SANTÉ

ÉTABLISSEMENTS DE SANTÉ

MINISTÈRE DES AFFAIRES SOCIALES ET DE LA SANTÉ

MINISTÈRE DE LA JUSTICE

Secrétariat général des ministères chargés des affaires sociales

Délégation à la stratégie des systèmes d'information de santé (DSSIS)

Secrétariat général du ministère de la justice

Instruction interministérielle n° SG/DSSIS/SGMJ/2016/217 du 4 juillet 2016 relative à la fourniture de cartes à puce « agents extérieurs justice » aux professionnels de santé et personnels administratifs habilités à accéder au système d'information du ministère de la justice

NOR : *AFSZ1618711J*

Date d'application : immédiate.

Validée par le CNP le 22 juillet 2016. – Visa CNP 2016-112.

Catégorie : directives adressées par le ministre aux services chargés de leur application, sous réserve, le cas échéant, de l'examen particulier des situations individuelles.

Résumé : la présente instruction a pour objectif d'expliciter le rôle des chefs d'établissement pénitentiaire et des directeurs d'établissement de santé dans l'authentification des personnels des unités sanitaires rattachés aux établissements de santé en vue de la remise d'une carte à puce « agent extérieur justice ».

Mots clés : authentification des personnels – carte à puce – unités sanitaires des établissements pénitentiaires.

Références :

Décret n° 87-604 du 31 juillet 1987 relatif à l'habilitation des personnes auxquelles peuvent être confiées certaines fonctions dans les établissements pénitentiaires et complétant l'article R. 79 du code de procédure pénale, modifié par les décrets n° 94-965 du 2 novembre 1994 et n° 2007-931 du 15 mai 2007 ;

Décret n° 2011-817 du 6 juillet 2011 portant création d'un traitement de données à caractère personnel relatif à la gestion informatisée des détenus en établissement (GIDE) ;

Décret n° 2014-558 du 30 mai 2014 portant création d'un traitement de données à caractère personnel relatif à la gestion nationale des personnes détenues en établissement pénitentiaire dénommé GENESIS ;

Circulaire interministérielle n° DGS/MC1/DGOS/R4/DAP/DPJJ/2012-94 du 21 juin 2012 relative aux recommandations nationales concernant la participation des professionnels de santé exerçant en milieu carcéral à la commission pluridisciplinaire unique (CPU) prévue par l'article D. 90 du code de procédure pénale ou à la réunion de l'équipe pluridisciplinaire prévue par l'article D. 514 du même code et au partage d'informations opérationnelles entre professionnels de santé et ceux de l'administration pénitentiaire et de la protection judiciaire de la jeunesse ;

Circulaire interministerielle n° DGOS/DSR/DGS/DGCS/DSS/DAP/DPJJ/2012-373 du 30 octobre 2012 relative à la publication du guide méthodologique sur la prise en charge sanitaire des personnes placées sous main de justice.

Annexes :

Convention relative à l'authentification pour l'accès de professionnels de sante et personnels administratifs au système d'information du ministère de la justice signée entre le ministère de la justice et le ministère de la santé.

Avenant n° 1 à la convention.

La ministre des affaires sociales et de la santé et le ministre de la justice à Mesdames et Messieurs les directeurs généraux des agences régionales de santé ; Mesdames et Messieurs les directeurs interrégionaux des services pénitentiaires.

1. **Contexte et enjeux**

Des personnels des unités sanitaires rattachées aux établissements de santé sont appelés à accéder au système d'information du ministère de la justice « GENESIS » qui gère le parcours des personnes détenues en établissement pénitentiaire. Cet accès doit permettre :

– la saisie d'observations à partager entre les secteurs justice et santé ;

– l'accès en consultation au livret du détenu.

Cet accès permettra en outre en 2016 l'extraction de listes pour faciliter, par exemple, la dispensation des médicaments.

Il est rappelé que GENESIS ne porte pas atteinte au secret médical.

Pour répondre aux exigences de la CNIL et du Conseil d'État, une authentification forte permet de sécuriser l'accès aux données sensibles à caractère personnel, traitées par ce système d'information. La procédure dérogatoire de connexion par « login-mot de passe » est remplacée par l'usage d'une carte à puce contenant un certificat d'authentification de chaque personne autorisée.

Cette procédure concerne les personnels « justice » et également les professionnels de santé et personnels administratifs, titulaires ou contractuels, des unités sanitaires, dûment habilités par le directeur de l'établissement de santé de rattachement.

Une « Convention relative à l'authentification pour l'accès de professionnels de santé et personnels administratifs au système d'information du ministère de la justice » a été signée en 2015 par le secrétaire général des ministères chargés des affaires sociales et le secrétaire général du ministère de la justice. Un avenant à cette convention a été signé en 2016 (voir annexe).

Cette convention prévoit la délivrance de cartes à puce « agents extérieurs justice » embarquant un certificat d'authentification relevant de l'IGC[1] justice aux professionnels de santé et personnels administratifs habilités qui ont besoin d'accéder au système d'information GENESIS.

Ces cartes sont fournies et renouvelées à titre gratuit par le ministère de la justice.

2. **Procédure**

2.1. *Arrivée d'un nouvel agent « extérieur »*

Les professionnels de santé et personnels administratifs concernés sont habilités dans un premier temps en application de la circulaire interministérielle n° DGOS/DSR/DGS/DGCS/DSS/DAP/DPJJ/2012/373 du 30 octobre 2012 relative à la publication du guide méthodologique sur la prise en charge sanitaire des personnes placées sous-main de justice. Elle peut être réalisée par le directeur de l'établissement de santé ou le Centre national de gestion (CNG).

Ces personnels sont habilités dans un second temps en application du décret n° 87-604 du 31 juillet 1987 modifié relatif à l'habilitation des personnes auxquelles peuvent être confiées certaines fonctions dans les établissements pénitentiaires et complétant l'article R. 79 du code de procédure pénale. Cette habilitation est réalisée par la direction interrégionale.

Le ministère de la Justice au vu de données numériques vérifiées par l'établissement de santé, prendra en compte ces agents dans son annuaire LDAP sous l'arborescence « agents extérieurs ». Ceux-ci doivent être dotés d'une boite à lettres électronique (BAL) au format de leur employeur, à qui il appartient de créer ladite boite. À défaut, une BAL au format « @externes.justice.gouv.fr » sera créée pour ces agents.

Le chef d'établissement pénitentiaire, autorité d'enregistrement, ou son délégué, procèdera à la remise en face à face de la carte Justice à l'agent « extérieur » habilité, sur présentation de sa carte d'identité et selon les formalités décrites dans le référentiel général de sécurité.

Les justificatifs sont classés au dossier d'habilitation de l'agent tenu par le chef de l'établissement pénitentiaire.

