle est correcte, l'invalidation est rendue possible. La carte est invalidée par l'opérateur du CSN. Un message confirmant cette invalidation est adressé au porteur, à son AEL et à son ADR ;
- dans le cas d'une réponse incorrecte à la question posée, l'invalidation de la carte ne peut pas être opérée par le CSN, elle devra être invalidée par un ADR.

Le traitement administratif de la perte ou du vol de la carte continue à suivre les dispositions actuellement en vigueur pour chaque catégorie d'agents.

Il est en revanche rappelé qu'eu égard aux droits attachés à cette carte, toute perte ou vol doit immédiatement être déclaré, dès que l'agent en a connaissance, afin d'empêcher l'utilisation frauduleuse de la carte.

Ce défaut de déclaration immédiate peut faire l'objet d'une sanction.

L'autorité informée de la perte ou du vol de la carte doit aviser immédiatement, par tous moyens, le responsable de la gestion des accès informatiques et bâtimentaires, aux fins de neutralisation des codes et autorisations d'accès.

V. – LA GESTION DES AUTORISATIONS LIÉE AUX MOUVEMENTS DES AGENTS

Dans tous les cas de mouvements de personnels, les modifications dans Dialogue sont effectuées par le gestionnaire RH dans les meilleurs délais. Le chef de service ou le référent RH avisera immédiatement des modifications par message l'AEL qui contactera le gestionnaire des accès aux applications et le service responsable de la sécurité et des accès aux bâtiments (SSMI pour les sites franciliens de l'administration centrale).

A. – LA MOBILITÉ INTERNE À UNE DIRECTION OU SERVICE

En ce qui concerne un changement de poste consécutif à une mobilité interne au sein d'un même service d'affectation opérationnelle ou administrative, il n'y aura pas de modification des certificats électroniques par l'autorité de certification émettrice du certificat.

La modification de l'affectation dans Dialogue sera effectuée par le gestionnaire RH.

Le référent RH ou le chef de service informera dans les meilleurs délais les services gestionnaires des autorisations aux nouvelles applications ainsi que les services concernés par la sécurité des accès aux bâtiments.

Il est précisé, en cas de modifications sur les autorisations d'accès aux applications que l'accès aux nouvelles applications ne peut être opéré que si les autorisations d'accès aux anciennes applications ont été fermées.

Ces opérations se feront sans délai sous forme d'un message visé par l'autorité hiérarchique et selon un schéma organisationnel propre à chaque entité administrative.

B. – LA MOBILITÉ ENTRE DIRECTIONS OU SERVICES DE L'ADMINISTRATION CENTRALE

En administration centrale, la modification de l'affectation de l'agent dans Dialogue par le gestionnaire RH sera effectuée dans les meilleurs délais.

L'AEL d'origine sera informé par le référent RH de départ de la mobilité de l'agent.

Le référent RH de départ ou le chef de service informera les services gestionnaires des autorisations d'accès aux applications et d'accès aux sites et bâtiments, de la mobilité de l'agent, en leur précisant les modifications éventuelles de celles-ci. Ces opérations s'effectueront conformément à la procédure du schéma organisationnel de l'entité administrative.

Le service concerné (SSMI) par la sécurité des accès aux bâtiments et sites doit être informé de la mobilité de l'agent par le référent RH de départ, conformément à la procédure du schéma organisationnel de l'entité administrative.

Le référent RH d'arrivée, à réception de l'arrêté d'affectation de l'agent par le gestionnaire RH, devra informer l'AEL d'arrivée ainsi que le chef de service. Il demandera, conformément aux instructions de la hiérarchie, aux services concernés l'ouverture des autorisations aux applications et au SSMI les droits d'accès aux bâtiments et sites.

Ces démarches se feront par message selon des procédures et un schéma organisationnel propres à chaque entité administrative.

Ces opérations se feront sans délai et après aval de la hiérarchie. Les référents RH devront être mobilisés pour mener celles-ci à bien.

C. – LES MOBILITÉS ENTRE ADMINISTRATION CENTRALE ET DÉCONCENTRÉE

En ce qui concerne le périmètre déconcentré, après modification de l'affectation dans Dialogue par le gestionnaire RH de l'administration centrale ou déconcentrée, le référent RH de départ avise l'AEL du départ de l'agent et veille à la fermeture des autorisations d'accès aux applications et aux accès des bâtiments.

