

Le, 07/07/2010

**CIRCULAIRE COMMUNE Circulaire Agirc-Arrco 2010 – 9 -DC**

**Objet : relevé individuel de situation électronique RIS/E**

Madame, Monsieur le directeur,

En application du Droit à l'Information institué par la loi du 21 août 2003, les assurés âgés de 35 à 50 ans doivent être destinataires d'un relevé de situation individuelle (RIS) élaboré par les 35 régimes participant au droit à l'information au sein du GIP INFO RETRAITE.

Le RIS permet à l'assuré de vérifier que tous les éléments relatifs à sa carrière professionnelle ont été pris en compte par les différents régimes de retraite auprès desquels il a été affilié en France.

Depuis janvier 2008, tous les assurés, quel que soit leur âge, ont également la possibilité de formuler auprès d'un gestionnaire d'un de leurs régimes, une demande de RIS (RIS « à la demande » ou RISD) qu'ils reçoivent par courrier.

Depuis mai 2010, ces demandes sont traitées sur un rythme hebdomadaire dans le cadre des mini-cohortes.

Afin d'améliorer la qualité du service rendu aux assurés, les régimes participant au droit à l'information ont décidé de compléter le dispositif par une publication sur Internet. Ce service est appelé RIS/E.

Fin juin 2011, tout assuré, quel que soit son âge, dès lors qu'il est connu de l'annuaire du GIP (certifié), aura la possibilité de demander, via son identifiant et son mot de passe, un RIS/E sur le portail de l'un de ses régimes de retraite d'affiliation.

Conformément au principe mis en œuvre pour la consultation du Relevé Actualisé de Points (RAP) établi par la circulaire 2008-12-DSI du 13/11/2008, le groupe de dernière affiliation de l'assuré, dit groupe d'interlocution, est seul autorisé à authentifier et à délivrer le service (à l'exception des cadres à affiliation dissociée et des participants à employeurs multiples PEM qui pourront consulter leur RIS/E sur le portail de tous leurs groupes d'affiliation simultanée).

Une interface fonctionnelle appelée Concentrateur est mise en place entre les portails des groupes de protection sociale AGIRC-ARRCO et les collecteurs NORD et SUD du GIP INFO RETRAITE afin de relayer les demandes et réponses de RIS/E dans la sphère AGIRC-ARRCO.

L'annexe 1 détaille les modalités d'accès au RIS/E.

Les données figurant sur le RIS/E sont, comme celles figurant sur les documents papier, confidentielles.

L'accès au service RIS/E par l'internaute n'est autorisé que suite à son authentification sur le portail du groupe. Cette authentification doit respecter les règles définies en annexe 2 (Cahier des charges – règles d'authentification RIS/E).

Une convention de service liant l'AGIRC et l'ARRCO au GIP INFO RETRAITE prévoit en effet le respect de règles fixées par la communauté des régimes pour l'authentification et les niveaux de sécurité d'accès aux portails.

Il est précisé que les portails ne présentant pas les niveaux de sécurité requis ne pourront pas proposer le service.

Veillez agréer, Madame, Monsieur le directeur, l'assurance de ma considération distinguée.

Le Directeur général,

## **ANNEXE 1**

### **Les modalités d'accès au RIS-E à partir des portails des groupes AGIRC-ARRCO**

Le service d'un RIS/E en temps réel est fourni lorsque tous les régimes d'affiliation de l'assuré sont en capacité de traiter par Web-Services (WS).

A contrario, si l'un des régimes de la carrière n'est pas en mesure de répondre (absence de WS ou dysfonctionnement ponctuel du WS), la demande de RIS/E est traitée dans le cadre du fonctionnement actuel des RISD, à savoir par collecte dans le cadre des « mini-cohortes » hebdomadaires.

Les régimes procèdent alors par échange "batch" de fichiers pour fournir le RIS/E sur un mode dit « dégradé » : le RIS/E est livré sous forme électronique mais dans un délai d'une à deux semaines.

La production d'un RIS/E en temps réel requiert la mise en place de WS sécurisés entre les régimes et les Collecteurs NORD et SUD du GIP INFO RETRAITE. S'agissant des régimes AGIRC et ARRCO, un « Concentrateur » est mis en place afin de mutualiser les développements des groupes de protection sociale AGIRC-ARRCO.

Les portails des groupes échangeront avec le Concentrateur qui assure le rôle de point unique d'entrée avec les Collecteurs NORD et SUD du GIP INFO RETRAITE.