Pour authentifier l'agent « extérieur » habilité, le chef de l'établissement pénitentiaire devra être informé par le directeur de l'Établissement de santé de rattachement :

– de l'identité de l'agent concerné ;

[1] Infrastructure de gestion de clefs.

– de sa position administrative ou de son statut ;
– de sa profession ;
– et de sa fonction.

Le directeur de l'établissement de santé chargé de la prise en charge sanitaire des personnes détenues fournit au chef de l'établissement pénitentiaire :

– la liste des personnes habilitées ;
– les informations associées au mouvement (voir ci-dessous le paragraphe 2.2).

Ces informations seront échangées, par voie électronique comportant une note administrative, au niveau local pour permettre au chef d'établissement pénitentiaire de procéder à la révocation des certificats justice détenus par des agents qui n'en ont plus l'utilité, dans les délais prévus par le RGS***.

Le dossier d'habilitation « justice » sera conservé 5 ans après la cessation de fonctions en établissement pénitentiaire de l'agent concerné et la restitution de la « carte agent extérieur justice », afin de répondre aux exigences de traçabilité de la CNIL et du Conseil d'État.

2.2. *Anticipation du départ d'un agent « extérieur »*

La liste des personnes habilitée est tenue à jour par le directeur de l'établissement de santé qui s'engage à fournir au chef de l'établissement pénitentiaire les mouvements effectifs et prévisionnels de personnels, notamment toute cause mettant fin à la nécessité pour un agent concerné de détenir un certificat justice à compter d'une date précise.

Le directeur de l'établissement de santé fournit au chef de l'établissement pénitentiaire :

– les nom et prénom de l'agent concerné ;
– ses position, fonction et profession ;
– la date prévisionnelle de son départ effectif ainsi que la cause de ce départ.

Toute question est à adresser aux boites fonctionnelles suivantes des ministères concernés et sera traitée en lien avec les bureaux concernés de la direction générale de l'offre de soins et de la direction de l'administration pénitentiaire :

Ministère des affaires sociales et de la santé :
DSSIS-SECR@sg.social.gouv.fr
Tél. : 01-40-56-40-20 et 01-40-56-43-68

Ministère de la justice :
carte-agent-justice.dap@justice.gouv.fr

Je vous saurais gré de bien vouloir nous tenir informés de toute difficulté rencontrée dans la mise en œuvre de la présente instruction.

Pour la ministre et par délégation :

Le secrétaire général des ministères chargés des affaires sociales,
P. Ricordeau

Le secrétaire général du ministère de la justice,
É. Lucas

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CONVENTION RELATIVE A L'AUTHENTIFICATION POUR L'ACCES DE PROFESSIONNELS DE SANTE ET PERSONNELS ADMINISTRATIFS AU SYSTEME D'INFORMATION DU MINISTERE DE LA JUSTICE

ENTRE LE MINISTERE DE LA JUSTICE
ET
LE MINISTERE DE LA SANTE

En date du 15 juin 2015
Référence : ConventionCarteAgent_MJ Santé_VF_15juin2015.doc
État : Final
Version : VF

Entre d'une part,

Le Ministère de la Justice, situé 13 Place Vendôme, Paris 1er,

représenté par Monsieur Eric LUCAS, Secrétaire Général du Ministère de la Justice,

d'autre part,

Le Ministère des Affaires sociales, de la Santé et des droits des femmes situé 14, avenue Duquesne 75350 PARIS 07 SP,

représenté par Monsieur Pierre RICORDEAU, Secrétaire général des ministères chargés des affaires sociales,

il a été convenu ce qui suit,

Préambule

Le ministère de la justice, a engagé un processus de dématérialisation de ses procédures que pilote son secrétariat général.

Les services d'authentification et de signature (l'infrastructure de gestion de clefs et la carte à puce) du Ministère de la Justice ont obtenu la certification *** au sens du RGS le 26 novembre 2012 ainsi que l'inscription sur la Trust-service Status List (TSL), liste européenne qui recense les autorités de certification de confiance.
Le ministère de la Justice devait choisir la certification *** puisque les magistrats émettent des jugements, ordonnances et arrêts, qui sont des actes authentiques dont la signature doit être présumée fiable au sens de l'article 1316-4 du code civil**.**

Le Ministère de la Justice n'ayant qu'une seule IGC, toutes les cartes « Justice » sont de ce fait soumises aux règles du RGS *.**

Pour rappel, le Référentiel Général de Sécurité (RGS, décret 2010-112 pris pour l'application des articles 9, 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) impose une vérification de l'identité, qualité et fonctions du porteur de carte ainsi qu'une remise en face à face par une autorité hiérarchique, dite autorité d'enregistrement.

Le ministère de la justice a ainsi conçu sa chaîne de remise de cartes (chaîne de confiance) en s'appuyant sur les services de gestion des ressources humaines qui sont habilités à accéder au dossier administratif des agents.

Dans les établissements pénitentiaires, du personnel d'autres instances que la direction de l'administration pénitentiaire (DAP), **dont des personnels des unités sanitaires rattachées aux établissements de santé**, sont rapidement appelés à accéder au système d'information « GENESIS » qui gère le détenu en établissement pénitentiaire.

Pour répondre aux exigences de la CNIL et du Conseil d'Etat, une authentification forte est progressivement mise en place pour sécuriser l'accès aux données sensibles à caractère personnel, traitées par le système d'information du Ministère de la Justice.
Il s'agit de remplacer la procédure de connexion par « login-mot de passe » par l'usage d'une carte à puce contenant un certificat d'authentification de l'agent.

Aussi, outre les personnels Justice, il convient que les personnels concernés professionnels de santé et personnels administratifs, titulaires ou contractuels, soient également dotés de cartes à puce.

Par convention ces personnels sont désignés sous le terme générique d'agents.

Il s'agit d'authentifier ces personnels selon les modalités décrites à l'article 5 ci-après par un certificat remis en face à face, de vérifier leur identité et leur appartenance aux professions de santé, et non de définir un profil leur donnant accès à certaines informations du SI Justice.

C'est un projet à multiples dimensions : organisationnelle, stratégique et technique.

Le dispositif objet de la présente convention représente une solution transitoire d'authentification des professionnels de santé dans le SI Justice. L'instruction de la solution

cible est décrite dans l'article 3. Cette solution cible fera l'objet d'une nouvelle convention qui remplacera la présente convention.

Article 1- Objet

L'objet de cette convention est de permettre le respect des délais et contraintes du RGS ***, dans les procédures de suivi du cycle de vie de la carte d'agent « extérieur Justice » émise par l'IGC Justice.

En effet la perte d'une * entrainerait une remise en cause des actes judiciaires signés électroniquement. Ces procédures font l'objet d'audit annuel de contrôle dans le cadre de la certification RGS ***.

Le premier usage du certificat justice d'authentification *** est l'accès au SI « GENESIS » en application du décret 2014-558 du 30 mai 2014.

Le système d'information « GENESIS » est déployé sur l'ensemble du territoire à compter d'octobre 2014.

