7. INFORMATIQUE

7.1. Outils de sécurisation de l'accès aux services du système d'information de la branche famille (Hab Tiers et Hab Nims)

DECLARATIONS

HAB TIERS - HABNIMS

Outils de sécurisation de l'accès aux services du système d'information de la branche Famille

DECLARATIONS

HAB TIERS - HABNIMS

Outils de sécurisation de l'accès aux services du système information de la branche Famille

Ces deux dossiers nationaux portent sur les nouveaux outils destinés à sécuriser l'accès au réseau informatique de la branche Famille en permettant une gestion uniformisée dans l'ensemble des Organismes de l'habilitation des utilisateurs et de la traçabilité des accès aux services du système d'information.

- Hab tiers assure la gestion de l'accès par les tiers,
- Habnims permet la gestion de l'accès par les personnels.

Notification Cnil

La Cnil a délivré des récépissés de déclaration :

→ pour Habtiers, le 26 mars 2008 ; le traitement est enregistré sous la référence 1184561.

→ pour Habnims, le 12 juin 2009 : numéro d'enregistrement 1338960.

Obligations des Organismes

Aucune formalité n'est requise.

En ce qui concerne l'obligation d'information des personnes, les modalités sont précisées à la rubrique des dossiers « mesures prises pour faciliter l'exercice du droit d'accès ».

DECLARATIONS

HAB TIERS

Outil de sécurisation de l'accès par les tiers
aux services du système d'information de la branche famille

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS
75340 PARIS cedex 07
Tél : 01 53 73 22 22
Fax : 01 53 73 22 00
www.cnil.fr

Déclaration NORMALE

1

PREMIERE DECLARATION	X
DECLARATION DE MODIFICATION	☐
DECLARATION DE SUPPRESSION	☐

Préciser dans ce cas le n° d'enregistrement du traitement que vous souhaitez modifier ou supprimer : ☐☐☐☐☐☐☐☐

Cadre réservé à la CNIL
N° d'enregistrement ☐☐☐☐☐☐☐☐
☐ D
☐ DT
☐ A

2 Organisme déclarant

Statut juridique : **Secteur public** X **Secteur privé** ☐
Nom ou Raison Sociale : Caisse Nationale des Allocations Familiales CNAF..... N° SIREN **180035065**
Adresse **32 Avenue de la Sibelle** ..... N° APE **753C**
Code postal **75685** Ville **Paris cedex 14**.....Téléphone **01.45.65.52.52**

3 Service ou organisme chargé de la mise en œuvre du traitement

Si le nom et les coordonnées sont identiques à ceux de l'organisme déclarant, cochez ☐ sinon complétez ci-dessous
Nom ou RS ... **Organismes de la branche Famille (Cnaf, Certi, Caf)**.....
Adresse.....
Code postal..... Ville ..... Téléphone .....

4 Service ou organisme auprès duquel s'exerce le droit d'accès *

Si le nom ET les coordonnées sont identiques 1) à ceux de l'organisme déclarant, cochez ☐ 1
2) à ceux du service chargé de la mise en œuvre, cochez X☐ 2 sinon complétez ci-dessous
Nom ou RS .....
Adresse .....
Code postal ☐☐☐☐☐ Ville ..... Téléphone ☐☐☐☐☐☐☐☐☐☐

5 Traitement déclaré

Nom du logiciel ..... **Année de mise en œuvre : 2006**
Population concernée (catégories de personnes concernées et nombre approximatif) **2 000**.....
Finalités principales : Gestion des habilitations et traçabilité des accès aux services du système d'information des Organismes de la branche Famille par les tiers .....

6 Transferts d'informations hors de l'Union européenne **

Existe-t-il des transferts d'informations hors de l'Union européenne ? OUI ☐ NON X
Si vous répondez « oui », précisez quels sont les pays concernés .....

7 Personne à contacter

Nom ...**FLORIMOND**.....Prénom ...**Jean**.....Fonction...**Directeur du projet**.....
Tél : **04 93 95 59 66** fax : **04 92 96 09 42** ..... Adresse électronique. **jean.florimond@cnedi06.cnafmail.fr**.....

8 En cas de déclaration de suppression signer ici et ne pas compléter la feuille 2

Nom du signataire ..... **Signature**
Fonctions l'habilitant à signer .....
Date **Le** (JJ/MM/AAAA) / /

*** Rubriques à compléter par des annexes. ** Si la réponse est oui, cette rubrique est à compléter par une annexe, dont un modèle est disponible sur le site de la CNIL ou sur simple demande.**

Les informations portées sur ce formulaire et figurant en gras sont obligatoires. Elles font l'objet d'un traitement informatisé à la CNIL et sont destinées aux membres et services de la Commission chargés de l'instruction de votre dossier et au public désireux de s'informer de l'existence d'un fichier dans les conditions prévues à l'article 31 de la loi du 6 janvier 1978. Vous pouvez exercer votre droit d'accès aux informations qui vous concernent en vous adressant à : la CNIL,21 rue Saint-Guillaume 75340 PARIS cedex 07

9 *Fonctions de l'application* *

1	**Instruction des demandes d'habilitation**
2	**Gestion du processus d'habilitation**
3	**Administration de la sûreté**
4	**Contrôle et audit des accès au système d'information**
5	**Publication des services applicatifs du système d'information**
6	
7	
8	
9	

10 *Sécurités et secrets*

Mettez-vous en place des règles permettant de contrôler l'accès à l'application ?
OUI X 1 NON ☐ 2
Prenez-vous des dispositions pour protéger votre réseau des intrusions extérieures ?
OUI X 1 NON ☐ 2
Les données elles-mêmes font-elles l'objet d'une protection particulière (anonymisation, chiffrement, …) ?
OUI X 1 NON ☐ 2

11 Catégories de données enregistrées *

X	A	Données d'Identification (nom, prénoms sexe, initiales, n°s d'ordre, date et lieu de naissance…)	☐	I	Moyens de déplacement des personnes
☐	B	NIR, N° de Sécurité Sociale ou consultation du RNIPP	X	J	Utilisation des médias et moyens de communication
☐	C	Situation familiale	☐	K	Données à caractère personnel faisant apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques, religieuses ou les appartenances syndicales des personnes
☐	D	Situation militaire	☐	L	Données biométriques
☐	E	Formation – Diplômes - Distinctions	☐	M	Santé, données génétiques, vie sexuelle
	F	Adresse, caractéristiques du logement	☐	N	Habitudes de vie et comportement
X	G	Vie professionnelle	☐	O	Informations en rapport avec la police
☐	H	Situation économique et financière	☐	P	Informations relatives aux infractions, condamnations ou mesures de sûreté

12 Catégories des destinataires

	Catégories des destinataires	Catégories d'informations fournies *															
		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	**Resp. habilitations (Mandataire du tiers)**	X	☐	☐	☐	☐	☐	X	☐	☐	X	☐	☐	☐	☐	☐	☐
2	**Administrateur de l'organisme de la branche**	X	☐	☐	☐	☐	☐	X	☐	☐	X	☐	☐	☐	☐	☐	☐
3	**Directeur / Agent comptable /délégataire**	X	☐	☐	☐	☐	☐	X	☐	☐	X	☐	☐	☐	☐	☐	☐
4	**Responsable sûreté**	X	☐	☐	☐	☐	☐	X	☐	☐	X	☐	☐	☐	☐	☐	☐
5		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
6		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
9		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
10		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

13 Interconnexion, mise en relation, rapprochement **

Le traitement a pour objet l'interconnexion de fichiers dont les finalités principales sont différentes ?
OUI X 1 NON 2
Le traitement a pour objet l'interconnexion de fichiers dont les finalités correspondent à des intérêts publics différents ?
OUI ☐ 1 NON X 2
Les données peuvent- elles êtres cédées, louées, échangées à des fins commerciales ?
OUI ☐ 1 NON X 2

14

Nom du signataire : Frédéric MARINACCE
Fonctions l'habilitant à signer Directeur des Prestations familiales
Date : 17 juillet 2006
Signature

*** Rubriques à compléter par des annexes. ** Si la réponse est oui, cette rubrique est à compléter par une annexe, dont un modèle est disponible sur le site de la CNIL ou sur simple demande.**

CNAF

Finalités principales et fonctions du traitement
Complément des rubriques 5 et 9

Dans le cadre des relations partenariales, tant avec les autres branches de l'institution qu'avec d'autres tiers comme les conseils généraux, les organismes financiers, bailleurs,l'UNEDIC etc... , la branche famille se propose de mettre en place un nouveau dispositif :

- pour permettre aux tiers d'accéder avec plus de facilité au système d'information quand cela est nécessaire, quel que soit le mode de communication d'informations prévu pour ces destinataires,

- pour réaliser des interconnexions entre système d'information avec les autres organismes de protection sociales,

- pour faciliter à certains d'entre eux l'accès aux services auxquels ils ont besoin,

- pour gérer et contrôler avec une bonne visibilité l'ensemble des protocoles ou conventions régissant les échanges au travers d'une dématérialisation intégrée et sécurisée.

Le dispositif consiste à attribuer une habilitation aux utilisateurs tiers pour accéder aux services mis à leur disposition et à consigner les données contributives dans un annuaire : c'est l'annuaire des tiers.

Bien entendu, avant leur mise en œuvre, les communications d'informations nominatives aux tiers doivent avoir fait l'objet des formalités auprès de la CNIL soit au niveau national, soit par les organismes locaux, pour des traitements spécifiques.

Nota : La gestion des habilitations et de la traçabilité des accès au système d'information par les personnels des Organismes de la branche Famille fait l'objet d'un autre dossier de déclaration dont la dénomination est HABNIMS.

1. Les finalités

Le dispositif comporte :

♦ **Du côté tiers**

- Un outil de gestion des habilitations des utilisateurs du tiers :

  Il est à l'usage exclusif du Responsable des habilitations (Mandataire du Tiers).
  Son accès nécessite une identification formelle du Tiers au moyen d'un dispositif d'authentification forte de type 'carte à puce' (agréé MINEFI).