#### **1. DISPONIBILITE DU SERVICE**

Pour l'ensemble des régimes offrant le service, les plages d'ouverture du service iront au-delà des heures de bureau et des jours ouvrés sans qu'une disponibilité de 24h/24 et de 7 jours sur 7 soit exigée.

Sont notamment prévus :

- des interruptions courtes de service à heures creuses, en particulier pour la maintenance ;
- un délai de reprise en cas d'incident, modulé selon les jours ouvrés ou non ouvrés.

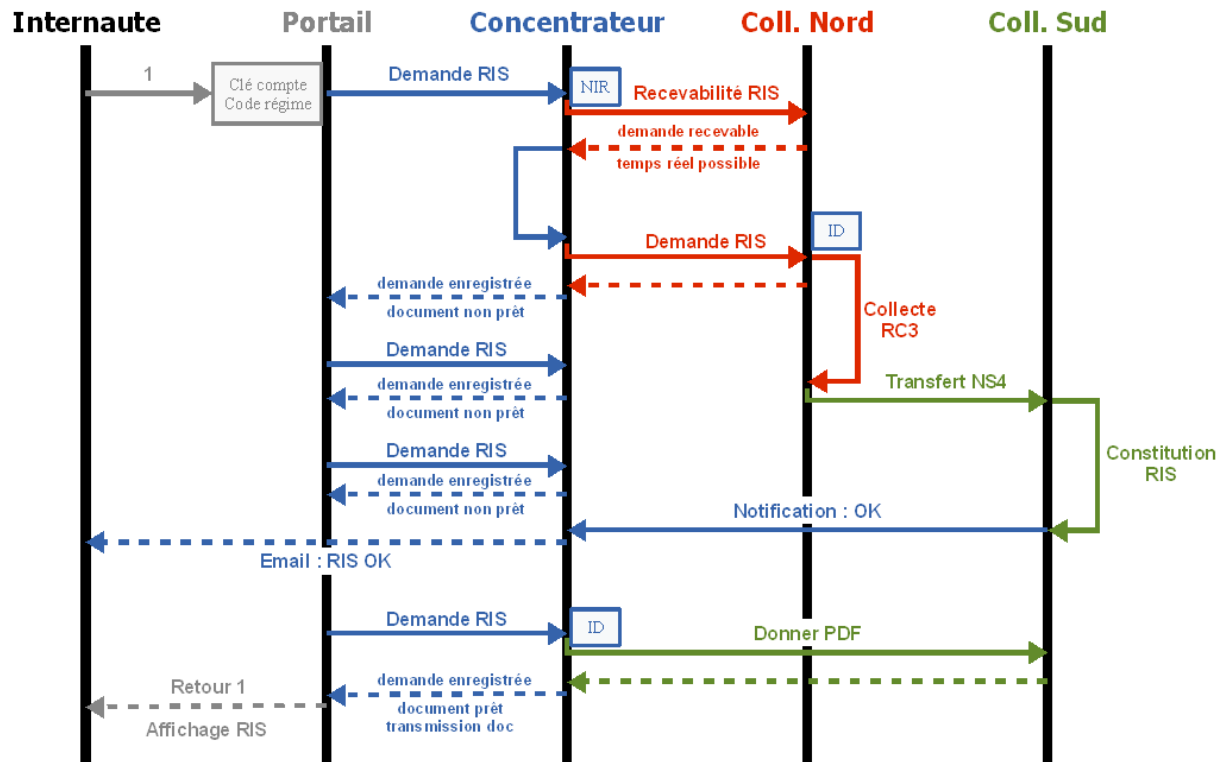
Chaque régime communique au GIP INFO RETRAITE ses plages d'indisponibilité. Les régimes AGIRC et ARRCO peuvent déclarer deux plages horaires d'indisponibilité pour chaque jour de la semaine (du lundi au dimanche).

Ces plages, qui seront répertoriées dans le descripteur du GIP INFO RETRAITE, sont communes à l'ensemble des groupes de protection sociale AGIRC-ARRCO. Elles seront précisées ultérieurement.

Un message écran figure sur le portail du groupe lors des interruptions de service.

## 2. PROCESSUS

Le processus de traitement des RIS/E peut être schématisé de la façon suivante (cf. Spécifications fonctionnelles générales RIS/E et Concentrateur V01.07).



### a) Dépôt de la demande

L'assuré se connecte sur le portail de son groupe de protection sociale AGIRC-ARRCO et active une demande de RIS/E.

Le portail du groupe doit :

- ⇒ identifier et authentifier l'assuré par un mot de passe communiqué au préalable dans les conditions décrites dans l'annexe 2,
- ⇒ demander à l'assuré de saisir une adresse e-mail valide.