Le référent RH d'arrivée informera par message l'AEL d'arrivée, ainsi que le chef de service d'affectation de l'agent.

IL veillera, comme indiqué dans le paragraphe *supra*, à l'ouverture des autorisations d'accès aux nouvelles applications et aux bâtiments.

Ces opérations devront être effectuées sans retard avec la mobilisation des référents RH.

Ces démarches se feront par message selon les procédures du schéma organisationnel propres à chaque entité administrative.

Lorsque la mobilité s'effectue hors du périmètre d'administration centrale vers un service déconcentré, l'agent conserve sa carte agent si son profil RH ne change pas. Il y a modification des certificats électroniques par l'autorité de certification compétente d'arrivée.

Les modifications d'affectation sont faites dans Dialogue sans délai par le gestionnaire RH de départ.

VI. – LA CHAÎNE DE SOUTIEN UTILISATEURS

Tous les porteurs de carte agent ministérielle ayant accès à l'Intranet du ministère peuvent accéder au portail carte agent ministériel à l'adresse suivante : <https://portail-agent-cartes.mi>.

Après s'être identifié et authentifié à l'aide de sa carte agent, le porteur peut :

- gérer ses questions/réponses secrètes;
- charger ses certificats sans avoir à se rendre devant une ADR (cas du renouvellement suite à dépassement de validité d'un certificat sans changement des données personnelles);
- débloquer le(s) code(s) PIN (global, signature);
- changer un des codes PIN de sa carte.

A N N E X E I

GLOSSAIRE

AEL : autorité d'enregistrement locale – personne responsable de la demande des cartes agent ministérielles pour toutes les personnes d'une structure.

ADR : autorité de délivrance de rattachement – personne responsable de la délivrance des cartes agent ministérielles pour toutes les personnes d'un structure.

Authentification : action qui consiste à vérifier l'identité d'une personne et autoriser l'accès de celle-ci à des ressources (systèmes, réseaux, applications).

Arpège : système d'information source des ressources humaines de la préfecture de police.

CARTES : logiciel « Centralisation pour l'Administration et la Remise des cartes Électroniques Sécurisées » permettant la commande et la remise des cartes agent ministérielles.

Certificat électronique : le certificat électronique (aussi appelé certificat numérique) est un fichier numérique permettant de s'identifier, de chiffrer et de signer électroniquement des documents.

Chiffrement : le chiffrement, aussi appelé cryptage, est le procédé grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de déchiffrement

Code PIN : il existe un code porteur global (code PIN global) et un code porteur de signature (code PIN de signature) dont la saisie peut être demandée pour l'accès aux applications.

CSN : centre de service national de la DSIC.

Dialogue : système d'information source des ressources humaines du ministère.

Gestionnaire RH : personne habilitée à modifier les données administratives dans Dialogue et Arpège.

Identification : action qui consiste à connaître l'identité d'une personne.

Invalidation : action qui consiste à rendre inactif des fonctionnalités de la carte agent.

Opérateurs AEL : opérateurs qui ont comme mission principale de commander les cartes pour les agents qui font partie de leur périmètre sous la responsabilité de l'AEL.

Opérateurs ADR : opérateurs qui ont comme mission principale de délivrer les cartes pour les agents qui font partie de leur périmètre sous la responsabilité de l'ADR.

Portail carte agent : portail intranet permettant aux agents d'accéder à un certain nombre d'informations relatives à la carte agent.

Puce avec contact : la puce avec contact est une puce visible sur la carte qui contient les certificats d'authentification, de signature et de confidentialité du porteur.

Puce sans contact (RFID) : la puce sans contact est non visible sur la carte, faisant partie intégrante de la carte. La radio-identification plus souvent désignée par le sigle RFID (*Radio Frequency Identification*) est une méthode pour mémoriser et récupérer des données à distance. Ces puces électroniques sont constituées d'une antenne et d'un microprocesseur. On peut y stocker des d'informations, et contrairement aux cartes à puces avec contact, on peut lire ces informations et les mettre à jour sans insérer la puce dans un lecteur.

PVe : Procès-verbal électronique.

PVPP : Plan de vidéo protection de Paris.

Questions/réponses secrètes : dispositif d'authentification secondaire d'un agent après un blocage du code PIN d'authentification.

RIO : référentiel des identités et des organisations – base de données élaborée à partir d'éléments de ressources humaines recensant tous les agents du ministère de l'intérieur et leur numéro unique permettant, entre autres, la commande de carte.