  Il permet :

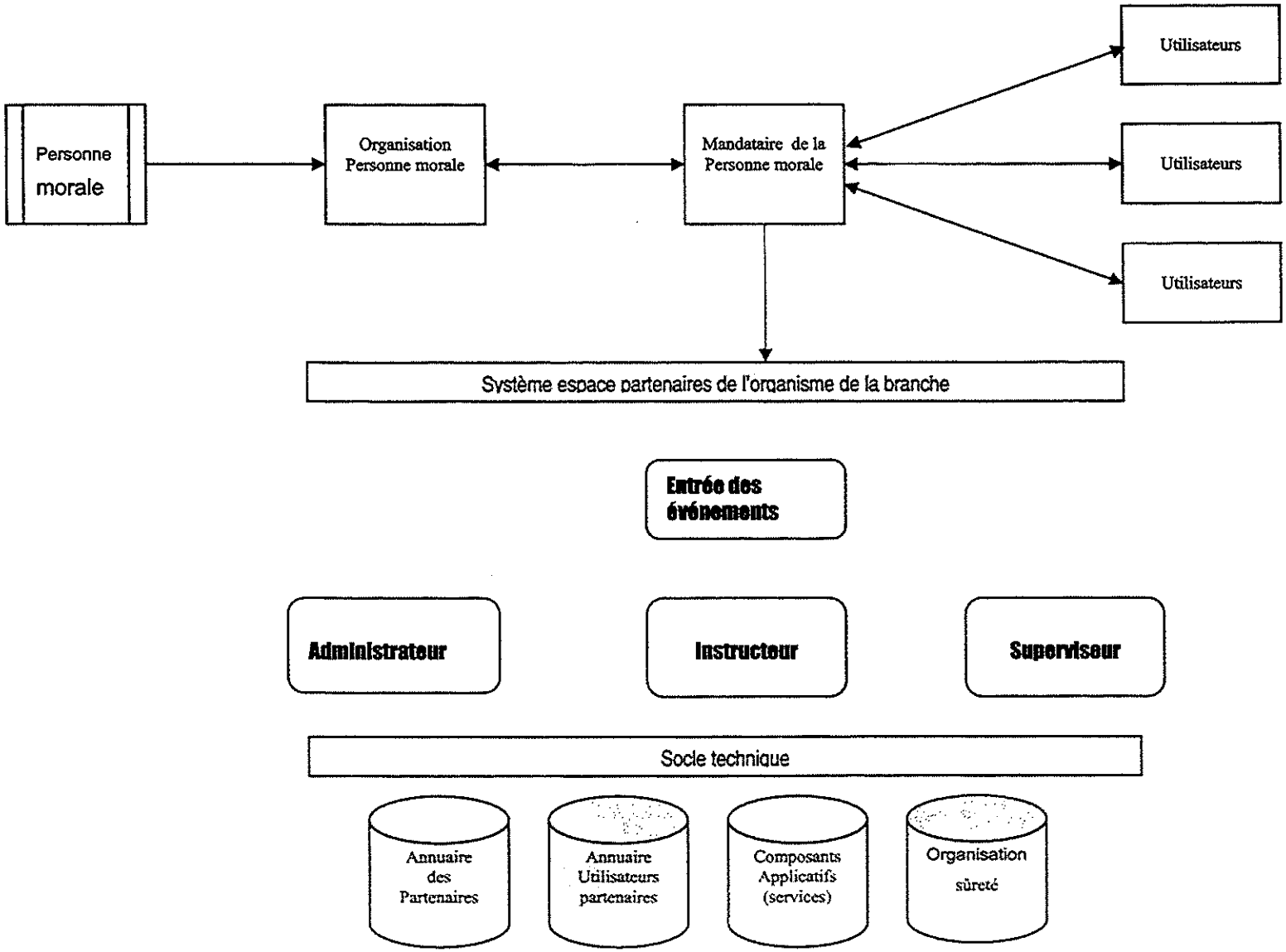
  - la prise en compte des événements organisationnels dans les structures de la personne morale (Tiers), et des événements inhérents aux personnes physiques, communiqués par le Mandataire (suspension de l'activité ou remplacement, changement de nom, etc...)
  - la détermination des services auxquels l'Utilisateur est habilité.
  - d'avoir la possibilité d'un contact direct avec chaque utilisateur sous sa responsabilité.

♦ **Du côté de l'organisme de la branche**

- Un outil de mise en œuvre des modalités d'accès au portail de l'organisme de la branche qui permet :
  - l'autorisation des accès aux Utilisateurs des Tiers préalablement habilités dans l'annuaire par l'authentification de leur nom, prénom et mot de passe.

- Un outil d'instruction et de supervision du processus d'habilitation pour :
  - la prise en compte des modifications concernant les informations du tiers (changement de nom, d'adresse, cessation d'activité ...),
  - la prise en compte des événements organisationnels du tiers et ayant un impact sur les habilitations d'un de ses mandataires ou utilisateurs (affectation de mission ou remplacement, changement d'adresse, de nom, de téléphone, de e-mail, ...),
  - la validation des services correspondants à la nature de la demande du tiers,
  - s'assurer que ces services appartiennent à l'ensemble des services applicatifs référencés et soumis à habilitation,
  - l'inscription de l'Utilisateur de la personne morale dans l'annuaire des tiers.
- Un outil de surveillance et d'audit permettant :
  - de s'assurer du bien fondé de l'activité des utilisateurs en fonction de leurs devoirs et engagements professionnels sans violation des libertés fondamentales,
  - de fournir en cas de litige, la preuve d'une utilisation illicite,
  - à l'utilisateur de s'assurer que ses propres moyens d'accès sont respectés.

Schéma général du processus d'habilitations des Tiers

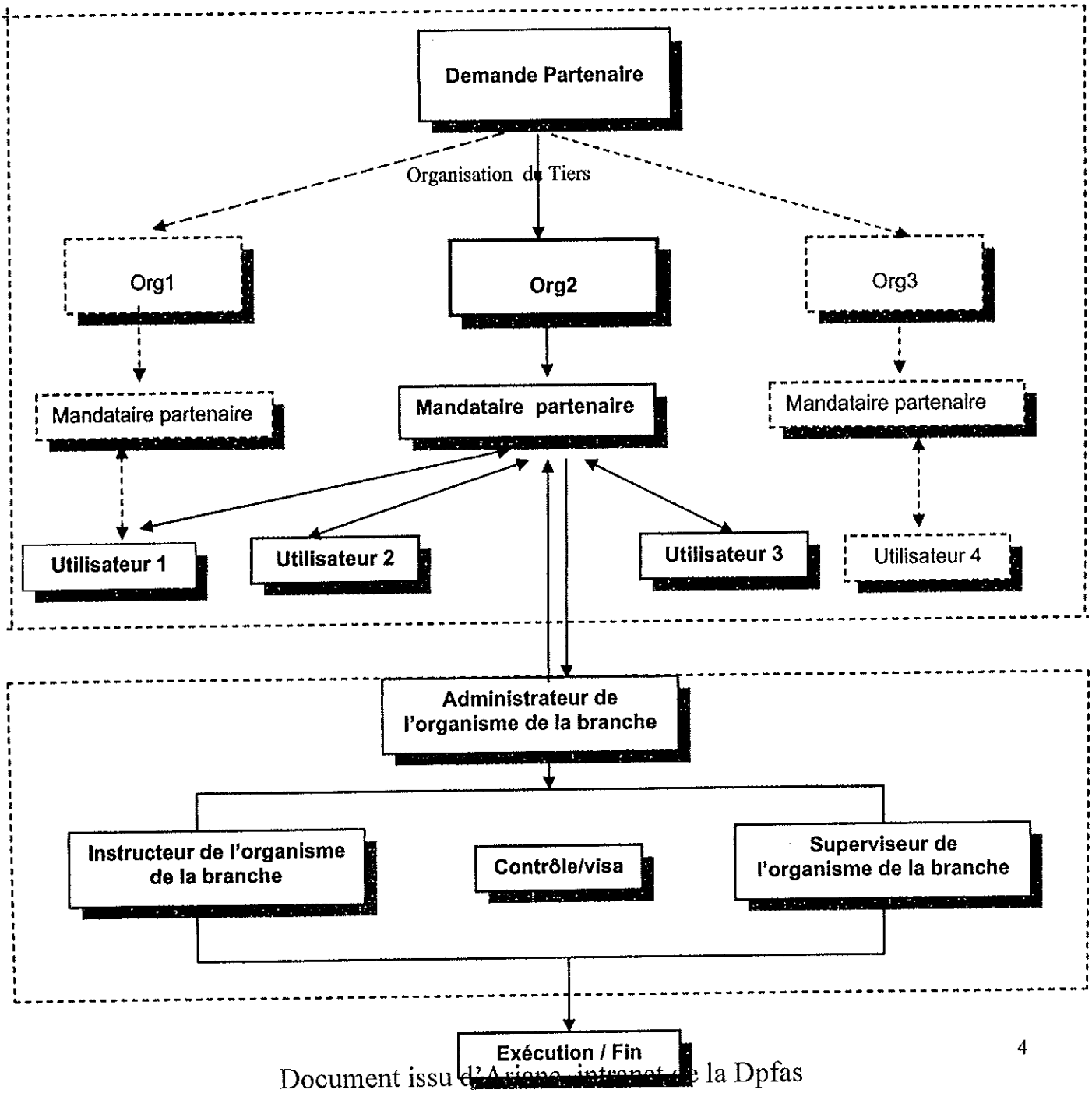


2. Les fonctions du traitement

2.1. Du côté tiers

2.1.1 Un outil de gestion de la demande d'habilitation permet au tiers ayant un ou plusieurs pôles d'intérêt dans l'organisme de la branche de disposer d'un ou plusieurs mandataires selon son organisation propre.
Le mandataire est chargé de formaliser la demande des utilisateurs relevant de sa responsabilité.
Le tiers ou mandataire indique pour chaque utilisateur de sa dépendance le ou les services sollicités auprès de l'organisme de la branche. Il a en charge d'apporter à la connaissance de l'administrateur de l'organisme de la branche toute modification qui peut intervenir dans le dossier de tout utilisateur relevant de sa responsabilité.

Le schéma ci-après décrit les différents rôles associés aux étapes du processus général.



- 2.1.2 Un outil de mise en relation et de reconnaissance permet au mandataire de la personne morale d'être seul à pouvoir effectuer les demandes ou des modifications dans le dossier des utilisateurs qui relèvent de son autorité. Il dispose pour ce faire d'un moyen de connexion doté d'une **carte à puce individuelle**. Il recevra à l'issue de la demande un accusé de réception de l'administrateur qui est son interlocuteur auprès de l'organisme de la branche pour la formulation des demandes.