Vis-à-vis du Concentrateur, le groupe doit au moins fournir la clé de compte participant de l'assuré pour l'identifier de manière unique. D'autres données pourront être demandées à des fins de traçabilité<sup>1</sup>.

<sup>1</sup> Les règles de traçabilité seront communiquées dès qu'elles auront été définies dans le cadre des travaux du Gip Info Retraite.

### **b) Contrôle de recevabilité**

En réponse à la demande de RIS/E, le portail du groupe appelle le WS « Contrôle et recevabilité de la demande » du Concentrateur qui effectue les traitements suivants :

- ⇒ En cas d'absence de RIS/E en cours et de RIS/E non périmé : la demande est transmise au Collecteur NORD.
- ⇒ En cas de présence d'un RIS/E non périmé au Collecteur Sud (un RIS/E a été demandé auprès de l'AGIRC-ARRCO ou d'un autre régime dans les quinze précédents jours) : le document existant est récupéré par le Concentrateur et affiché en temps réel.
- ⇒ En cas de demande de RIS/E en cours (un RIS/E a été demandé auprès régime de l'AGIRC-ARRCO ou d'un autre régime et est en cours de traitement au Collecteur NORD) : la demande est annulée et le portail du groupe informé.

Dans la première hypothèse, le WS « Contrôle et recevabilité de la demande » du Concentrateur appelle ensuite le WS « Contrôle et recevabilité de la demande » du Collecteur NORD qui effectue un nouveau contrôle de recevabilité de la demande (assuré non décédé, non liquidé, présent à l'annuaire et affilié au régime demandeur) ainsi qu'un contrôle de faisabilité de la demande en temps réel.

Comme pour le RIS/D, une demande de RIS/E est rejetée lorsqu'un autre document est en cours dans le cadre d'une campagne systématique ou dans le cadre d'une mini-cohorte (RISD ou RIS rectificatif / RISR ou EIG rectificative / EIGR).

### **c) Contrôle de faisabilité et conséquences**

Le contrôle de faisabilité consiste, pour le Collecteur NORD, à lister, en consultant l'annuaire, les différents régimes d'affiliation de l'assuré et à vérifier qu'ils sont tous en mesure de répondre en temps réel.

Le traitement de la demande de RIS/E dépendra en effet de la capacité des régimes d'affiliation à restituer la carrière et les droits et des délais que nécessitera cette restitution :

- i. Si tous les régimes d'affiliation sont en mesure de traiter la demande (WS opérationnels), celle-ci donnera lieu à une réponse immédiate. Il s'agira d'un **traitement en temps réel**. Le portail du groupe peut informer l'internaute que sa demande est prise en compte en temps réel.
- ii. Si la demande ne peut pas être traitée en temps réel parce qu'elle arrive dans une plage d'indisponibilité des WS d'un des régimes d'affiliation, **le traitement passe en « en mode différé »**. Le portail du groupe informe alors l'internaute que sa demande ne peut être traitée immédiatement. Il lui précise le délai

prévisionnel de restitution de l'information (en principe le lendemain).

- iii. Si un (ou plusieurs) des régimes concernés ne sont pas en mesure de traiter la demande en temps réel ou en mode différé, **la gestion de la demande passe automatiquement « en mode dégradé »** et est réorientée vers le traitement hebdomadaire le plus proche (mini cohorte). Le portail du groupe informe alors l'internaute que sa demande ne peut être traitée immédiatement. Il lui précise le délai prévisionnel de restitution de l'information (dans les quinze jours).

### 3. LA NOTIFICATION

Lors de la connexion au service après identification et authentification, le portail du groupe demande à l'internaute de communiquer son e-mail ou demande confirmation de celui-ci.

Dans le cas d'adresse e-mail non valide, un message propose à l'assuré de ressaisir une adresse valide.

Des messages écran sont en outre affichés en lien avec les contrôles de recevabilité et de faisabilité du RIS/E.

Dès lors que la demande de RIS/E est recevable, un message écran indique à l'assuré que sa demande est prise en compte.

Dans les cas de non recevabilité du RIS/E pour cause de document en cours de traitement (RIS systématique, à la demande ou rectificatif ou EIG systématique ou rectificative), un message écran informe l'assuré que sa demande ne peut aboutir, en indique la raison et fournit les coordonnées du groupe d'interlocution.