Référent RH : le référent RH est l'interlocuteur privilégié des directions de l'administration centrale ou des structures administratives (services territorialement compétents) avec les bureaux de gestion des personnels et les agents.

Il exerce les missions suivantes : gestion administrative des agents affectés dans le service, notifications des divers actes de gestion, suivi des effectifs, position statutaire, primes, rémunérations, etc.

Référentiel général de sécurité (RGS) : le référentiel général de sécurité définit un ensemble de règles de sécurité qui s'imposent aux autorités administratives dans la sécurisation de leurs systèmes d'information. Il propose des bonnes pratiques en matière de sécurité des systèmes d'information que les autorités administratives sont libres d'appliquer. Le RGS est élaboré conformément à l'article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux

échanges électroniques entre les usagers et les autorités administratives ainsi qu'entre les autorités administratives. Il fixe les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique.

Invalidation de certificat : action demandée par une autorité de certification ou une autorité administrative, par le porteur de certificat ou son autorité de sécurité et dont le résultat est la suppression de la caution de l'autorité de certification sur un certificat donné, avant la fin de sa période de validité. Cette action peut être la conséquence de différents types d'évènements tels que la compromission d'une clé, le changement d'informations contenues dans un certificat, etc.

SHFD : service du haut fonctionnaire de défense.

Signature électronique : il s'agit d'une combinaison chiffrée qui permet d'authentifier l'émetteur d'un message. D'un point de vue réglementaire, la signature électronique consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garanti.

SSMI : service de sécurité du ministère de l'intérieur qui est ADR pour les administrations centrales du ministère.

ANNEXE II

CRÉATION – SUPPRESSION – MODIFICATION
D'AUTORITÉS AEL ET ADR
«Carte agent ministérielle»

Direction / Service (*dénomination et adresse*) :

Date :

.....

Document à envoyer par courriel (à l'adresse suivante: et à l'adresse du SHFD – place Beauvau)

I. – AEL

1.1 – Création

NOM de l'autorité	CODE DIALOGUE du service responsable de cette autorité	CODE DIALOGUE des services devant être inclus dans le périmètre de l'autorité (1)	DATE de création souhaitée	ADRESSE MAIL DE L'AUTORITÉ Nom_du_service-ael@interieur.gouv.fr	OBSERVATIONS

1.2. Suppression

NOM de l'autorité	CODE DIALOGUE du service responsable de cette autorité	DATE de suppression souhaitée	OBSERVATIONS

1.3. Modification (préciser dans le tableau ce qui doit être modifié)

NOM de l'autorité	CODE DIALOGUE du service responsable de cette autorité	CODE DIALOGUE des services devant être inclus dans le périmètre de l'autorité (2)	DATE de modification souhaitée	ADRESSE MAIL DE L'AUTORITÉ Nom_du_service-ael@interieur.gouv.fr	OBSERVATIONS

II. – ADR

2.1. Création

NOM de l'autorité	CODE DIALOGUE du service responsable de cette autorité	CODE DIALOGUE des services devant être inclus dans le périmètre de l'autorité (3)	DATE de création souhaitée	ADRESSE MAIL DE L'AUTORITÉ Nom_du_service-adr@interieur.gouv.fr	OBSERVATIONS

2.2. Suppression

(utilisation du même tableau que 2.1)

(1) Si l'autorité couvre une entité complète, préciser laquelle, sans énumérer tous les services (exemples: préfecture XX, DDSPXX).

(2) Si l'autorité couvre une entité complète, préciser laquelle, sans énumérer tous les services (exemples: préfecture XX, DDSPXX).

(3) Si l'autorité couvre une entité complète, préciser laquelle, sans énumérer tous les services (exemples: préfecture XX, DDSPXX).

ANNEXE III

LES VISUELS DE LA CARTE AGENT MINISTÉRIELLE

- A** Policier actif ou réserviste
- B** Personnels techniques et scientifiques de la police nationale/adjointes de sécurité
- C** Personnels administratifs et techniques
- D** Agent des administrations parisiennes (préfecture de police)
- E** Temporaire
- F** Corps préfectoral
- G** IGA
- H** Externes
- I** Hauts fonctionnaires
- J** Cabinet du ministre
- K** Agent de surveillance de Paris (préfecture de police)

ANNEXE IV

LES ACCÈS AUX SITES ET BÂTIMENTS

S'agissant de l'accès aux bâtiments, le document de référence technique de la puce sans contact (RFID) a été finalisé et validé le 31 janvier 2012. Il a été transmis sous le n° 12-02590-D du 17 février 2012. Ce document est disponible sur le site intranet du ministère de l'intérieur, rubrique carte agent, onglet SHFD.