Article 2 - Périmètre de la convention

Les cartes agents concernent les professionnels de santé et personnels administratifs qui interviennent dans les unités sanitaires et qui sont habilités à accéder au SI Justice.
Le nombre d'intervenants personnels hospitaliers potentiellement concernés est précisé en annexe 2.

Article 3 - Le Système cible

L'authentification des professionnels de santé et personnels administratifs est mise en œuvre par l'ASIP Santé (autorité de certification de l'IGC Santé) qui gère et administre l'infrastructure de gestion de clefs (IGC) de la carte de professionnel de santé (CPS) et des autres produits de certification.

La détermination de la solution cible nécessite la réalisation d'une instruction technique et organisationnelle complète portant sur les modalités selon lesquelles des personnels intervenant dans les unités sanitaires rattachées aux établissements de santé (professionnels de santé et personnels administratifs) peuvent accéder au système d'information Justice dans des conditions respectant le niveau de sécurité du SI Justice et les principes et contraintes d'enrôlement des cartes agent Justice.
Ces travaux d'instruction seront menés conjointement par l'ASIP Santé et les services concernés du ministère de la justice et devront aboutir, dans un délai maximal de 6 mois à compter de la signature de la présente convention, à la définition de la solution cible et de la trajectoire à mettre en œuvre pour y parvenir.

Un comité de pilotage de l'avancement des travaux est mis en place à compter de la signature de la présente convention. La première réunion du comité de pilotage devra se tenir dans les 3 mois suivant la signature de la présente convention.

Article 4 - Conditions et procédure d'habilitation

Les conditions d'habilitation sont définies par le décret n° 87-604 du 31 juillet 1987 modifié par le décret n° 94-965 du 2 novembre 1994 et le décret 20 07-931 du 15 mai 2007 relatif à l'habilitation des personnes physiques ou morales auxquelles peuvent être confiées certaines fonctions au sein des Etablissements pénitentiaires et complétant l'article R.79 du code de procédure pénale.

Les dispositions d'habilitation et d'autorisation d'accès des personnels sanitaires sont précisées dans la CIRCULAIRE INTERMINISTERIELLE N°DGOS/DSR/DGS/DGCS/ DSS/DAP/DPJJ/2012/373 du 30 octobre 2012 relative à la publication du guide méthodologique sur la prise en charge sanitaire des personnes placées sous-main de justice.

Article 5 - L'authentification des agents concernés

Durant la période transitoire, le Ministère de la Justice procèdera à l'authentification des agents concernés travaillant en établissement pénitentiaire et leur délivrera des « cartes d'agents Justice extérieurs » embarquant un certificat d'authentification relevant de l'IGC[1] Justice.

A cette fin, des mesures organisationnelles doivent être prises afin de permettre à tout instant de connaître l'identité d'un utilisateur de certificat « Justice » porteur d'une carte d'agent « extérieur ». Ces mesures sont déclinées ci après.

Pour authentifier l'agent « extérieur » habilité, le chef de l'établissement pénitentiaire devra être informé par le directeur de l'établissement de santé de rattachement :

- de l'identité de l'agent concerné,
- de sa position administrative le cas échéant,
- de sa profession,
- et de sa fonction,

selon des modalités précisées par une instruction conjointe des deux ministères concernés.

Le Ministère de la Justice au vu de données numériques vérifiées par l'établissement de santé, créera ces agents dans son annuaire LDAP sous l'arborescence « agents extérieurs ». Ceux-ci doivent être dotés d'une boite à lettres électronique (BAL) au format de leur employeur, à défaut, au format @externes.justice.gouv.fr

Le chef d'établissement pénitentiaire, autorité d'enregistrement, ou son délégué, procèdera à la remise en face à face de la carte Justice à l'agent habilité, sur présentation de sa carte d'identité et selon les formalités décrites dans le référentiel général de sécurité.
Les justificatifs sont conservés au dossier d'habilitation de l'agent par le chef d'établissement qui le détient.

Le dossier d'habilitation sera conservé 5 ans après la cessation de fonctions en établissement pénitentiaire de l'agent concerné et la restitution de la « carte agent extérieur justice », afin de répondre aux exigences de traçabilité de la CNIL et du Conseil d'Etat.

[1] Infrastructure de gestion de clefs

Voir annexe 1 de la présente convention : présentation de la carte agent Justice et des procédures liées.

Article 6 - Gestion des mouvements de personnels

Le directeur de l'établissement de santé chargé de la prise en charge sanitaire des personnes détenues fournit au chef de l'établissement pénitentiaire :

- La liste des personnes habilitées,
- Les informations associées au mouvement.

Cette liste est tenue à jour par le directeur de l'établissement de santé qui s'engage à fournir au chef de l'établissement pénitentiaire les mouvements[2] effectifs de personnels, notamment toute cause qui met fin à la nécessité pour un agent concerné de détenir un certificat Justice à compter d'une date précise.

Ces informations seront échangées, par voie électronique, au niveau local pour permettre au chef d'établissement pénitentiaire de procéder à la révocation des certificats justice détenus par des agents qui n'en ont plus l'utilité, dans les délais prévus par le RGS ***.

Les modalités seront décrites dans l'instruction précitée à l'article 5 ci-dessus.

Article 7 - Respect des conditions générales d'utilisation de la carte agent Justice

Le Ministère de la Justice a fixé les conditions générales d'utilisation de la carte agent Justice et en particulier prévoit que :

- Le professionnel de santé s'engage à faire un usage professionnel de sa carte uniquement dans le milieu Justice.
- Il s'engage à ne pas prêter sa carte ni communiquer son code PIN.
- En cas de compromission, perte ou vol, il s'engage à en faire la déclaration immédiate sur le site prévu à cet effet : https://www.asscap.justice.ants.gouv.fr.
- Le porteur de la carte « Justice » s'engage à ne signer que des documents dans le cadre de son activité Justice, sur des applications Justice, dans des locaux Justice et sur des postes Justice.

Voir annexe 3.

Le Ministère de la Justice informe le porteur de ses obligations.

Toute utilisation frauduleuse de la carte à puce ou des certificats qu'elle porte, engage sa responsabilité civile et pénale.
La responsabilité de l'Etat est engagée selon le droit en vigueur.

Les atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques sont prévues et réprimées par les articles 226-16 à 226-24 du code pénal.

[2] Mutation, retraite, congé de longue maladie, détachement, mise en disponibilité, etc.

Les atteintes aux systèmes de traitement automatisé de données sont prévues et réprimées par les articles 323-1 à 323-7 du code pénal.