Dans les cas de non recevabilité du RIS/E pour des causes autres (absence à l'annuaire GIP, véto autre régime...), un message écran informe l'assuré que sa demande ne peut aboutir et lui communique les coordonnées de son groupe d'interlocution.

Dans le cas d'un incident technique temporaire rendant impossible le traitement du RIS/E un message l'invite à se connecter ultérieurement.

Dans le cas où l'assuré a déjà activé une demande de RIS/E et que celle-ci est en cours de traitement un message écran le lui rappelle et, le cas échéant (si cette demande est différée ou dégradée), le message précise la date à laquelle le document sera disponible sur le portail.

Si la demande est bien recevable mais que l'établissement du document prend trop de temps (plus de 30 secondes), un message écran indique à l'assuré qu'il sera avisé de la disponibilité du document par e-mail.

Si la demande a été traitée avec succès en temps réel, un message écran indique que le document est prêt.

L'hypothèse d'un document prêt mais corrompu ou vide est envisagée et un message invite l'internaute à renouveler sa demande de RIS/E.

Que l'assuré soit ou non connecté au portail après avoir activé sa demande de RIS/E, la notification de disponibilité du document est systématiquement adressée en message électronique par le groupe auquel s'est adressé le demandeur (en principe le groupe d'interlocution).

Ces messages n'ont pas vocation à faire l'objet de réponse de l'assuré en particulier pour formuler une réclamation. Il s'agit d'expéditeur du type « [noreply@agirc-arrco.fr](mailto:noreply@agirc-arrco.fr) ».

Le document RIS/E ne figure pas en pièce jointe. Le message électronique affiche le lien et invite à se reconnecter au portail du groupe pour consulter le RIS/E.

Si un incident diffère l'édition du RIS/E (cas de RIS/E ayant basculé en mode différé ou dégradé), le message électronique indique à l'internaute que le traitement de sa demande est différé et que le document sera disponible à une date donnée.

Il est précisé que le document reste consultable pendant une durée de quinze jours.

Si le service RIS/E ne peut pas être fourni, un message électronique invite l'assuré à prendre contact avec son groupe.

#### **4. LE DOCUMENT**

Le document produit est identique au RIS sur lequel figurent le nom d'usage et/ou le nom patronymique de l'intéressé son prénom et son NIR.

Le feuillet AGIRC-ARRCO indique les coordonnées du groupe d'interlocution déterminé selon les règles applicables au RISD et au RAP (voir Circulaire 2008-12 DSI du 13/11/2008).

Comme sur le RIS papier, les données restituées en synthèse sur le document sont, jusqu'au 1<sup>er</sup> juillet, les droits de l'année n-2 et, après le 1<sup>er</sup> juillet, ceux de l'année n-1. Néanmoins, les régimes disposant des données n-1 avant le 1<sup>er</sup> juillet de l'année n indique les données les plus récentes sur leur feuillet.

#### **5. LE CALENDRIER DE MISE EN OEUVRE**

Le calendrier prévisionnel de mise en œuvre du RIS/E est le suivant :

- 15/05/2010 - 30/11/2010 : Accrochage technique aux différents services du GIP INFO RETRAITE par les régimes.
- 15/10/2010 - 30/11/2010 : Tests internes du GIP INFO RETRAITE.
- 01/12/2010 – 31/12/2010 : Tests de la collecte de droits auprès des régimes (Carrière en ligne).
- 01/01/2011 – 28/02/2011 : Test complet avec les portails des régimes.
- 01/03/2011 : Mise en production du service.

L'ouverture du service est prévue à partir du 14 mars 2011 à la suite d'une période initiale de deux semaines où seul le portail du GIP aura la possibilité d'ouvrir des processus RIS/E sur des effectifs très restreints.

La montée en charge s'effectuera progressivement en ouvrant le service par tranches d'âge de plus en plus nombreuses selon le calendrier suivant :

<b>Semaines concernées</b>	<b>Années de naissance éligibles âge limite</b>	<b>Effectifs présents dans l'annuaire du GIP INFO RETRAITE (tous régimes confondus)</b>
<b>S 11 – S 13 Du 14/03 au 03/04/2011</b>	<b>2011 – 1971(inclus) &lt; 40 ans</b>	<b>17 480 962</b>
<b>S 14 – S16 Du 04/04 au 24/04/2011</b>	<b>2011 – 1966 (inclus) &lt; 45 ans</b>	<b>22 405 422</b>
<b>S 17 – S 19 Du 25/04 au 15/05/2011</b>	<b>2011 – 1961 &lt; 50 ans</b>	<b>27 372 631</b>
<b>S 20 – S 22 Du 16/05 au 05/06/2011</b>	<b>2011 – 1956 (inclus) &lt; 55 ans</b>	<b>32 095 862</b>
<b>S 23 – S 25 Du 06/06 au 26/06/2011</b>	<b>2011 – 1951 &lt; 61 ans</b>	<b>36 600 500</b>
<b>S 26 A partir du 27/06/2011 : ouverture totale du service</b>	<b>Toutes générations</b>	<b>46 961 863</b>

## 6. TRAITEMENT DES RECTIFICATIFS

Suite à la consultation de son RIS/E, l'assuré est susceptible de contacter son groupe d'interlocution pour demander, si nécessaire, des rectifications.