Il devra être annexé au cahier des clauses techniques particulières lors de toutes les démarches d'appels d'offres des travaux de sécurisation des bâtiments (document joint).

Il sera fait référence à la circulaire NOR/INT/SG/HFDAIOCA 1208138 du 19 mars 2012 relative à la protection des préfetures, des sous-préfetures et de leurs personnels.

ANNEXE V

PROCÈS-VERBAL DE DESTRUCTION
« Carte agent ministérielle »

- Direction/Service (*dénomination et adresse*):
- NOM et prénom du demandeur:
- NOM et prénom du titulaire:
- Service d'affectation opérationnelle du titulaire:
- Service d'affectation administrative du titulaire:

Date:

Signature:

Type de carte (visuel):

Libellé:

MOTIF DE LA DESTRUCTION:		
NUMÉRO DE LA CARTE (indiqué au verso)	VISUEL	NOM ET PRÉNOM DU TITULAIRE

PARTIE RÉSERVÉE À LA DESTRUCTION

Nom et prénom de l'opérateur	
Signature	

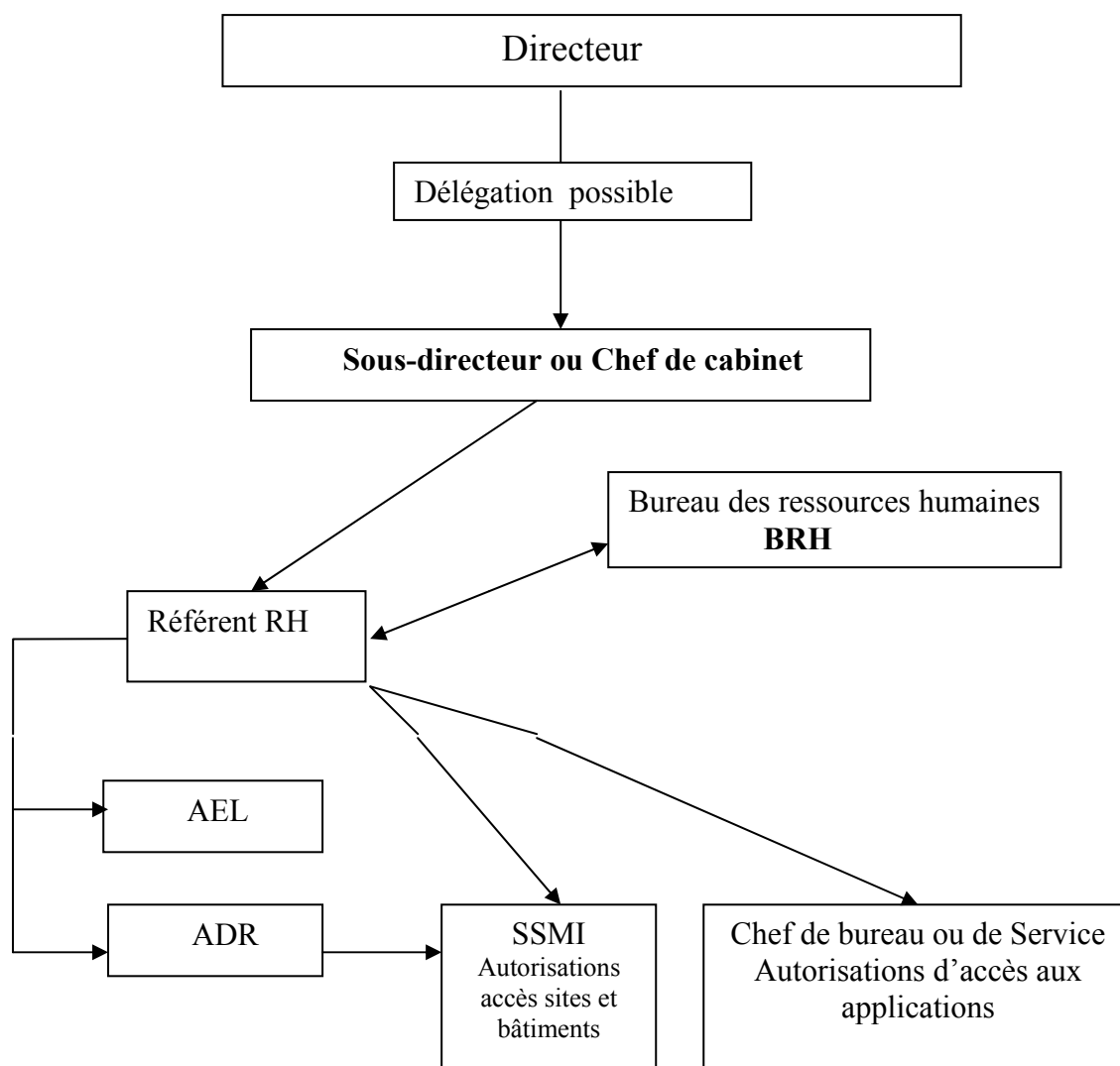
Nom et prénom du vérificateur	
Signature	