  Une procédure de substitution sera mise en place en cas de perte de la carte à puce en attendant l'attribution d'une nouvelle carte.

  Une fois que la demande est agréée, chaque utilisateur reçoit directement par voie de messagerie le premier mot de passe qui lui est attribué par le système de sécurité de l'organisme de la branche.

Sont décrits ci-dessous les différents rôles associés aux étapes et les informations traitées à chacune des étapes.

Etape n°1 - Demande du tiers

Informations sur la personne morale:

- Nom ou Raison sociale
- Siret
- Adresse
- Région
- Téléphone
- Fax
- E-mail
- Fonction - web
- Dénomination

Informations sur le mandataire de la personne morale

- Nom
- Prénom
- N° Téléphone
- Adresse professionnelle
- Mot de Passe
- E-mail
- Rôles
- Services sollicités
- Date de la demande

Informations sur les utilisateurs dépendant du mandataire

- Nom
- Prénom
- Mot de passe
- Adresse professionnelle
- téléphone
- E-mail

La demande est transmise automatiquement dans l'espace de l'administrateur de l'organisme de la branche pour réception et vérification de complétude et pour un contrôle de forme.

2.2. Du côté de l'organisme de la branche

2.2.1 Un outil de réception des demandes et de contrôle permet de diriger toutes les demandes faites par les tiers vers l'espace réservé à l'administrateur de l'organisme de la branche.

Celui-ci exerce un contrôle de forme sur les informations transmises et adresse un accusé de réception avec ou sans observation au mandataire de la personne morale.

Les dossiers jugés complets et sans observation sont estampillés et passent à l'instruction.

Etape n°2 - Réception de la demande du tiers

L'administrateur est l'interlocuteur privilégié du représentant du tiers. Il est en relation avec le mandataire du tiers et lui apporte tout complément de renseignement utile pour faire ses demandes d'habilitations. Il est également l'intervenant de premier niveau pour résoudre tout problème technique concernant le dispositif utilisé par le tiers. L'administrateur avalise les demandes de son espace de travail et celles-ci sont transmises à l'instructeur des demandes.

Toute action exercée sur le dossier est tracée.

2.2.2 Un outil d'instruction et de supervision du processus d'habilitation

L'instruction consistera à examiner de plus près la cohérence entre le profil de l'utilisateur et les services dont les accès lui sont demandés par un des Délégués du Directeur de l'organisme.

Quant à la supervision, elle obéit à la même délégation à la différence que celle-ci relève de l'autorité de l'Agent comptable de l'organisme de la branche.

Toutefois, dans les deux cas, selon l'organisation de l'organisme de la branche et de la délégation, on peut avoir la possibilité de ré acheminer une demande pour pouvoir la router vers un autre instructeur ou superviseur (ou un groupe d'instructeurs ou superviseurs).

Il peut arriver également le cas où les mêmes personnes cumulent les deux délégations.

Etape no. 3 - L'instruction - supervision -

Acteur : **Instructeur - superviseur** (selon l'organisation de l'organisme : Responsable / Agence Comptable / Direction)

Cette étape est obligatoire pour l'inscription des utilisateurs tiers.
Le nombre de niveaux de supervision peut varier de 1 à n. (fonction du paramétrage général)

A l'issue de cette étape, il y a :

- soit refus avec indication du motif de refus, la demande peut faire un va et vient entre l'instructeur et le superviseur ou elle est retournée à la personne morale par le canal de son mandataire,

- soit accord : la demande est validée, un visa est apposé sur la demande pour cette étape, la demande poursuit son circuit.

Une fois les différentes étapes d'instruction et de supervision franchies, la demande est transmise pour exécution/fin.

Etape no. 4 - L'exécution -

Acteur : **Exécutant** (système informatique)

Cette étape permet de déclencher les opérations d'inscription ou de mise à jour automatique des annuaires et bases de données.

A l'issue de cette étape, la demande est exécutée. Une notification est adressée aux personnes concernées par leur e-mail.

2.3. L'outil d'administration de la Sûreté spécifique aux tiers

Il doit prendre en charge entre autres :

- la prise en compte des évolutions liées à une nouvelle version suite à publication dans le Répertoire des services tiers (R.D.S.T) les ajouts ou les suppressions de fonctions applicatives dans un service applicatif, à intégrer dans des tâches applicatives déjà définies, l'intégration d'un service au sein de la B.O.S.T (Base d'organisation de la sûreté des tiers).

- la journalisation de toutes les mises à jour.

2.4. L'outil de surveillance et d'audit

Il est mis en place une fonction de traçabilité permettant d'auditer les connexions au système d'information

Acteurs et rôles

Les acteurs intervenant dans le cadre du processus d'habilitation côté tiers sont :

- L'autorité de tutelle de la personne morale (Président, Directeur, ...)
- Le mandataire de la personne morale
- Les utilisateurs

Les acteurs intervenant dans le cadre du processus d'habilitation interne de la branche sont :

- L'administrateur de l'organisme de la branche
- Le Directeur et l'Agent Comptable de l'organisme
- Le responsable de la sûreté
- Le référent technique informatique

Leurs rôles sont définis selon le tableau suivant : Tiers d'une part et Organisme de la branche d'autre part

Côté tiers

Acteurs et rôles	Pilotage	Expertise	Exécution	Surveillance et audit
Président ou Directeur de la personne morale	▪ Il est responsable de la structure organisationnelle de son organisme, ou de son association, et du bon fonctionnement du système mis en place	Propre au tiers	▪ Il peut superviser l'attribution des habilitations	▪ Il s'assure de la mise en œuvre de la sécurité du dispositif mis en place et atteste du bon déroulement des opérations telles qu'elles sont prévues en accord avec son mandataire auprès de l'organisme de la branche
Mandataire de la personne morale	▪ Il est le représentant de la personne morale auprès de l'organisme de la branche. ▪ Il est responsable de la collecte des informations nécessaires des utilisateurs sous sa dépendance pour l'attribution des droits d'accès. ▪ Il transmet les modifications susceptibles de subvenir dans les informations qu'il a pu transmettre.	▪ Il est le référent de la personne morale pour spécifier les services de chacun des utilisateurs qui sont sous sa responsabilité. ▪ Il est l'interlocuteur de l'administrateur de l'organisme de la branche pour signaler tout problème du système	▪ Il supervise la saisie des informations des utilisateurs en vue d'une demande d'habilitation. ▪ Il fait un usage exclusif et personnel de sa carte à puce par laquelle il a accès au système des demandes	▪ Il s'assure que ses utilisateurs ont chacun les services qu'il a sollicités pour eux et signalera tout dysfonctionnement à l'administrateur de l'organisme de la branche
Utilisateur tiers			▪ Il se conforme aux directives de son responsable. Il indique à son responsable tout problème rencontré dans l'exercice de sa fonction à son responsable ▪ .Il fait un usage strictement personnel de son mot de passe et change celui-ci aux fréquences exigées par le système et doit respecter les consignes de sécurité.	▪ Il peut vérifier sa dernière connexion au système d'information

Côté Organisme de la branche

Acteurs et rôles	Pilotage	Expertise	Exécution	Surveillance et audit
Directeur et Agent Comptable	▪ Ils sont responsables de la sécurité ▪ Ils définissent les consignes générales de sécurité ▪ Ils définissent les règles d'attribution des habilitations en application des délégations attribuées ▪ Ils définissent l'organisation liée au dispositif de surveillance et d'audit		▪ Ils peuvent superviser l'attribution des habilitations	▪ Ils s'assurent de la mise en œuvre de la sécurité
Instructeur ou superviseur Suivant l'organisation de l'organisme, il peut être le Représentant du Directeur ou le Délégué de L'Agent comptable	▪ Il supervise et définit les modalités d'utilisation des services ▪ Il détermine les habilitations adaptées aux utilisateurs.			▪ En fonction des délégations de la Direction de l'organisme, il peut être conduit à exploiter des journaux d'accès au système d'information des utilisateurs
Administrateur de l'organisme Désigné pour son niveau d'expertise ou de maîtrise du système mis en place, il est le correspondant du Mandataire de la personne morale. Il gère l'espace d'accueil des demandes.		▪ Il vérifie la complétude des dossiers de demandes et apporte son assistance à distance au mandataire de la personne morale.	▪ Il s'assure de la bonne mise en œuvre des modalités d'usage du système	

Sécurité de la Base d'organisation de la sûreté des tiers (BOST)

Il est mis en place une base spécifique contenant pour chaque utilisateur, les services auxquels il peut avoir accès en relation avec la base de données de l'annuaire des tiers.

CNAF

DISPOSITIF DE SURETE DES ACCES
AU SYSTEME D'INFORMATION
PAR LES TIERS

Mesures prises pour faciliter l'exercice du droit d'accès
Complément de la rubrique 4

Dans le cadre du présent traitement, il appartient aux responsables partenaires d'informer leurs personnels concernés sur l'existence d'un dispositif de sûreté des accès aux services mis à leur disposition par les Organismes de la Branche Famille.

Conformément aux articles 39 et suivants de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les personnes doivent être informées qu'elles bénéficient d'un droit d'accès et le cas échéant de rectification aux informations qui les concernent, et qu'elles peuvent exercer ce droit auprès de l'Organisme visé dans la demande d'habilitation.

Un message sur cette obligation d'information sera notifié, via la messagerie électronique et/ou par courrier, individuellement à toute personne, lors de son inscription dans l'annuaire des tiers.

CNAF

Sécurités
Complément de la rubrique 10

La finalité du nouveau dispositif est d'assurer et d'organiser la sécurisation des droits d'accès octroyés aux partenaires des organismes de la branche afin d'accéder à des services mis à leur disposition. Le processus d'habilitation en constitue l'élément essentiel. Mais la sécurité du processus et la confidentialité des données tracées est aussi garantie par un certain nombre de mécanismes liés aux accès à ces services.

L'authentification des utilisateurs

Selon la responsabilité dans la structure organisationnelle du partenaire, l'authentification de l'Utilisateur peut être faite à l'aide d'une carte à puce et ou de l'identité associée à un mot de passe.
Dans le respect des textes réglementaires et de la délégation du Directeur ou de l'Agent Comptable de l'organisme de la branche, la carte à puce, l'identité et le mot de passe sont les propriétés d'une personne et d'une seule qui en devient le propriétaire et seul responsable.