Article 8- Conditions financières

Le Ministère de la Justice adressera une facturation interne semestrielle aux établissements de santé de rattachement des personnels des unités sanitaires selon des modalités décrites dans l'instruction précitée à l'article 5 ci-dessus. Le montant des cartes est celui payé à l'ANTS.[3]

Article 9 - Durée de la convention - modalités de dénonciation

Cette convention est conclue pour une durée d'un an reconductible tacitement jusqu'à fin de la période transitoire et atteinte de la cible.
Elle peut être révisée et amendée à la demande de l'une ou l'autre des parties.
Elle peut être dénoncée par l'une ou l'autre des parties, chaque année, 3 mois avant la date anniversaire de sa signature.

Le Secrétaire Général	Le Secrétaire Général
Signé	Signé
Eric LUCAS	Pierre RICORDEAU

[3] 30 euros la carte nominative valide 6ans - certificat renouvelable une fois, après 3ans. Délai de livraison des cartes 10 à 15 jours après commande.

Annexe 1 présentation de la carte agent justice et des procédures liées

Le présent document vise
- à présenter les processus techniques et organisationnels liés à la carte agent justice,
- et à démontrer les fonctionnalités inhérentes permettant de garantir la fiabilité et la sécurité des accès.

Partenariat avec l'ANTS

Selon l'article 1 II, 2° 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, est considérée comme **prestataire de services de confiance** : *"toute personne offrant des services tendant à la mise en œuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique*".

Selon l'article 1 du décret n° 2001-272 du 30 mars 2001 relatif à la signature électronique, on entend par prestataire de services de certification électronique : "*toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique*."

L'ANTS est ainsi un prestataire de services de confiance et un prestataire de services de certification électronique au sens des dispositions précitées.

Par ailleurs, l'ANTS assure l'exploitation de l'infrastructure de gestion de clefs (IGC) et gère les certificats électroniques permettant l'authentification des agents du ministère de la justice.

En application de l'article 2 du décret 2007-240 du 22 février 2007 portant création de l'Agence nationale des titres sécurisés, le ministère de la Justice et l'ANTS sont liés par convention.

1- Autorité de Certification et schéma organisationnel de la chaîne de confiance

L'organigramme ci-dessous décrit la chaîne de confiance telle que précisée dans la Politique de Certification « Personnes » disponible sur le site WEB du Ministère de la Justice (http://www.justice.gouv.fr/igc/ants).

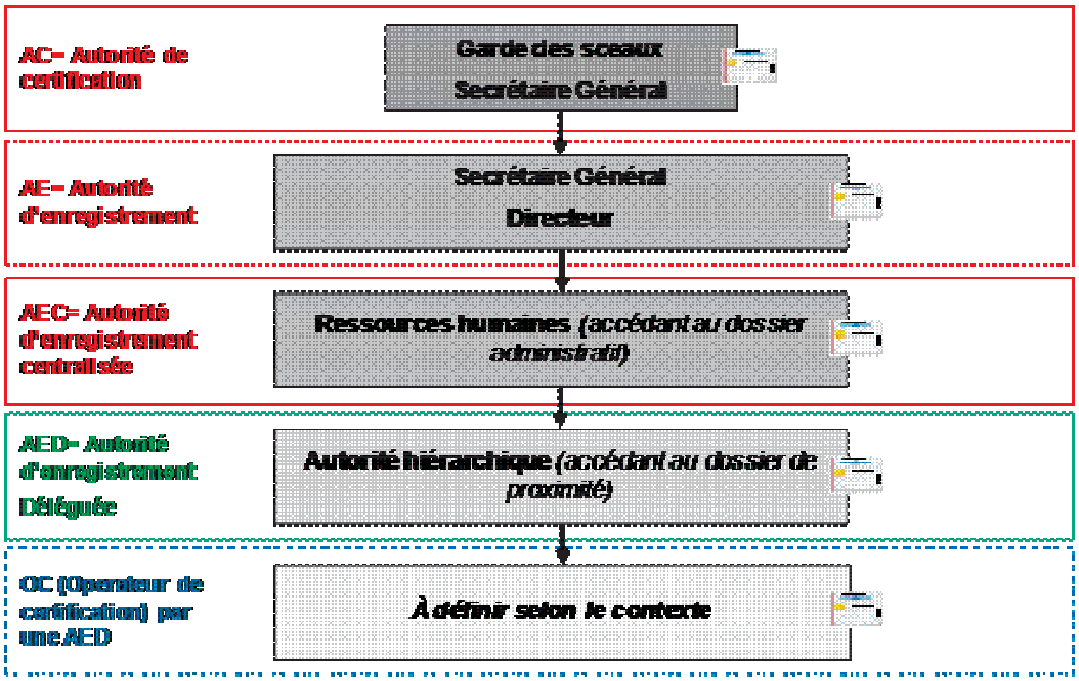

Figure 1 - Schéma de distribution des rôles de confiance

Ainsi, la politique de certification du Ministère de la Justice définit les rôles comme suit :
« L'AC a pour responsabilité de garantir le lien (infalsifiable et univoque) entre l'identifiant d'un porteur et une bi-clé cryptographique pour un usage donné. Cette garantie est apportée par des certificats de clé publique qui sont signés par la clé privée de l'AC.». En outre,

« L'AE est responsable de la délivrance des supports de clés et des certificats aux porteurs lors d'un face à face. L'AE effectue en outre, les opérations de demandes de certificat à la vue des données fournies par différents systèmes d'information. L'AE peut intervenir pour la révocation d'un certificat octroyé à toute personne située dans la hiérarchie de l'AE (AEC, AED ou OC).

L'Autorité d'Enregistrement du MJ est structurée sur la base d'un système hiérarchique à quatre niveaux.

- Le niveau inférieur est celui des Opérateurs de Certification (OC). Ils ont un contact en face à face avec les porteurs lors de la remise du support cryptographique. Les Opérateurs de Certification (OC) sont désignés par des personnes ayant le rôle d'Autorité d'Enregistrement Déléguée (AED).
- Les personnes ayant le rôle d'Autorité d'Enregistrement Déléguée (AED) sont désignées par des personnes ayant le rôle d'Autorité d'Enregistrement Centralisée (AEC). Les personnes ayant le rôle d'AED assurent la validation des demandes de certificat initiées par les Opérateurs de Certification (OC). Chacune des personnes ayant le rôle d'AED peut

désigner d'autres AED pour l'assister dans son travail. Les responsables RH désignent ainsi comme AED les directeurs de greffe ou d'établissement pénitentiaire ou pour mineurs, de leur ressort et ayant accès au dossier administratif personnel.

- Les personnes ayant le rôle d'Autorité d'Enregistrement Centralisée (AEC) sont désignées par des personnes ayant le rôle d'Autorité d'Enregistrement (AE). L'AEC est chargée de désigner les Responsables RH comme AED et d'assurer le suivi de ces acteurs.
- Les personnes ayant le rôle d'Autorité d'Enregistrement (AE) sont initialement désignées, sur demande du Secrétariat Général du MJ, par l'administrateur technique de l'annuaire du MJ. L'AE « direction des services judiciaires » désigne une AEC au sein de ses services. Toute personne ayant acquis le rôle d'Autorité d'Enregistrement (AE) peut désigner un alter-ego.