Destinataires :

- SHFD (par courrier, adresse mail: deploiement-carte-agents@interieur.gouv.fr);
- Titulaire de la carte;
- Supérieur hiérarchique;
- Demandeur, opérateur, vérificateur;
- Copie dossier RH titulaire.

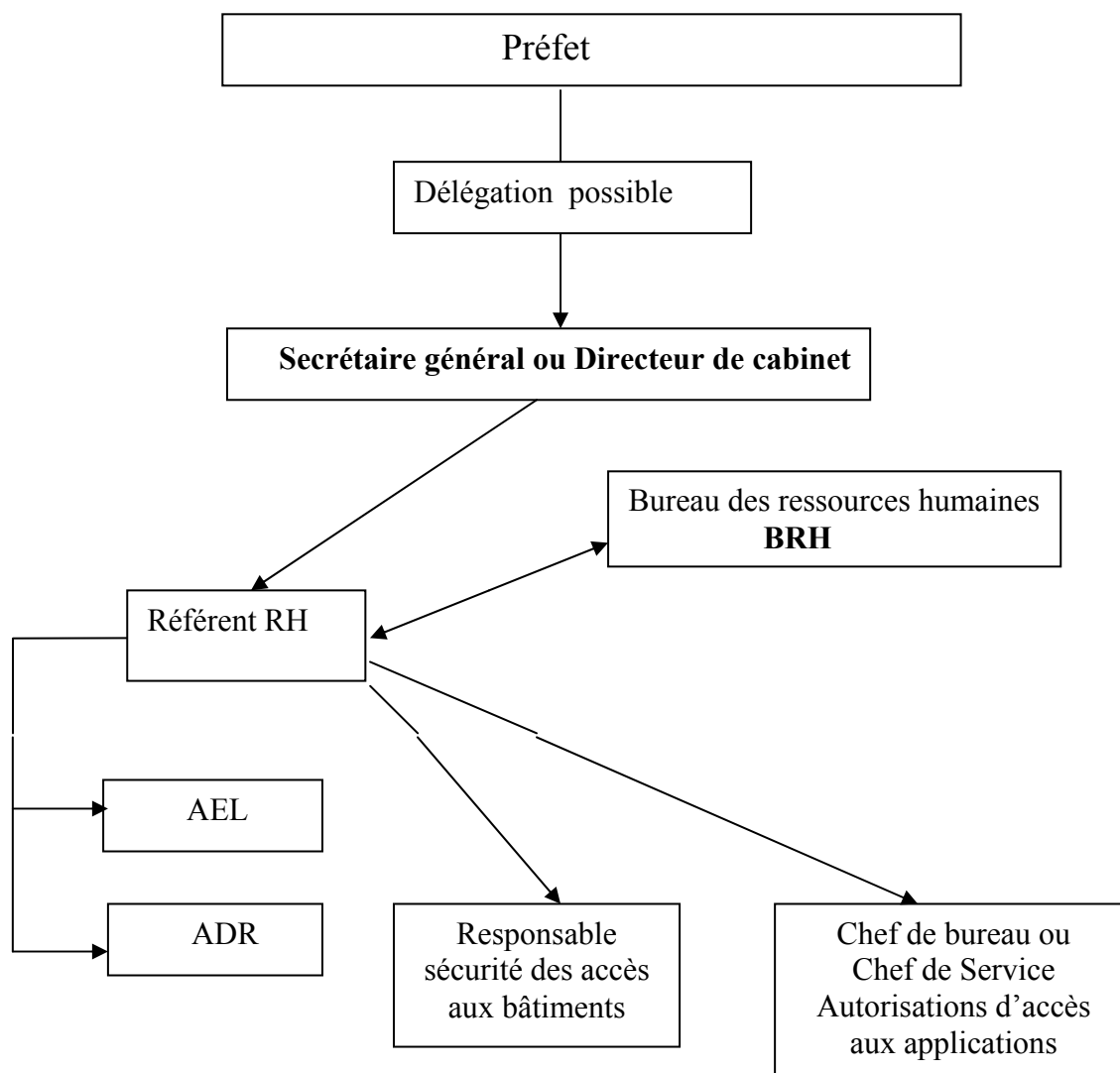
ANNEXE VI

ORGANIGRAMME FONCTIONNEL TYPE EN ADMINISTRATION CENTRALE



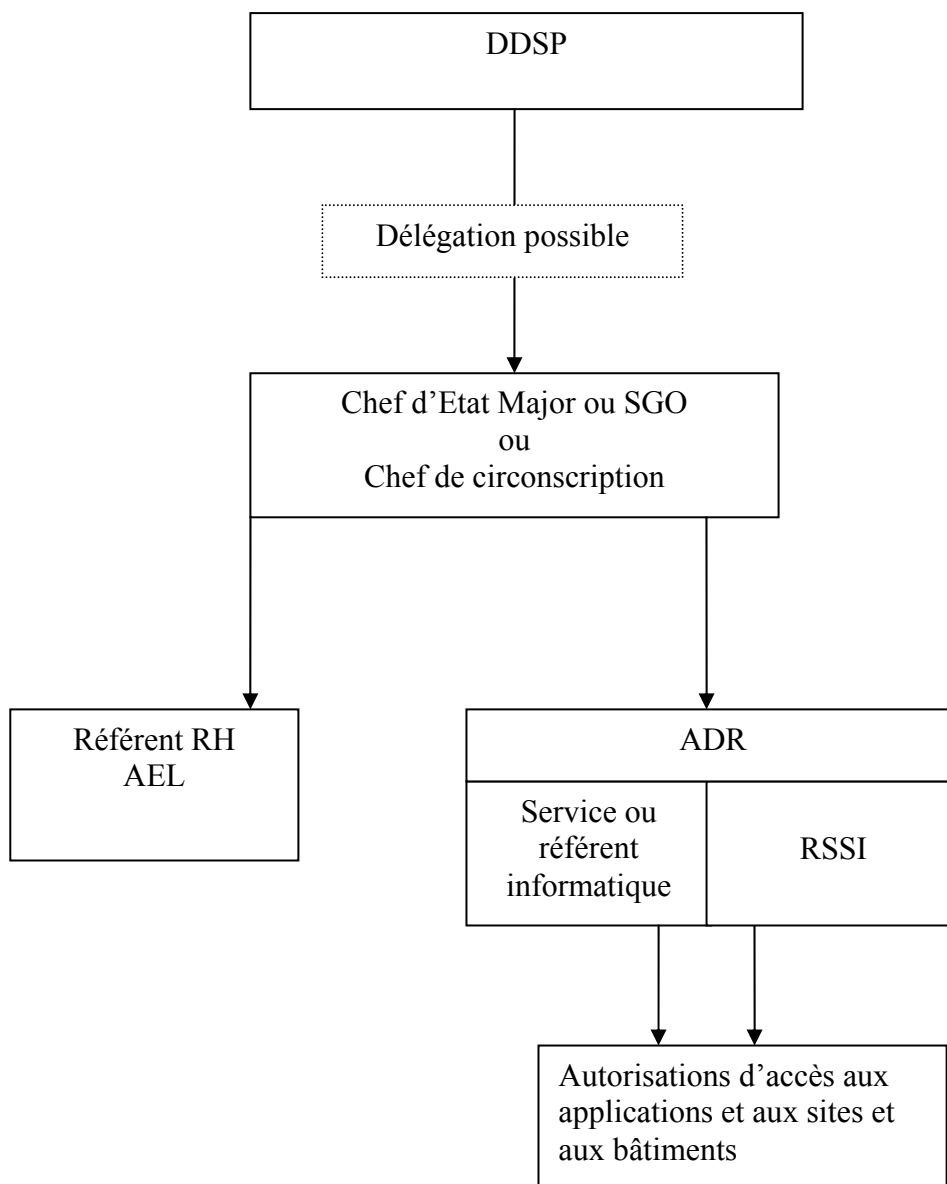
ANNEXE VII