La carte à puce

Elle est la propriété exclusive du détenteur de droit.

L'identité

C'est le nom et prénom associé à la raison sociale de la personne morale d'appartenance.

L'identité (cas d'homonymie)

En cas d'homonymie, l'e-mail de l'utilisateur servira pour son identification univoque.

La carte à puce et le mot de passe

La carte à puce et ou Le mot de passe associé à l'identité permet d'authentifier l'utilisateur qui se connecte aux services.

L'initialisation du mot de passe

Un mot de passe prédéfini est initialisé à la création dans l'annuaire des partenaires.
A la première connexion de l'utilisateur, il est demandé obligatoirement à celui-ci de modifier ce mot de passe initial.

La structure du mot de passe

Dans le respect des préconisations de la CNIL, la longueur minimale du mot de passe est fixée à six caractères alphanumériques.

La gestion des mots de passe

La gestion des mots de passe est assurée par l'utilisateur qui introduit sur demande du système, à expiration de celui-ci ou à sa convenance, un nouveau mot de passe obligatoirement différent au moins des trois précédents.

Le délai de rétention du mot de passe

Le délai de rétention du mot de passe est fixé au maximum à 45 jours, de date à date, passé ce délai le mot de passe est expiré et l'utilisateur est invité à le changer.

Délai minimum de changement entre les mots de passe

Le délai minimum toléré entre les changements de mot de passe est de 3 jours.

Réutilisation du mot de passe

Le nouveau mot de passe généré est obligatoirement différent des trois derniers mots de passe précédemment introduits.

La protection des mots de passe

Dans le but de garantir la confidentialité, les fichiers contenant les mots de passe sont protégés (cryptographie ou chiffrement).

La récupération d'un mot de passe oublié

L'utilisateur qui a oublié son mot de passe doit contacter le mandataire de la personne morale qui en avise l'administrateur le l'organisme de la branche pour attribution d'un nouveau mot de passe qui est obligatoirement changé par l'utilisateur lors de la connexion de celui-ci à son poste de travail.

La période d'inactivité

Après une période d'inactivité mesurée du code utilisateur, une déconnexion automatique sera effectuée par le système.

Le blocage de l'identifiant après un délai de non utilisation

Le système enregistre automatiquement la date de dernière connexion de chaque utilisateur. Les détections de non connexion sur une longue durée (45 jours minimum) entraîneront un blocage de l'accès aux services.

La sécurité des accès

La sécurité des accès est assurée par le système dès la connexion après authentification de l'utilisateur (carte à puce et ou identité et mot de passe) un message apparaît sur le poste de travail indiquant : ***la date et l'heure de la dernière connexion sous le même code utilisateur et mot de passe.***

Annexe sur les sécurités

[Note : plusieurs cases peuvent être cochées en réponse à une question]

A. L'architecture informatique, les sécurités et sauvegardes.

1. Description du système informatique. Il est constitué :

- ☐ d'un parc de micro-ordinateurs sans serveur central
- ☐ d'un mini/petit serveur d'entreprise
- X d'un ensemble de serveurs au sein de l'organisme ou externalisés
- X d'un gros ordinateur au sein de l'organisme ou externalisé
- ☐ par l'hébergement chez un fournisseur internet. Nom de l'hébergeur : _____
- ☐ autre architecture informatique : _____

Nom(s) du (des) fournisseur(s) et du (des) modèle(s) : **ZOS 390 SERIES**
Nom(s) du (des) système(s) d'exploitation : **2 Linus , ZOS**

2. Nature du réseau informatique permettant les échanges d'informations en interne.

- ☐ aucun réseau (par ex. des micro-ordinateurs isolés)
- X un réseau local d'entreprise. Nom (par ex. Netware) : **LAN**
- X un serveur interne accessible de l'extérieur via internet
- ☐ un hébergement externe accessible via internet.
- ☐ un extranet mis en œuvre par un Réseau Privé Virtuel (RPV ou VPN en anglais). Nom du dispositif technique ou du prestataire : _____
- ☐ des lignes privatives louées à un opérateur de télécommunication
- ☐ utilisation de technologies sans contact. Nom (WiFi par ex.) : _____
- ☐ utilisation de postes de travail nomades (micro-ordinateurs par ex.)
- ☐ autre type de réseau : _____

Nombre total de postes de travail : **2000**

Eventuellement, nom(s) du (des) logiciel(s) réseau(x) ou du moniteur de télétraitement :
_____

3. En cas d'échanges d'informations avec des partenaires ou organismes extérieurs, préciser le(s) procédé(s).technique(s) utilisé(s) :

- ☐ support magnétique ou analogue (disque, bande, cd-rom, clé USB,..) : _____
  Chiffrement : OUI NON
- X messagerie internet. Chiffrement : **OUI**
- X transfert de fichier par internet. Chiffrement : **OUI**
- ☐ transfert via un réseau privatif. Nom éventuel du réseau : _____.
  Chiffrement : OUI NON
- ☐ autre procédé : _____.
  Chiffrement : OUI NON

4. Sécurité (protection) physique des locaux et équipements, sauvegarde du système informatique.

X Décrire brièvement les dispositifs/procédures permettant d'assurer la sécurité physique des locaux et équipements informatiques (badge d'accès, gardiennage etc.) :

Surveillance 24 h / 24 h sous Camera Vidéo / Sécurisation des salles – Serveur par carte magnétique

X Mesures assurant la sauvegarde du système informatique
- Type de support utilisé : **Bandes**
- Fréquence des sauvegardes : **Hebdomadaire**
- Chiffrement des sauvegardes : **NON**
- Lieu de stockage : **Externalisé chez un prestataire (Rotation des bandes)**

X Protection supplémentaire du lieu de stockage des supports de sauvegarde. Préciser :

SRDF (Réplication des données sur site de secours)

5. Prtection contre les intrusions extérieures utilisant le canal des réseaux informatiques. Procédé(s) technique(s) utilisé(s) :

X un routeur. Nom : **CISCO**
X un pare-feu (firewall). Nom : **Checkpoint**
X un système complet de détection d'intrusion (IDS). Nom : **Inclus dans le Checkpoint**
X autre procédé : **Reverse Proxy APACHE 2 Linux**

6. Mesures destinées à assurer la confidentialité des données lors du développement de l'application informatique.

X Le développement de l'application s'effectue dans un environnement informatique distinct de celui de la production (par ex. sur des ordinateurs différents, dans des salles machine différentes)
X Le personnel affecté aux tâches de développement est distinct de celui assurant la gestion /l'exploitation des équipements informatiques de production
X La mise au point des logiciels s'effectue sur des données fictives et non sur des données réelles
☐ Autres mesures destinées à protéger la confidentialité des données de production :

_____

7. Mesures destinées à assurer la confidentialité des données lors des opérations de maintenance des équipements informatiques

☐ Les interventions de maintenance des matériels sont enregistrées dans une main-courante
X Les interventions de maintenance des matériels par un sous-traitant se font en présence d'un informaticien de l'entreprise
X La télé-maintenance des matériels n'est pas autorisée
☐ Les supports de stockage envoyés à l'extérieur à fin de réparation font l'objet d'une procédure de protection particulière. Si oui, préciser laquelle :

_____

X Les supports de stockage destinés à la destruction font l'objet d'une procédure de protection particulière. Si oui, faire une description : **Réinitialisation**

8. Mesures destinées à assurer la confidentialité des données lors des opérations de maintenance des logiciels informatiques

☐ Les interventions de maintenance des logiciels dans l'environnement de production sont enregistrées dans une main-courante
X Les interventions de maintenance des logiciels de l'environnement de production se font sous le contrôle du chef d'exploitation en respectant une procédure spécifique
X La télé-maintenance des logiciels de l'environnement de production n'est pas autorisée
☐ Une procédure particulière est mise en œuvre dans le cas où une opération de maintenance logicielle nécessiterait un accès aux fichiers de données nominatives. Si oui, la décrire :
_____

B. Le logiciel d'application.

9. Il met en œuvre :

X une base de données.(ou un logiciel de gestion d'un entrepôt de données).
Nom : **DB2 (IBM) LDAP ZOS**
☐ un (des) progiciel(s). Nom(s) : **ILEX (SIGN & GO MEIBO)**

10. Finalités mettant des procédés techniques particuliers

X carte à puce
☐ biométrie (voir également la rubrique 13)
☐ RFID (reconnaissance à distance par radio-fréquence)
☐ vidéo-surveillance
☐ autre : _____

11. Authentification/identification des personnes habilitées à accéder à l'application. Le contrôle d'accès se fait-il par :

X un mot de passe.
Préciser :
- s'il a une structure obligatoire (par ex. alphanumérique, présence d'un caractère spécial,...) : **Alphanumérique**
- sa longueur minimale : **6**
- sa durée de vie avant changement obligatoire : _____
- s'il y a interdiction de réutiliser les n précédents mots de passe : _____
- s'il y a interdiction d'utiliser certains mots de passe (par ex. date de naissance, prénom,..) : _____
- s'il y a blocage automatique du terminal d'accès au bout d'un certain nombre d'essais infructueux (si oui, préciser ce nombre) : _____

X des profils d'habilitation définissant pour chaque utilisateur les fonctions autorisées ou les catégories d'informations accessibles
X une carte à puce
☐ un dispositif biométrique (voir également la rubrique 13)
☐ autre : _____

X Lors d'une connexion, des informations concernant la précédente connexion s'affichent sur le terminal (par ex. date, heure et identifiant de l'utilisateur)

X Les accès à l'application font l'objet d'une journalisation (données de connexion). Si oui, préciser les informations journalisées :

- X date/heure de connexion
- ☐ identifiant du poste de travail
- X identifiant de l'utilisateur
- ☐ date/heure de déconnexion
- ☐ autres informations journalisées :

_____

☐ Les accès aux fichiers de données nominatives de l'application font l'objet d'une journalisation spécifique. Si oui, préciser les informations journalisées :

- ☐ date/heure d'accès
- ☐ identifiant du poste de travail
- ☐ identifiant de l'utilisateur
- ☐ la référence des données du fichier auxquelles il a été accédé
- ☐ autres informations journalisées : _____
- ☐ type d'accès journalisés, pour : CONSULTATION CREATION MISE A JOUR

12. Confidentialité/authentification. L'application met en œuvre des procédés :

☐ d'anonymisation des données. Nom : _____

☐ de chiffrement des données.
Nom (par ex. 3DES) : _____ Longueur de la clé : _____

X de chiffrement du transport des données.
Nom (par ex. SSL) : **SSL** Longueur de la clé : **2048**

X d'authentification émetteur/destinataire (signature électronique, certificat,...).
Procédé et nom commercial : _____

☐ Expliquer brièvement les raisons du recours à ces procédés :

_____

_____

13. En cas d'usage d'un procédé biométrique. Préciser :

- sa nature (par ex. contour de la main, empreinte digitale, iris,...) :

  _____
- le nom commercial du dispositif ou du fournisseur : _____
- si l'empreinte biométrique est mémorisée sur un support individuel : OUI NON
- si les empreintes biométriques sont mémorisées dans un fichier : OUI NON

NB : les traitements de données biométriques sont soumis à autorisation préalable de la CNIL.