Les personnes ayant le rôle d'Autorité d'Enregistrement (AE), d'Autorité d'Enregistrement Centralisée (AEC), d'Autorité d'Enregistrement Déléguée (AED) ou d'Opérateur de Certification (OC) sont dotées de certificats de clé publique et de supports de clés (cartes agent). »

2 - Attributs de la carte agent justice

Présentation générale et fonctionnement pratique

La carte agent justice contient deux certificats distincts permettant de :

- S'authentifier de manière forte aux applications (Concaténation de ce que l'entité connaît, à savoir un code PIN, et de ce que l'entité détient, à savoir une carte à puces),
- Signer électroniquement les documents lorsque la signature fait partie des fonctionnalités de l'application.

Chaque certificat est de surcroît protégé par un code PIN choisi par l'utilisateur lors de l'activation de sa carte. L'attaque par force brute du code PIN n'est pas possible car la carte est bloquée après **3 codes PIN erronés.**

Ces fonctionnalités permettent une connexion unique et sécurisée aux différentes applications du Ministère de la Justice.

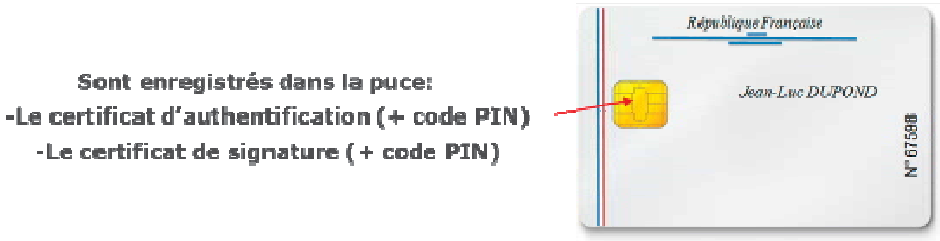

Figure 2 – Exemple de visuel d'une carte à puce "agent justice "

Les données à caractère personnel figurant dans les certificats sont : « nom –prénom »

L'authentification forte

L'authentification forte est une procédure d'identification qui requiert la concaténation d'au moins deux éléments ou « facteurs » d'authentification. On considère que ces éléments peuvent être :

- **Ce que l'entité connaît (un mot de passe, un code PIN, une phrase secrète, etc.)**
- Ce que l'entité détient (**une carte magnétique**, RFID, une clé USB, un PDA, **une carte à puce**, un Smartphone, etc.). Soit un élément physique appelé « authentifieur » ou Token.
- Ce que l'entité est, soit une personne physique (empreinte digitale, empreinte rétinienne, structure de la main, structure osseuse du visage ou tout autre élément biométrique)
- Ce que l'entité sait faire ou fait, soit une personne physique (biométrie comportementale tel que signature manuscrite, reconnaissance de la voix, un type de calcul connu de lui seul, un comportement, etc.

On dénombre actuellement trois familles technologiques pour l'authentification forte :
One Time Password (OTP) / Mot de passe à usage unique, **le certificat numérique** et la biométrie. **La carte agent justice a recours au certificat numérique.**

- La carte fournie par l'ANTS respecte la norme relative aux exigences de sécurité des dispositifs de création de signature électronique de la directive européenne et du décret n° 2001-272 du 30 mars 2001: CWA 14169 - PP SSCD (Profil de Protection Secure Signature Creation Device)
- La carte a une certification Critères Communs EAL5+ délivrée en novembre 2011 et est référencée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Il s'agit de la carte IDeal Citiz[4] de la société Morpho.
- L'ANTS fournit des cartes à puces à la norme IAS/ECC (Identification Authentification Signature European Citizen Card) respectant ce profil de protection SSCD.
- Les cartes à contact sont produites par l'imprimerie nationale qui dispose par décret n°2006-1436 du 24 novembre 2006 d'un monopole d'état sur les « Cartes permettant d'identifier les agents publics »

La signature électronique

La signature électronique, comme la signature manuscrite, permet **d'identifier le signataire** d'un document et de créer un lien entre le signataire et le document. Elle a la même utilité que la signature manuscrite, elle **engage la responsabilité de son auteur** de la même manière.

La signature électronique a été mise en place par l'article 1316-4 du code civil et l'article 801-1 du code de procédure pénale.

Elle n'est pas l'image ou la numérisation d'une signature manuscrite : C'est une opération mathématique complexe réalisée par le processeur de la carte à puce, **qui rend impossible :**

- **La capture de la signature pour une réutilisation frauduleuse,**
- **La falsification ou l'altération du document**

La signature électronique *** à valeur probante **permet le renversement de la charge de la preuve (**prévu par le code civil pour les actes authentiques) et garantit aux actes judiciaires la valeur **d'actes authentiques** comme le fait la signature manuscrite du magistrat.

[4] http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-qualifies/p_47_Carte_a_puce_CC_Ideal_Citiz_versions_1.6.0_et_1.6.1_(applications_passeport_ICAO_EAC_et_IAS_ECC).html

Le MJ est le seul ministère français à avoir obtenu la certification * par l'ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information) pour ces certificats d'authentification et signature électronique, son Infrastructure de gestion des clefs (IGC) et le dispositif de signature qu'est la carte à puce.

Le MJ est le seul ministère français à être inscrit sur la « Trust services list » européenne (liste des services de confiance).

Le MJ est **audité chaque année** sur ses processus.

Remise des cartes

Principe

Les cartes « agent justice » distribuées doivent permettre de s'authentifier et garantir la valeur probante des documents signés, puisque ces dernières répondent à des conditions techniques de sécurité.
La réglementation prévoit leur remise en face à face afin de s'assurer de l'identité du futur porteur de la carte. Cette remise en face à face est un des éléments contribuant à la présomption de l'identité de la personne qui l'utilise et de fiabilité de la signature du porteur de la carte, telle que prévue à l'article 1316-4 du Code Civil.
La remise de la carte de signature en face à face constitue donc une garantie pour le signataire en renversant la charge de la preuve en cas de contestation de la signature.

Modalités de remise des cartes agents

Réception des cartes et des codes PIN

1. Le futur porteur de carte reçoit sous pli confidentiel à son attention exclusive, sur son lieu de travail, son code PIN provisoire à personnaliser.
2. Le responsable de la gestion des ressources humaines du SAR ou de la DISP ou de la DIRPJJ reçoit les cartes personnalisées aux noms des personnels de son ressort aux fins de remise en face à face.
3. Le directeur de site (greffe ou établissement pénitentiaire ou établissement pour mineurs) qui a été délégué par le responsable RH en tant qu'AED reçoit les cartes personnalisées pour les personnes de son site.