ORGANIGRAMME FONCTIONNEL TYPE EN ADMINISTRATION TERRITORIALE



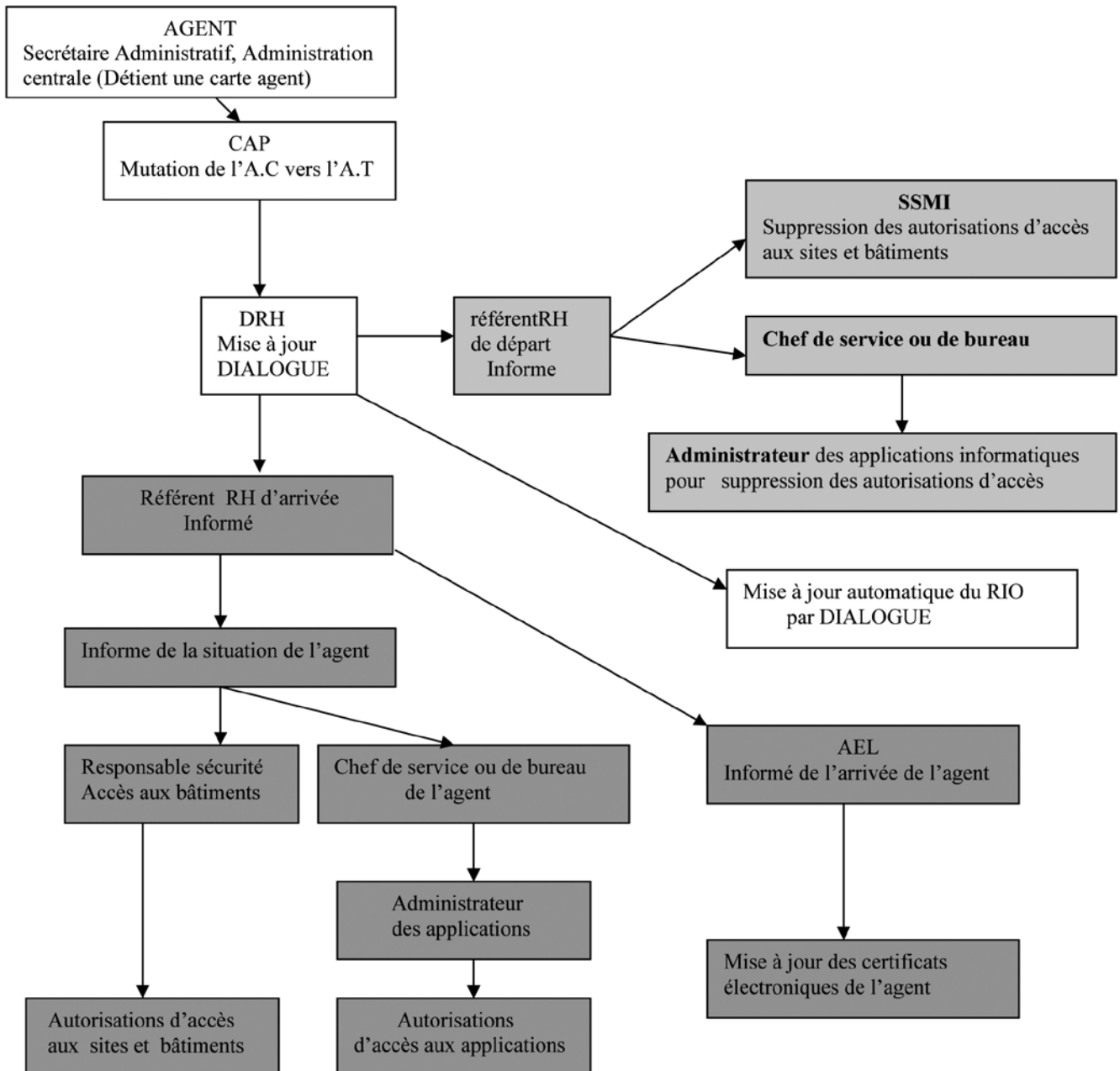
ANNEXE VIII

ORGANIGRAMME FONCTIONNEL TYPE
EN DIRECTION DÉPARTEMENTALE DE LA SÉCURITÉ PUBLIQUE (DDSP)