C. Sensibilisation des utilisateurs à la politique de sécurité.

X La politique de sécurité/confidentialité est formalisée dans des documents

☐ Action de sensibilisation des utilisateurs à la politique de sécurité.
Si oui, sous quelle forme (formation, affiche,....) : _____

CNAF

Données traitées, origine, destinataires, durée de conservation
Complément des rubriques 11 et 12

Détail des données à caractère personnel traitées	Origine des données	Destinataire des données	Durée de conservation sur support informatique
Identification du tiers utilisateur ▪ Nom , Prénom ▪ N° téléphone ▪ Adresse professionnelle ▪ E-mail	Personne morale (Tiers)	▪ Le responsable des habilitations (mandataire du Tiers)	Jusqu'à la fin de l'habilitation de l'utilisateur
	fichiers existants chez le tiers et dans l'organisme de la branche	▪ l'Administrateur de l'organisme de la branche ▪ L'instructeur et le Superviseur (Directeur, Agent comptable ou leurs délégataires)	
Trace de la précédente connexion ▪ Identité de l'utilisateur ▪ Date et heure	Organisme de la branche	▪ L'utilisateur	Jusqu'à la prochaine connexion de l'utilisateur.
Connexions infructueuses ▪ Identité de l'utilisateur ▪ Date et heure ▪ Nom de la station de travail et soumis ou non à restriction géographique ▪ Poste ▪ Mission ▪ Remplacement ▪ Motif du rejet de connexion (horaire, mot de passe...)	Organisme de la branche	▪ Le Directeur ▪ L'Agent Comptable ▪ Le responsable sûreté	6 mois.
Trace des activités et des tâches à l'intérieur du système d'information ▪ Identité de l'utilisateur ▪ Date et heure ▪ Services utilisés	Organisme de la branche	▪ Le Directeur ▪ L'Agent Comptable ▪ Le responsable sûreté	6 mois en ligne Au-delà de la durée de conservation en ligne, les données sont archivées sur autre support informatique pendant 6 mois.

CNIL
Commission Nationale de l'Informatique et des Libertés

Récépissé de déclaration

Numéro de déclaration
1184561

Monsieur Frédéric MARINACCE
CAISSE NATIONALE DES ALLOCATIONS FAMILIALES
PRESTATIONS FAMILIALES
32 AVENUE DE LA SIBELLE
75685 PARIS CEDEX 14

Conformément à la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée en août 2004,

CAISSE NATIONALE DES ALLOCATIONS FAMILIALES
32 AVENUE DE LA SIBELLE
75685 PARIS CEDEX 14

A déclaré à la Commission Nationale de l'Informatique et des Libertés un traitement automatisé d'informations nominatives dont la finalité principale est :

GESTION DES HABILITATIONS ET TRACABILITE DES ACCES AUX SERVICES DU SYSTEME D'INFORMATION DES ORGANISMES DE LA BRANCHE FAMILLE PAR LES TIERS

La délivrance du présent récépissé ne vaut pas constatation de la conformité du traitement à la loi et n'exonère le déclarant d'aucune de ses responsabilités.

Paris, le 26 mars 2008
Par délégation de la commission

Alex Türk

Alex TÜRK
Président de la commission

DECLARATIONS

HABNIMS

Outil de sécurisation de l'accès par les personnels
aux services du système d'information de la branche famille

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS
75340 PARIS cedex 07
Tél : 01 53 73 22 22
Fax : 01 53 73 22 00
www.cnil.fr

Déclaration NORMALE

1

PREMIERE DECLARATION	X
DECLARATION DE MODIFICATION	☐
DECLARATION DE SUPPRESSION	☐

Préciser dans ce cas le n° d'enregistrement du traitement que vous souhaitez modifier ou supprimer :
|_|_|_|_|_|_|_|_|

Cadre réservé à la CNIL
N° d'enregistrement |_|_|_|_|_|_|_|_|

☐ D
☐ DT
☐ A

2 Organisme déclarant

Statut juridique : **Secteur public** X **Secteur privé** ☐
Nom ou Raison Sociale : Caisse Nationale des Allocations Familiales CNAF..... N° SIREN **180035065**
Adresse **32 Avenue de la Sibelle** ..... N° APE **753C**
Code postal **75685** Ville **Paris cedex 14**.....Téléphone **01.45.65.52.52**

3 Service ou organisme chargé de la mise en œuvre du traitement

Si le nom et les coordonnées sont identiques à ceux de l'organisme déclarant, cochez ☐ sinon complétez ci-dessous
Nom ou RS ... **Organismes de la branche Famille (Cnaf, Certi, Caf)**.....
Adresse.....
Code postal..... Ville ..... Téléphone .....

4 Service ou organisme auprès duquel s'exerce le droit d'accès *

Si le nom ET les coordonnées sont identiques 1) à ceux de l'organisme déclarant, cochez ☐ 1
2) à ceux du service chargé de la mise en œuvre, cochez X☐ 2 sinon complétez ci-dessous
Nom ou RS .....
Adresse .....
Code postal |_|_|_|_|_| Ville ..... Téléphone |_|_|_|_|_|_|_|_|_|_|

5 Traitement déclaré

Nom du logiciel ...**HABNIMS**.....Année de mise en œuvre .2006 .....
Population concernée (catégories de personnes concernées et nombre approximatif) **30 000**.....
Finalités principales : Gestion de l'habilitation et de la traçabilité des accès aux services du système d'information des personnels des Organismes de la branche .....

6 Transferts d'informations hors de l'Union européenne **

Existe-t-il des transferts d'informations hors de l'Union européenne ? OUI ☐ NON X
Si vous répondez " oui ", précisez quels sont les pays concernés .....

7 Personne à contacter

Nom ...**FLORIMOND**.....Prénom ...**Jean**.....Fonction...**Directeur du projet**.....
Tél : **04 93 95 59 66** fax : **04 92 96 09 42** ..... Adresse électronique. **jean.florimond@cnedi06.cnafmail.fr**.....

8 En cas de déclaration de suppression signer ici et ne pas compléter la feuille 2

Nom du signataire ..... **Signature**
Fonctions l'habilitant à signer .....
Date Le (JJ/MM/AAAA) / /

*** Rubriques à compléter par des annexes. ** Si la réponse est oui, cette rubrique est à compléter par une annexe, dont un modèle est disponible sur le site de la CNIL ou sur simple demande.**

Les informations portées sur ce formulaire et figurant en gras sont obligatoires. Elles font l'objet d'un traitement informatisé à la CNIL et sont destinées aux membres et services de la Commission chargés de l'instruction de votre dossier et au public désireux de s'informer de l'existence d'un fichier dans les conditions prévues à l'article 31 de la loi du 6 janvier 1978. Vous pouvez exercer votre droit d'accès aux informations qui vous concernent en vous adressant à : la CNIL,21 rue Saint-Guillaume 75340 PARIS cedex 07

9 *Fonctions de l'application* *

1	**Gérer le processus d'habilitation**
2	**Administrer la sûreté**
3	**Contrôler et auditer les accès aux système d'information**
4	**Publier les services applicatifs du système d'information**
5	
6	
7	
8	
9	
10	

10 *Sécurités et secrets*

Mettez-vous en place des règles permettant de contrôler l'accès à l'application ?
OUI X 1 NON ☐ 2
Prenez-vous des dispositions pour protéger votre réseau des intrusions extérieures ?
OUI X 1 NON ☐ 2
Les données elles-mêmes font-elles l'objet d'une protection particulière (anonymisation, chiffrement, ...) ?
OUI X 1 NON ☐ 2

11 Catégories de données enregistrées *

X	A	Données d'Identification (nom, prénoms sexe, initiales, n°s d'ordre, date et lieu de naissance...)	☐	I	Moyens de déplacement des personnes
☐	B	NIR, N° de Sécurité Sociale ou consultation du RNIPP	X	J	Utilisation des médias et moyens de communication
☐	C	Situation familiale	☐	K	Données à caractère personnel faisant apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques, religieuses ou les appartenances syndicales des personnes
☐	D	Situation militaire	☐	L	Données biométriques
☐	E	Formation – Diplômes - Distinctions	☐	M	Santé, données génétiques, vie sexuelle
	F	Adresse, caractéristiques du logement	☐	N	Habitudes de vie et comportement
X	G	Vie professionnelle	☐	O	Informations en rapport avec la police
☐	H	Situation économique et financière	☐	P	Informations relatives aux infractions, condamnations ou mesures de sûreté

12 Catégories des destinataires

Catégories d'informations fournies *

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1 **Service demandeur de l'habilitation**	X	☐	☐	☐	☐	☐	X	☐	☐	X	☐	☐	☐	☐	☐	☐
2 **Cadre hiérarchique**	X	☐	☐	☐	☐	☐	X	☐	☐	X	☐	☐	☐	☐	☐	☐
3 **Directeur / Agent comptable /délégataire**	X	☐	☐	☐	☐	☐	X	☐	☐	X	☐	☐	☐	☐	☐	☐
4 **Responsable sécurité**	X	☐	☐	☐	☐	☐	X	☐	☐	X	☐	☐	☐	☐	☐	☐
5 **Responsable application / processus**	X	☐	☐	☐	☐	☐	X	☐	☐	X	☐	☐	☐	☐	☐	☐
6	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
7	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
9	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
10	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