Remise des cartes aux agents

1. L'Autorité d'Enregistrement Déléguée ou leur Opérateur de Certification remet, en face à face, les cartes aux utilisateurs des applications métier concernées.
2. Chaque nouveau porteur de carte se connecte à l'application à travers l'intranet Justice avec sa carte à puce et s'authentifie avec son code PIN provisoire, il est alors reconnu par le système.
3. Le porteur de carte est invité à changer son code d'authentification et son code de signature dès l'initialisation de sa carte (il peut choisir 2 codes identiques, même si, pour des raisons de sécurité évidentes, cela n'est pas recommandé).
4. Le porteur de carte choisit et déclare 4 secrets (3 de ces 4 secrets sont à choisir dans une liste de 4 questions, le 4ème secret est un mot de passe comportant au moins 8 caractères

dont un caractère spécial). Ces secrets lui permettront d'être reconnu par le système (application de gestion des cartes) en cas d'oubli de son code, de perte ou vol de sa carte.

5. Le porteur de carte signe électroniquement le PV de remise en face à face de sa carte dont il vient de vérifier le bon fonctionnement. L'application stocke ce PV qui peut être consulté par l'autorité émettrice du certificat ou le porteur de cartes.
6. L'autorité d'enregistrement déléguée ou leurs Opérateurs de Certification respectifs, qui a procédé à la remise de carte :
    - Se connecte par l'intranet justice à l'application de gestion des cartes,
    - Accède à son parapheur électronique pour contresigner les PV de remise des cartes du jour en tapant une seule fois son code de signature,

Gestion du cycle de vie des cartes

Les cartes distribuées doivent permettre de garantir la valeur probante des documents signés. Pour ce faire, leur remise et leur production doivent obéir à des conditions strictes. Leur gestion quotidienne doit également suivre quelques principes simples.
Elle est confiée aux personnes des services des ressources humaines déléguées par une autorité de certification.
Compte-tenu des pouvoirs de signature associés à ces cartes, il importe que certaines opérations (déclaration de perte ou de vol) puissent être menées rapidement. La dématérialisation offre à cet égard une grande flexibilité.

Demande de carte pour un agent Justice

Le service RH vérifie les informations d'identification dans le dossier administratif de la personne pour laquelle l'autorité demande un certificat. Il crée une demande de certificat, sur l'application dédiée, ASSCAP (Application de Saisie et Suivi des Cartes d' Agents Publics)

L'autorité déléguée se connecte à l'application ASSCAP [5]à travers l'intranet Justice :

1. Il se rend sur l'onglet « gestion des cartes ».
2. Il clique sur « faire une demande de carte ».
3. Il renseigne les noms et prénoms du futur titulaire de carte.
4. Il signe électroniquement la demande.
5. La carte est produite et expédiée sur le site de l'autorité d'enregistrement pour remise selon les modalités prévues dans la fiche « remise de carte ».

[5] [5] L'ASSCAP a été déclaré à la CNIL sous le N° 1611140 27 août 2012.
[5]L'ANTAI (Agence Nationale de Traitement Automatisé des Infractions) intervient en tant que fournisseur de l'outil de signature WLSigner.

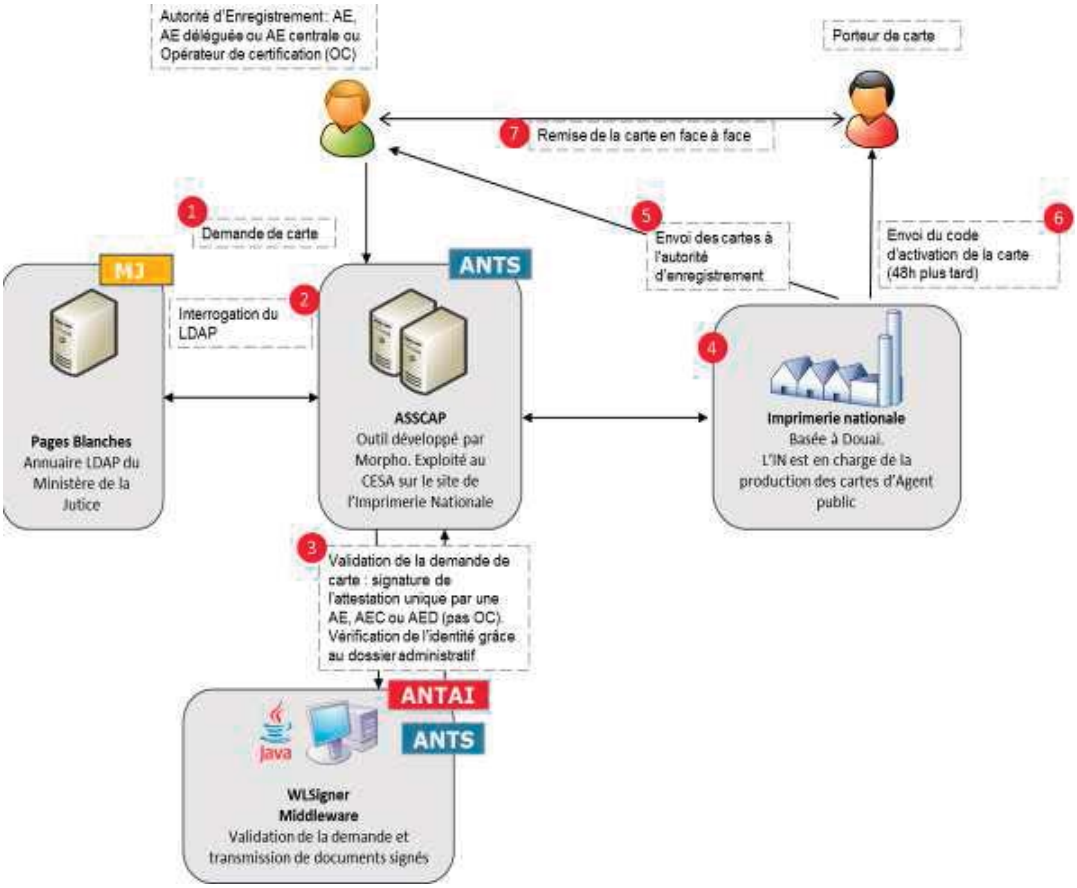

Figure 3 - Schéma macroscopique simplifié de demande d'une carte agent

Demande de révocation d'une carte

Suite à cessation de fonctions, les certificats permettant l'authentification et la signature doivent être révoqués :

1. L'autorité d'enregistrement se connecte à l'application ASSCAP à travers l'intranet justice.
2. Il se rend sur l'onglet « gestion des cartes ».
3. Il clique sur « révoquer une carte ».
4. Il renseigne les nom et prénoms du titulaire de carte.
5. Il signe électroniquement la demande de révocation.
6. Les certificats contenus dans la carte sont révoqués.
7.