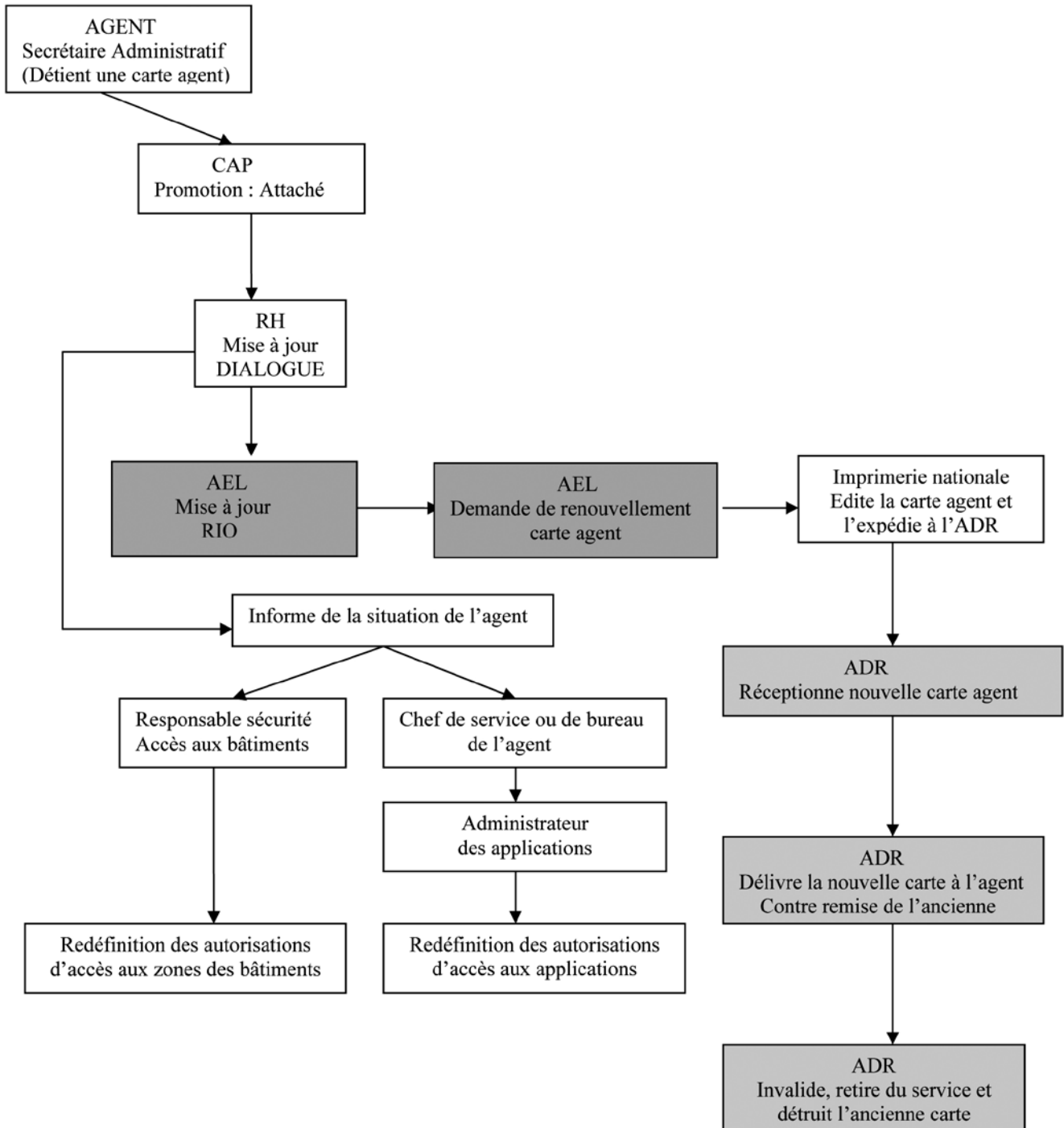
ANNEXE IX

MODIFICATION DE LA SITUATION DE L'AGENT N'ENTRAÎNANT PAS DE CHANGEMENT DE SA CARTE AGENT



ANNEXE X

MODIFICATION DE LA SITUATION DE L'AGENT ENTRAÎNANT UN CHANGEMENT DE SA CARTE AGENT



ANNEXE XI

MODIFICATION DE LA SITUATION DE L'AGENT ENTRAÎNANT UN RETRAIT
DE SA CARTE AGENT