13 Interconnexion, mise en relation, rapprochement **

Le traitement a pour objet l'interconnexion de fichiers dont les finalités principales sont différentes ?
OUI X 1 NON 2
Le traitement a pour objet l'interconnexion de fichiers dont les finalités correspondent à des intérêts publics différents ?
OUI ☐ 1 NON X 2
Les données peuvent- elles êtres cédées, louées, échangées à des fins commerciales ?
OUI ☐ 1 NON X 2

14

Nom du signataire : Frédéric MARINACCE **Signature**
Fonctions l'habilitant à signer Directeur des Prestations familiales
Date : - 8 AOUT 2006

*** Rubriques à compléter par des annexes. ** Si la réponse est oui, cette rubrique est à compléter par une annexe, dont un modèle est disponible sur le site de la CNIL ou sur simple demande.**

Finalités principales et fonctions du traitement
Complément des rubriques 5 et 9

Pour répondre au souci de sécurisation de son réseau informatique, la branche famille met en place un nouvel outil de sûreté *dénommé HABNIMS (habilitation navigateur intranet multi-services),* permettant :

- d'uniformiser dans l'ensemble des organismes, les habilitations des utilisateurs du système d'information avec différents niveaux d'approbation.
- de centraliser la gestion des autorisations qui était auparavant intégrée au sein de chaque application et d'attribuer une signature unique à l'utilisateur.
- d'offrir aux dirigeants des organismes une vision globale des droits d'accès et une meilleure maîtrise de l'utilisation du système d'information par la mise en place d'un dispositif sécurisé, fiable et d'un outil d'audit.
- de créer un annuaire local des utilisateurs de chaque organisme.
- de créer un annuaire national des utilisateurs regroupant les annuaires locaux de chaque organisme.

1. Les finalités

Il est mis en place un dispositif se composant :

- D'un outil de gestion du processus d'habilitations permettant :
  - la prise en compte des événements professionnels contenus dans la base de gestion des ressources humaines (embauche, absences, démission...)
  - la prise en compte des événements organisationnels et non intégrés dans base de gestion des ressources humaines et ayant un impact sur les habilitations d'un utilisateur (affectation de mission ou remplacement...),
  - l'adaptation du poste de travail en fonction du métier de l'utilisateur qui n'a alors accès qu'aux activités auxquelles il est habilité, au travers d'un plan de navigation personnalisé.

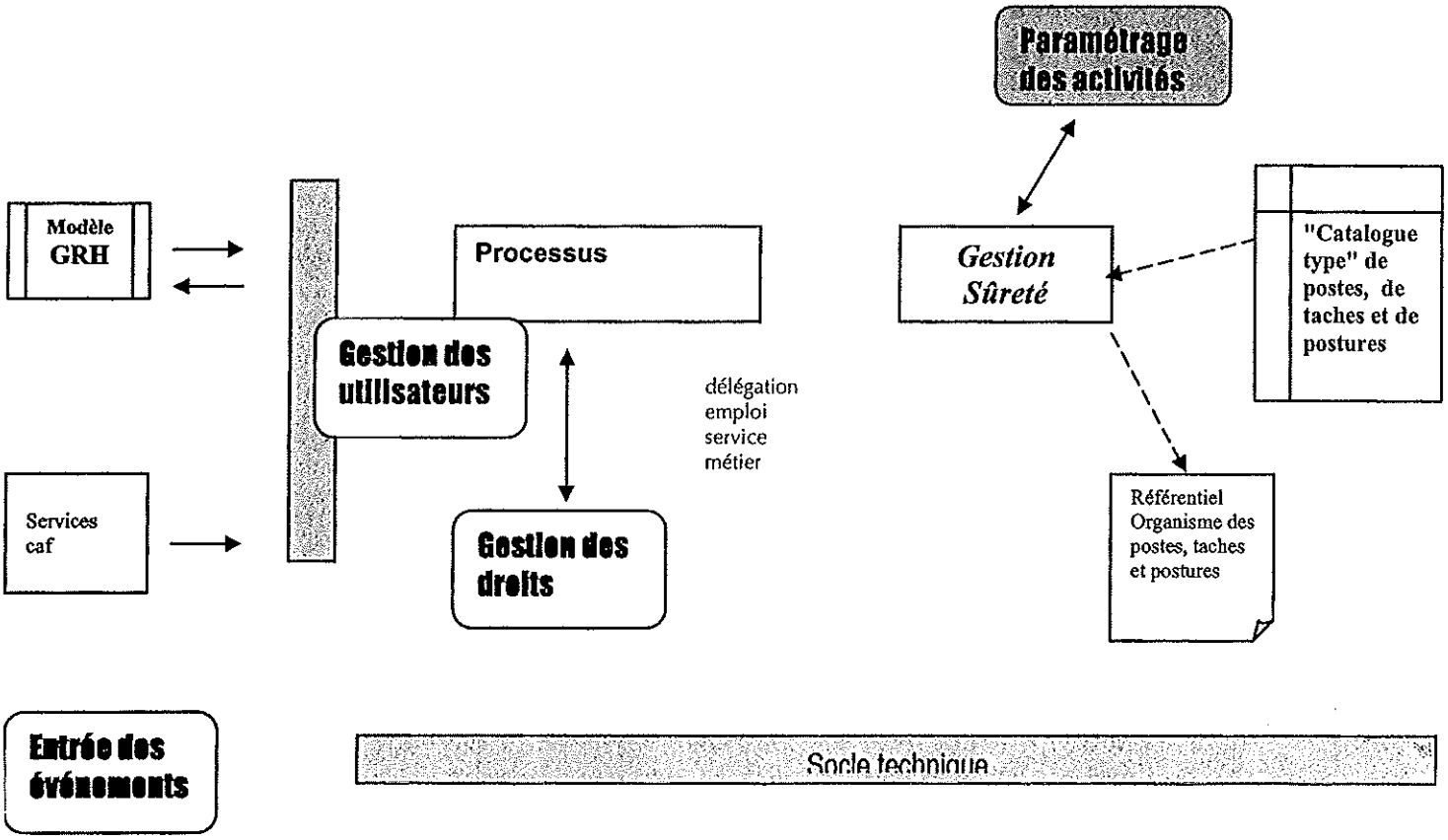
- D'un outil d'administration générale de la sûreté permettant :
  - de mettre en place un ensemble de paramètres de l'organisme (lieux géographiques, services, horaires...) et de définir les postes, les postures d'activité et les tâches applicatives, propres à l'organisme,
  - de définir le paramétrage général de l'activité de supervision et les éléments nécessaires au contrôle et au suivi des habilitations.

- D'un outil de surveillance et d'audit permettant :
  - de s'assurer du bien fondé de l'activité des utilisateurs en fonction de leurs devoirs et engagements professionnels sans violation des libertés fondamentales,
  - de fournir en cas de litige, la preuve d'une utilisation illicite,
  - à l'utilisateur de s'assurer que ses propres moyens d'accès sont respectés.

- D'un outil d'administration permettant de répertorier les services informatiques.

  L'ensemble des services applicatifs métiers et outils informatiques soumis à habilitations sont répertoriés.

Schéma général du processus d'habilitations



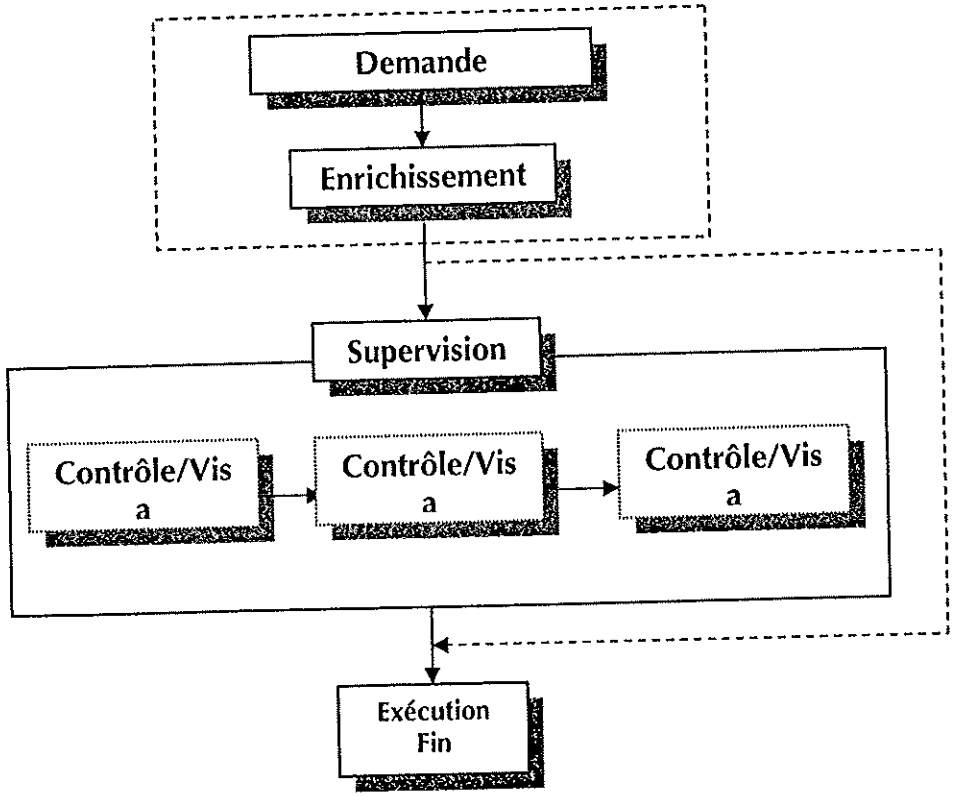
arrivée d'un nouvel agent
départ de longue durée / retour
départ définitif
modification de nom

modification d'affectation temporaire
mission
remplacement
modification d'affectation définitive (poste)
titularisation
prolongation de contrat à durée déterminée
modification administrative
changement de gestion
détachement
formation de longue durée

2. Les fonctions du traitement

2.1. L'outil de gestion du processus d'habilitation

Schéma général



Le processus comprend pour chaque étape les informations suivantes :

Etape no.1 - La demande -

Acteur : **Demandeur** (GRH, responsable hiérarchique, ...)