Déclaration de la perte ou du vol d'une carte

1. Le titulaire de la carte informe l'Autorité d'enregistrement déléguée ou son mandataire de la perte de sa carte.
2. Le titulaire se connecte à l'application Internet accessible 7 jours sur 7 24h/24, Il s'authentifie grâce à ses quatre secrets (3 questions réponses et un mot de passe) https:\\www.asscap.justice.ants.gouv.fr
3. Il clique sur « déclarer la perte ou le vol d'une carte »
4. Il saisit les informations sur la déclaration de perte ou de vol.
5. Si le titulaire de la carte a oublié ses secrets la demande de révocation peut être faite par l'autorité d'enregistrement déléguée ou son mandataire

6. Les certificats contenus dans la carte perdue ou volée sont révoqués.
7. La commande d'une nouvelle carte est faite par l'autorité d'enregistrement déléguée pour remise selon les modalités prévues dans la fiche « remise de cartes ».

NB : en cas d'oubli ou perte de sa carte par un agent, il appartient à l'application utilisatrice de la carte, de décider en fonction de sa « sensibilité » si :

- de façon **temporaire et exceptionnelle** cet agent repasse en authentification faible (login mot de passe)
- ou bien si l'agent n'a pas d'accès au SI tant qu'il n'est pas en possession de sa carte.

Procéder au renouvellement des certificats

Les certificats contenus dans les cartes ont une durée de vie de trois ans. A cette échéance, il faut procéder à leur renouvellement selon la procédure suivante :

1. Le titulaire de la carte reçoit une alerte lui indiquant que les certificats de sa carte arrivent à expiration.
2. Il se connecte à l'application à travers l'intranet Justice et se rend sur l'onglet « gestion des cartes ».
3. Il clique sur « renouveler des certificats ».
4. Il valide le renouvellement de ses certificats.
5. Le système télécharge les certificats sur la carte.
6. Le titulaire de carte signe une attestation de renouvellement et la stocke dans le parapheur pour contre-signature par l'autorité d'enregistrement déléguée.

La carte a une durée de vie de six ans, le titulaire est informé de la nécessité de la renouveler tous les 3 ans. C'est ensuite l'autorité d'enregistrement déléguée ou son mandataire (OC) qui remet la nouvelle carte au titulaire contre remise de l'ancienne carte qui doit être détruite.

Débloquer une carte suite à la saisie erronée du code PIN ou à l'oubli du code PIN

Afin de contribuer à garantir la confidentialité des échanges et de respecter la réglementation, il n'est plus possible de saisir son code PIN après trois saisies erronées.
Pour débloquer une carte le porteur :

1. Se connecte à l'application de gestion des cartes
2. Sélectionne la fonctionnalité de déblocage du pin.
3. Répond à ses 4 questions secrètes qu'il a renseignées lors du processus de remise.

Si les réponses sont valides, L'application de gestion des cartes déclenche à distance le déblocage du pin. L'opération de déblocage est tracée au niveau de l'application de gestion des cartes.
L'accès à cette fonction ne peut se faire qu'aux heures ouvrées.

Annexe 2 Volumétrie des personnels concernés

La DAP estime la volumétrie à 2000 cartes/an.

Annexe 3 conditions d'utilisation de la carte agent extérieur Justice

ATTESTATION DE REMISE DE CARTE

Je soussigné « Prénom NOM » atteste avoir reçu de « Prénom NOM », autorité d'enregistrement qui signe également la présente attestation, la carte numéro *** dotée d'un certificat d'authentification et d'un certificat de signature.

CONDITITIONS GENERALES D'UTILISATION

Je reconnais être informé(e) que cette carte est personnelle et que mes codes d'authentification et de signature sont strictement confidentiels. En conséquence, je m'engage à ne pas les divulguer. Je m'engage également à ne pas prêter ma carte et à la conserver constamment sous ma garde.

Je m'engage à ne m'authentifier au moyen de cette carte que sur les systèmes d'information en relation avec mon activité professionnelle au sein du ministère de la Justice. Je m'engage à ne signer les décisions judiciaires que sur des applications validées et diffusées par le ministère de la Justice, et dans l'enceinte des locaux du ministère. Je m'engage enfin à ne pas signer de décisions judiciaires à l'aide d'un autre module de signature que celui fourni par le ministère de la Justice.

Je m'engage à vérifier que les informations me concernant dans l'annuaire « Pages Blanches » (http://pagesblanches.intranet.justice.gouv.fr) du ministère de la Justice sont correctes, notamment au niveau de l'affectation, de l'état civil et de l'adresse physique du site auquel je suis rattaché(e).

En tant que récipiendaire de documents signés, je m'engage à vérifier le statut du certificat ayant permis cette signature (en particulier en m'assurant de sa non-révocation en consultant la liste de révocation de l'Autorité de Certification disponible à l'adresse : http://www.justice.gouv.fr/igc/ants/).

En cas d'identification d'une cause possible de révocation de ma carte ou des informations contenues dans ma carte (perte, vol, cessation d'activité, compromission potentielle…), je m'engage à ne plus faire usage de la carte si elle est en ma possession et à déclarer la cause de révocation auprès de mon autorité d'enregistrement ou sur l'un des sites prévu à cet effet (https://www.asscap.justice.ants.gouv.fr ou https://asscap-mjl.interieur.ader.gouv.fr en cas d'accès sur un poste du ministère de la Justice) dès la découverte de cette dernière. En cas de divulgation avérée ou suspectée d'un code PIN, je m'engage à le modifier le plus rapidement possible sur l'un des sites de l'application de gestion des cartes (https://www.asscap.justice.ants.gouv.fr ou https://asscap-mjl.interieur.ader.gouv.fr) en cas d'accès sur un poste du ministère de la Justice) prévu à cet effet.

Je reconnais être informé(e) que sont conservées dans l'application de gestion des cartes des données à caractère personnel (nom et prénoms-) nécessaires à la gestion de la carte remise. Les droits d'accès et de rectification de ces informations (prévus aux articles 39 et 40 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés) s'exercent auprès du service qui a remis la carte.

J'autorise le ministère de la Justice à publier les certificats de ma carte sur l'annuaire ministériel.

Le document de référence concernant l'émission de cette carte et des certificats de clé publique associés est la politique de certification publiée sur le site du ministère à l'adresse www.justice.gouv.fr/igc/ants sous les OID : 1.2.250.1.120.2.2.1.3 et 1.2.250.1.120.2.3.1.3.

LIMITATIONS DE RESPONSABILITE

Le ministère décline toute responsabilité à l'égard de l'usage qui est fait des cartes qu'il a émises dans des conditions et à des fins autres que celles prévues dans la politique de certification disponible sur le site du ministère ainsi que dans tout autre document contractuel applicable associé.