Informations obligatoires :

- identifiant : prénom – nom – numéro d'agent GRH
- emploi (si issu de la GRH)
- service GRH
- contrat : type et dates début et fin
- date d'effet de la demande

Informations facultatives :

- informations lieu géographique (siège, antenne(s), bureau, téléphone...)
- boite à lettres (oui/non)
- poste
- photo

A l'issue de cette étape, la demande est transmise pour enrichissement (no. étape 2).

Etape no.2 - L'enrichissement -

Acteur : **Instructeur** (responsable hiérarchique)

Informations complémentaires :

- informations lieu géographique (siège, antenne(s), bureau, téléphone)
- boite à lettres (oui/non)
- poste
- accès aux informations dossier du Personnel
- choix des ressources techniques/bureautiques associées au poste
- choix des outils associés au poste

A l'issue de cette étape, la saisie est complète, la demande est transmise pour supervision ou exécution/fin, en fonction du paramétrage.

Il faut, néanmoins, prévoir la possibilité de ré-acheminer une demande pour pouvoir la router vers un autre instructeur (ou un groupe d'instructeurs).

Etape no. 3 - La supervision -

Acteur : **Superviseur** (selon l'organisation de l'organisme : Responsable / Agence Comptable / Direction)

Cette étape est facultative (fonction du paramétrage général)
Le nombre de niveaux de supervision peut varier de 1 à n. (fonction du paramétrage général)

A l'issue de chaque niveau, il y a soit :

- refus avec indication du motif de refus, la demande est retournée à l'instructeur,
- accord : la demande est validée, un visa est apposé sur la demande pour ce niveau, la demande poursuit son circuit.

Une fois, les différents niveaux de supervision effectués, la demande est transmise pour exécution/fin.

L'étape de supervision consiste entre autre à :

- valider l'affectation du poste
- enrichir la fiche de délégation

Etape no. 4 - L'exécution -

Acteur : **Exécutant** (service informatique)

Cette étape permet de déclencher les opérations de mise à jour automatique des annuaires et bases de données, et, d'effectuer, par le service informatique, les opérations telles que la mise en place des outils et des ressources réseau.

A l'issue de cette étape, la demande est exécutée. Une notification est adressée aux personnes concernées.

2.2. *L'outil d'administration générale de la Sûreté*

En amont du processus de gestion des habilitations des personnes, un certain nombre de paramètres permet à chaque organisme d'élaborer, de définir et de gérer au plus proche de son organisation, l'ensemble des éléments en matière d'habilitations et de droits d'accès au système d'informations.
L'outil d'administration intègre :

- des paramètres généraux nécessaires à la personnalisation du processus d'habilitations de l'organisme.
- des paramètres d'environnement propres à chaque organisme :
  site, codes organismes, lieux géographiques, services, outils, ressources...
- des paramètres d'habilitations propres à chaque organisme :
  - **tâches applicatives** correspondant à un regroupement de fonctions applicatives au sein d'un service applicatif,
  - **postures d'activité** correspondant à un ensemble de tâches applicatives,
  - **postes** correspondant à un ensemble de postures d'activité,
- des paramètres outils associés à un poste,
- des paramètres ressources associés à un poste,

Il prend en charge :

- la prise en compte des évolutions liées à une nouvelle version suite à publication dans le Répertoire Des Services, R.D.S. (ajout ou suppression de fonctions applicatives dans un service applicatif, à intégrer dans des tâches applicatives déjà définies, intégration d'un service au sein de la B.O.S. (étape de personnalisation))
- la journalisation de toutes les mises à jour,
- l'activation, pour un service applicatif, d'une nouvelle version (c'est-à-dire, la rendre opérationnelle dans un environnement d'exécution particulier).

2.3. *L'outil de surveillance et d'audit*

Il est mis en place une fonction de traçabilité permettant d'auditer d'une part, les connexions au système d'information et d'autre part, les opérations de paramétrage et les actions dans le processus d'habilitation. cet ensemble de paramètres est contenu dans une base de données locale : la Base de Surveillance de l'Activité (B.S.A.).

Acteurs et rôles

Les acteurs intervenant dans le cadre du processus d'habilitation sont :

- Le Directeur et l'Agent Comptable de l'organisme
- Le responsable de la sécuité
- Le responsable de l'application ou du processus
- Le référent fonctionnel
- Le référent technique informatique
- Le demandeur
- L'utilisateur

Leurs rôles ont été définis selon le tableau suivant.

Acteurs et rôles	Pilotage	Expertise	Exécution	Surveillance et audit
Directeur et Agent Comptable	▪ Ils sont responsables de la sécurité ▪ Ils définissent les consignes générales de sécurité ▪ Ils définissent les règles d'attribution des habilitations en application des délégations attribuées ▪ Ils définissent l'organisation liée au dispositif de surveillance et d'audit		▪ Ils peuvent superviser l'attribution des habilitations	▪ Ils s'assurent de la mise en œuvre de la sécurité
Responsable de la Sécurité Suivant l'organisation de l'organisme il peut être un responsable informatique ou une personne en charge de la maîtrise des risques	▪ Il définit les modalités d'application des consignes générales et des règles de sécurité	▪ Il est responsable du suivi opérationnel des procédures de gestion des sécurités	▪ Il contrôle la mise en œuvre de la sécurité	▪ Il exploite les journaux d'accès au système d'information et rend compte au Directeur et à l'Agent Comptable

Responsable de l'Application ou du processus Suivant l'organisation de l'organisme, il peut être Directeur de branche ou responsable de service. Il coordonne et pilote le déploiement de l'applicatif	▪ Il supervise et définit les modalités d'utilisation de l'applicatif ▪ Il détermine les habilitations adaptées à l'organisation de l'organisme.			▪ En fonction des délégations de la Direction de l'organisme, il peut être conduit à exploiter des journaux d'accès au système d'information de ses utilisateurs
Référent Fonctionnel Désigné pour son niveau d'expertise ou de maîtrise fonctionnelle d'un applicatif donné, il est l'interlocuteur privilégié des utilisateurs et le correspondant des instances internes et externes (*pôle, CERTI, Equipe projet*)		▪ Il participe à la définition du paramétrage des habilitations de l'applicatif lors de la mise en œuvre et à chaque évolution (technique, fonctionnelle ou organisationnelle)	▪ Il s'assure de la bonne mise en œuvre des sécurités définies	
Référent Technique informatique Il est chargé de la mise en place technique de l'applicatif dans le Système d'Information de l'organisme. Il est le correspondant technique des instances internes et externes		▪ Il recherche les réponses techniques liées à la mise en œuvre des habilitations (*contrôle des pré-requis*) ou lors de dysfonctionnement	▪ Il est chargé de mettre en œuvre les procédures de sécurités et habilitations liées au système d'exploitation et aux ressources du réseau informatique ▪ Il met en œuvre et assure le fonctionnement du dispositif de surveillance et audit ▪ Il met à disposition du responsable de la sécurité les journaux et informations nécessaires à l'analyse des traces	
Demandeur			▪ Il initialise la demande d'habilitation	
Utilisateur			▪ Il gère son mot de passe et doit respecter les consignes de sécurité	▪ Il vérifie sa dernière connexion au système d'information

Sécurité de la B.O.S et de la B.S.A.

Données relatives à la sûreté

Les fichiers de données relatifs à la sûreté sont déclarés "vitaux " pour l'organisme. A ce titre ils sont obligatoirement protégés en :

- mise à jour
- destruction
- changement de nom ...

Disponibilité

Pierre angulaire de l'accès au système d'information, la B.O.S. et la B.S.A. seront sécurisées pour assurer en permanence leur accessibilité.

De plus, afin de satisfaire aux exigences d'un sinistre majeur, la B.O.S et la B.S.A. sont intégrées aux procédures de sauvegarde des serveurs de l'organisme.

Procédures de reprise en cas de perte ou d'altération des données

Le ou les fichier(s) de données sauvegardé(s) est ou sont restauré(s). Les modifications d'accès précédemment effectuées sont à réintroduire dans les bases de sécurité.

2.4. L'outil d'administration du Répertoire Des Services (R.D.S)

Un outil permet de répertorier les services informatiques : les applications métiers (Cristal, GRH etc...) et les autres outils (tels qu'internet, messagerie ...), soumis à habilitation et entrant dans la confection du portail d'accès de l'utilisateur, N.I.M.S. (Navigateur Intranet Multi Services).

Principe de mise en œuvre

- au niveau national, les fonctions soumises à habilitations sont définies dans le Répertoire national Des Services, (R.D.S.),
- au niveau local, l'organisme définit les services développés localement et déclare les fonctions associées, soumises à habilitations, dans le Répertoire Local des Services,
- une étape dite d'intégration, permet de prendre en compte les services nationaux et locaux, en leur ajoutant les paramètres propres à chaque organisme et de constituer un ensemble dit de services intégrés, stockés dans la base locale de l'organisme.

Ces services intégrés et les fonctions applicatives associées entrent dans la constitution des paramètres d'habilitations propres à chaque organisme.

Mesures prises pour faciliter l'exercice du droit d'accès
Complément de la rubrique 4

Chaque Organisme de la Branche devra, selon le modèle joint, assurer une information auprès de ses personnels sur l'existence du dispositif de sûreté des accès au système d'information, précisant sa finalité, les destinataires d'informations, le service ou la personne habilité(e) pour répondre aux demandes de droit d'accès.

Modèle

Note d'information

La caisse d'allocations familiales *(ou autre organisme)* met en œuvre un dispositif à caractère national de sûreté des accès au système d'information, dont la finalité est de garantir une utilisation normale des ressources par un processus d'habilitation des personnes et une traçabilité des accès.

Les destinataires des informations enregistrées sont, dans la limite de leurs attributions*: .....

Conformément aux articles 39 et suivants de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les personnes bénéficient d'un droit d'accès et le cas échéant de rectification aux informations qui les concernent. Pour exercer ce droit, elles peuvent s'adresser *.....

* *à compléter par l'organisme, en fonction de son organisation.*

Délai de communication des informations : immédiat à quinze jours.

Complément de la rubrique 10 " *Sécurités* "

Le principal même de l'outil soumis à la Cnil est d'assurer et d'organiser la sécurisation du système d'information de la branche famille. Le processus unifié et contrôlé d'habilitation en constitue la pierre angulaire. Mais la sécurité du processus et la confidentialité des données tracées est aussi garantie par un certain nombre de mécanismes liés aux accès au système d'information.