Le ministère décline toute responsabilité quant aux conséquences des retards ou pertes, liés ou non à l'altération ou autres erreurs pouvant se produire dans la transmission de toute télécommunication,

que pourraient subir dans leur transmission tous messages électroniques, lettres et documents. Il ne saurait être tenu responsable, et n'assume aucun engagement, pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant de la présente politique lorsque les circonstances y donnant lieu et qui pourraient résulter de l'interruption totale ou partielle de son activité, ou de sa désorganisation, relèvent de la force majeure au sens de l'Article 1148 du Code civil.

Les tribunaux administratifs sont compétents dans la résolution des conflits.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Avenant n°1 à la convention relative à l'authentification pour l'accès de professionnels de santé et personnels administratifs au système d'information du ministère de la justice

Entre d'une part,

Le Ministère de la Justice, situé 13 Place Vendôme, Paris 1er, représenté par Monsieur Eric LUCAS, Secrétaire général du Ministère de la Justice,

Et d'autre part,

Le Ministère des Affaires sociales et de la santé, situé 14 avenue Duquesne, 75350 PARIS 07 SP, représenté par Monsieur Pierre RICORDEAU, Secrétaire général des ministères chargés des affaires sociales.

Article 1 : Objet de l'avenant

Le présent avenant :

- annule l'article 3
- et modifie le préambule et les articles 5, 8 et 9 de la convention relative à l'authentification pour l'accès de professionnels de santé et personnels administratifs au système d'information du ministère de la justice.

Le préambule et les articles 5, 8 et 9 sont remplacés par les préambule et articles ci-dessous.

Préambule

Le ministère de la justice, a engagé un processus de dématérialisation de ses procédures que pilote son secrétariat général.

Les services d'authentification et de signature (l'infrastructure de gestion de clefs et la carte à puce) du Ministère de la Justice ont obtenu la certification *** au sens du RGS le 26 novembre 2012 ainsi que l'inscription sur la Trust-service Status List (TSL), liste européenne qui recense les autorités de certification de confiance.

Le ministère de la Justice devait choisir la certification *** puisque les magistrats émettent des jugements, ordonnances et arrêts, qui sont des actes authentiques dont la signature doit être présumée fiable au sens de l'article 1316-4 du code civil**.**

Le Ministère de la Justice n'ayant qu'une seule IGC, toutes les cartes « Justice » sont de ce fait soumises aux règles du RGS *.**

Pour rappel, le Référentiel Général de Sécurité (RGS, décret 2010-112 pris pour l'application des articles 9, 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) impose une vérification de l'identité, qualité et fonctions du porteur de carte ainsi qu'une remise en face à face par une autorité hiérarchique, dite autorité d'enregistrement.

Le ministère de la justice a ainsi conçu sa chaîne de remise de cartes (chaîne de confiance) en s'appuyant sur les services de gestion des ressources humaines qui sont habilités à accéder au dossier administratif des agents.

Dans les établissements pénitentiaires, du personnel d'autres instances que la direction de l'administration pénitentiaire (DAP), **dont des personnels des unités sanitaires rattachées aux établissements de santé**, sont rapidement appelés à accéder au système d'information « GENESIS » qui gère le détenu en établissement pénitentiaire.

Pour répondre aux exigences de la CNIL et du Conseil d'Etat, une authentification forte est progressivement mise en place pour sécuriser l'accès aux données sensibles à caractère personnel, traitées par le système d'information du Ministère de la Justice.

Il s'agit de remplacer la procédure de connexion par « login-mot de passe » par l'usage d'une carte à puce contenant un certificat d'authentification de l'agent.

Aussi, outre les personnels Justice, et en l'absence d'un système interministériel de fédération d'identité, il convient que les personnels concernés professionnels de santé et personnels administratifs, titulaires ou contractuels, soient également dotés de cartes à puce.

Par convention ces personnels sont désignés sous le terme générique d'agents.

Il s'agit d'authentifier ces personnels selon les modalités décrites à l'article 5 ci-après par un certificat remis en face à face, de vérifier leur identité et leur appartenance aux professions de santé, et non de définir un profil leur donnant accès à certaines informations du SI Justice.

C'est un projet à multiples dimensions : organisationnelle, stratégique et technique.

Article 3 - Le Système cible

Cet article est supprimé.

Article 5 - L'authentification des agents concernés

Le Ministère de la Justice procèdera à l'authentification des agents concernés travaillant en établissement pénitentiaire et leur délivrera des « cartes d'agents Justice extérieurs » embarquant un certificat d'authentification relevant de l'IGC[1] Justice.

A cette fin, des mesures organisationnelles doivent être prises afin de permettre à tout instant de connaître l'identité d'un utilisateur de certificat « Justice » porteur d'une carte d'agent « extérieur ». Ces mesures sont déclinées ci après.

[1] Infrastructure de gestion de clefs

Pour authentifier l'agent « extérieur » habilité, le chef de l'établissement pénitentiaire devra être informé par le directeur de l'établissement de santé de rattachement :

- de l'identité de l'agent concerné,
- de sa position administrative le cas échéant,
- de sa profession,
- et de sa fonction,

selon des modalités précisées par une instruction conjointe des deux ministères concernés.

Le Ministère de la Justice au vu des données numériques vérifiées par l'établissement de santé, identifiera ces agents dans son annuaire LDAP sous l'arborescence « agents extérieurs ». Ceux-ci doivent être dotés d'une boite à lettres électronique (BAL) au format de leur employeur, à défaut, au format @externes.justice.gouv.fr.

Le chef d'établissement pénitentiaire, autorité d'enregistrement, ou son délégué, procèdera à la remise en face à face de la carte Justice à l'agent habilité, sur présentation de sa carte d'identité et selon les formalités décrites dans le référentiel général de sécurité.

Les justificatifs sont conservés au dossier d'habilitation de l'agent par le chef d'établissement qui le détient.

Le dossier d'habilitation sera conservé 5 ans après la cessation de fonctions en établissement pénitentiaire de l'agent concerné et la restitution de la « carte agent extérieur justice », afin de répondre aux exigences de traçabilité de la CNIL et du Conseil d'Etat.

Voir annexe 1 de la convention : présentation de la carte agent Justice et des procédures liées.

Article 8 - Conditions financières

Les cartes sont fournies et renouvelées à titre gratuit par le Ministère de la Justice.

Article 9 - Durée de la convention - modalités de dénonciation

Cette convention est conclue pour une durée d'un an reconductible tacitement.

Elle peut être révisée et amendée à tout moment à la demande de l'une ou l'autre des parties.

Elle peut être dénoncée par l'une ou l'autre des parties, chaque année, 3 mois avant la date anniversaire de sa signature.

Un comité de suivi de la convention est mis en place à compter de la signature du présent avenant. Il se réunira annuellement.

Fait en deux exemplaires originaux, à Paris le 4 juillet 2016

Pour le ministre et par délégation,	Pour la ministre et par délégation,
Signé	Signé
Eric LUCAS	Pierre RICORDEAU
Secrétaire général du ministère de la justice	Secrétaire général des ministères chargés des affaires sociales