L'authentification des utilisateurs

Elle est effectuée à l'aide de son identité associé à un mot de passe. Dans le respect des textes réglementaires et de la délégation du Directeur ou de l'Agent Comptable, l'identité et le mot de passe sont les propriétés d'une personne et d'une seule qui en devient le propriétaire et seul responsable.

En conséquence, il n'est pas possible de se connecter à plusieurs sous la même identité.

L'identité

C'est le nom et prénom associé au numéro d'agent GRH et au code de l'organisme d'appartenance.

Le mot de passe

Le mot de passe associé à l'identité permet d'authentifier l'utilisateur qui se connecte au système d'information.

L'initialisation du mot de passe

Le mot de passe est initialisé à la création de l'utilisateur dans la B.O.S.. (suivant le paramétrage il peut être à blanc ou être prédéfini).

A la première connexion de l'utilisateur il est demandé obligatoirement à celui-ci de modifier ce mot de passe initial.

La structure du mot de passe

Dans le respect des préconisations de la CNIL, la longueur minimale du mot de passe est fixée à six caractères alphanumériques.

Dans le but de limiter l'utilisation de mots de passe de type courant (nom de l'utilisateur, nom de l'organisme, etc...) une table des mots de passe interdits est gérée.

La gestion des mots de passe

La gestion des mots de passe est assurée par l'utilisateur qui introduit sur demande du système, à expiration de celui-ci ou à sa convenance, un nouveau mot de passe obligatoirement différent au moins des trois précédents.

Le délai de rétention du mot de passe

Le délai de rétention du mot de passe est fixé au maximum à 45 jours, de date à date, passé ce délai le mot de passe est expiré et l'utilisateur est invité à le changer.

Délai minimum de changement entre les mots de passe

Le délai minimum toléré entre les changements de mot de passe est de 3 jours.

Réutilisation du mot de passe

Le nouveau mot de passe généré est obligatoirement différent des trois derniers mots de passe précédemment introduits.

Le paramètre des contraintes

Il est effectué par le référent technique informatique, au moment de l'installation du produit pour répondre à de nouvelles normes ou directives de la CNAF.

Le contrôle du mot de passe en cours de session

Il peut être paramétré un contrôle des mots de passe en cours de session dans le but de répondre à la surveillance d'un groupe de travail ou d'un ou plusieurs utilisateurs.

La protection des mots de passe

Dans le but de garantir la confidentialité, les fichiers contenant les mots de passe sont protégés (cryptographie ou chiffrement).

La récupération d'un mot de passe oublié

L'utilisateur qui a oublié son mot de passe doit contacter le responsable de la sécurité pour attribution d'un nouveau mot de passe qui est obligatoirement changé par l'utilisateur lors de la connexion de celui-ci à son poste de travail.

La propagation des mots de passe

Le système permet la propagation des mots de passe entre les différentes services informatiques du poste de travail.

La période d'inactivité

Après une période d'inactivité mesurée, maximum d'1 heure, du code utilisateur, une déconnexion automatique est effectuée par le système.

La période d'inactivité est paramétrable par les organismes.

Le blocage de l'identifiant après un délai de non utilisation

Le système GRH communique les absences de longue durée au système qui bloque les accès.

La sécurité des accès

La sécurité des accès est assurée par le système dès la mise sous tension du poste de travail. Après authentification de l'utilisateur (code identifiant et mot de passe) un message apparaît sur

le poste de travail indiquant : ***la date et l'heure de la dernière connexion sous le même code utilisateur et mot de passe.***

Mesures prises en cas de tentatives de violation d'accès

Après trois tentatives successives d'accès infructueux (associé à un code identifiant correct) le couple code identifiant et mot de passe est invalidé.

- un blocage de l'accès est systématiquement effectué par le système.
- un message apparaît à l'utilisateur l'invitant à contacter le responsable sécurité.
- une déconnexion automatique est effectuée.

Les tentatives de violation sont obligatoirement enregistrées à destination du directeur, de l'agent comptable et du responsable de la sécurité.

Procédure de "by pass"

Le système est normalement incontournable. Toutefois une procédure exceptionnelle peut éventuellement être activée pour répondre à des problèmes de fonctionnement du serveur de données.

Données traitées, origine, destinataires, durée de conservation
Complément des rubriques 11 et 12

Les données de base dans la B.S.A. (Base de Surveillance de l'activité)

Catégorie d'information	Détail des données à caractère personnel traitées	Origine des données	Destinataire des données	Durée de conservation
Informations liées à la GRH	**Identification de l'utilisateur** ▪ Nom – Numèro d'agent GRH ▪ Emploi ▪ Service ▪ Contrat : type et dates début et fin	Organisme Logiciel GRH	▪ Demandeur d'une habilitation ▪ Cadre hiérarchique ▪ Superviseur (Directeur, agent comptable ou leurs délégataires) ▪ Référent technique informatique ▪ Responsable de la sécurité	Données importées. Conservation jusqu'au départ de l'utilisateur
	Evénements touchant l'agent et suscitant une modification de l'habilitation ▪ départ définitif ▪ modification de nom ▪ modification d'affectation temporaire (mission, remplacement) ▪ modification d'affectation définitive (poste) ▪ titularisation ▪ prolongation de contrat à durée déterminée ▪ modification administrative ▪ changement de gestion ▪ détachement	Organisme Logiciel GRH	▪ Demandeur d'une habilitation ▪ Cadre hiérarchique ▪ Superviseur (Directeur, agent comptable, ou leurs délégataires) ▪ Référent technique informatique ▪ Responsable de la sécurité	
	Absences de longue durée (fermeture des accès au système d'information)	Organisme Logiciel GRH	*En cas d'anomalie :* ▪ Directeur ▪ Agent comptable Responsable de la sécurité	

Les données de base dans la B.S.A. (Base de Surveillance de l'activité)

Catégorie d'information	Détail des données à caractère personnel traitées	Origine des données	Destinataire des données	Durée de conservation
Informations liées aux interventions dans le processus d'habilitation	**Interventions dans la BOS : paramètres** ▪ Identité du référent technique ▪ Date et heure ▪ Nom de la station de travail ▪ Intitulé et contenu du paramètre concerné ▪ Action réalisée ▪ Date et heure d'effet de l'action.	Organisme	▪ Directeur ▪ Agent Comptable ▪ Responsable sécurité ▪ Responsable de l'application ou du processus	1 an. [1]
	Interventions dans la BOS : Actions dans le processus d'habilitation ▪ Identité de chaque acteur du processus d'habilitation ▪ Date et heure /acteur ▪ Nom de la station de travail /acteur ▪ Fait générateur (affectation d'un poste, d'une mission, d'un remplacement...) ▪ Date d'effet et durée, ▪ Identité de la personne habilitée ▪ Commentaires	Organisme	▪ Directeur ▪ Agent Comptable ▪ Responsable sécurité	1 an[1]
Informations liées aux accès et interventions dans le système d'information	**Trace de la précédente connexion** ▪ Identité de l'utilisateur ▪ Date et heure Nom de la station de travail.	Outil d' administration de la sûreté	▪ L'utilisateur	Jusqu'à la prochaine connexion de l'utilisateur.
	Connexions fructueuses aux activités et aux tâches à l'intérieur du système d'information ▪ Identité de l'utilisateur ▪ Date et heure ▪ Nom de la station de travail ▪ Trace systématique des connexions aux services, aux applications et aux ressources informatiques identifiés dans le R.D.S. et soumis à habilitations dans la B.O.S.. ▪ Trace paramétrable des activités de production de l'utilisateur . ▪ Durée de la connexion au service, à l'application et au poste de travail.	Outil d' administration de la sûreté	▪ Directeur ▪ Agent Comptable ▪ Responsable sécurité ▪ Responsable de l'application ou du processus	1 an [1]

[1] En application du décret n° 2006-358 du 24 mars 2006, relatif à la conservation des données des communications électroniques. Au delà les données sont archivées 2ans dans le cadre de la prescription en cas de délits.

Les données de base dans la B.S.A. (Base de Surveillance de l'activité)

Catégorie d'information	Détail des données à caractère personnel traitées	Origine des données	Destinataire des données	Durée de conservation
Informations liées aux accès et interventions dans le système d'information	**Connexions infructueuses** ▪ Identité de l'utilisateur ▪ Date et heure ▪ Nom de la station de travail et soumis ou non à restriction géographique ▪ Poste ▪ Mission ▪ Remplacement ▪ Motif du rejet de connexion (horaire, restriction GRH, mot de passe, service non autorisé…)	Outil d' administration de la sûreté	▪ Directeur ▪ Agent Comptable ▪ Responsable sécurité	1 an [1]
	▪ Relevé des codes utilisateur non utilisés ou bloqués par le système.	GRH Outil d' administration de la sûreté	▪ Directeur ▪ Agent Comptable ▪ Responsable sécurité	1 an [1]

[1] En application du décret n° 2006-358 du 24 mars 2006, relatif à la conservation des données des communications électroniques. Au delà les données sont archivées 2ans dans le cadre de la prescription en cas de délits.

CNIL
Commission Nationale de l'Informatique et des Libertés

Récépissé de déclaration

Numéro de déclaration
1338960

Monsieur Frédéric MARINACCE
CAISSE NATIONALE DES ALLOCATIONS FAMILIALES
DIRECTION DES PRESTATIONS FAMILIALES
32 AVENUE DE LA SIBELLE
75685 PARIS CEDEX 14

Conformément à la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée en août 2004,

CAISSE NATIONALE DES ALLOCATIONS FAMILIALES
32 AVENUE DE LA SIBELLE
75685 PARIS CEDEX 14

A déclaré à la Commission Nationale de l'Informatique et des Libertés un traitement automatisé d'informations nominatives dont la finalité principale est :

GESTION DE L'HABILITATION ET DE LA TRACABILITE DES ACCES AUX SERVICES DU SYSTEME D'INFORMATION DES PERSONNELS DES ORGANISMES DE LA BRANCHE

La délivrance du présent récépissé ne vaut pas constatation de la conformité du traitement à la loi et n'exonère le déclarant d'aucune de ses responsabilités.

Paris, le 12 juin 2009
Par délégation de la commission

Alex Türk

Alex TÜRK
Président de la commission