Le principe retenu est que le document rectificatif soit également accessible sous forme dématérialisée (RIS/E -RIS/E rectificatif).

Néanmoins, une nouvelle consultation électronique après corrections permet en tout état de cause à l'assuré de vérifier si les modifications ont été intégrées dans son relevé de situation individuelle.

ANNEXE 2



DIRECTION SYSTEMES D'INFORMATION  
RETRAITE COMPLEMENTAIRE  
ETUDES GENERALES

# **RIS e**

## **Cahier des charges relatif aux mesures d'authentification**

Rédaction : Jean-Claude GUICHARD  
Date de mise à jour : 28/06/2010 17:00:00  
Date d'impression : 09/07/2010 12:13

**Cahier des charges relatif aux mesures d'authentification****ETAT DU DOCUMENT**

	Date	Auteur
Version V0.0 - Rédaction initiale	21/11/2009	Jean-Claude GUICHARD
Version V0.1 – Modifications suite à réunion avec les Groupes du 4 décembre 2009	07/12/2009	Jean-Claude GUICHARD
Version V0.2 – Modifications suite à réunion avec les Groupes du 11 décembre 2009	14/12/2009	Jean-Claude GUICHARD
Version V1 – Modifications pour diffusion	01/01/2010	Jean-Claude GUICHARD
Version V1.1 – Modifications suite au Comité de pilotage stratégique "Information des actifs"	19/03/2010	Jean-Claude GUICHARD
Version V1.2 – Modifications suite à la réunion du Groupe Authentification du Gip-MDS du 2 avril 2010 – Les contrôles d'authentification de niveau 2 sont uniquement recommandés	02/04/2010	Jean-Claude GUICHARD
Version V1.3 – Coordination avec la circulaire Ris-e	07/06/2010	Jean-Claude GUICHARD

**SOMMAIRE**

<b>1</b>	<b>PREAMBULE – RAPPEL DE L'OBJECTIF DU DOCUMENT .....</b>	<b>4</b>
<b>2</b>	<b>DOCUMENTS DE REFERENCE .....</b>	<b>4</b>
<b>3</b>	<b>IDENTIFICATION DE L'INTERNAUTE POUR L'INSCRIPTION AU SERVICE DU RIS EN LIGNE .....</b>	<b>4</b>
<b>4</b>	<b>CONTROLE DE COHERENCE – PHASE D'AUTHENTIFICATION DE LA PERSONNE POUR L'INSCRIPTION AU SERVICE .....</b>	<b>5</b>
4.1	CONTROLE DE CONNAISSANCE DE L'ASSURE DANS LES BASES D'AFFILIATION DE L'INSTITUTION. ....	5
4.2	CONFRONTATION AVEC DES INFORMATIONS INSCRITES DANS LE SYSTEME D'INFORMATION.....	5
4.3	GESTION DES ECARTS .....	6
<b>5</b>	<b>MODE DE TRANSMISSION DES CLES D'ACCES AU PORTAIL (IDENTIFIANT – MOT DE PASSE).....</b>	<b>6</b>
<b>6</b>	<b>GESTION DU COMPTE DE L'INTERNAUTE.....</b>	<b>7</b>
6.1	IDENTIFIANT POUR ACCEDER AU SERVICE.....	7
6.2	GESTION DES MOTS DE PASSE .....	7
6.3	GESTION DU COMPTE.....	7
6.4	PROCEDURE EN CAS DE PERTE DU MOT DE PASSE.....	8
<b>7</b>	<b>ELEMENTS TECHNIQUES.....</b>	<b>8</b>
7.1	LIAISON HTTPS OBLIGATOIRE.....	8
7.2	GESTION DES TRACES .....	8
<b>8</b>	<b>POLITIQUE DE REPRISE DU PASSE.....</b>	<b>9</b>
<b>9</b>	<b>SUIVI DE MISE EN ŒUVRE DES REGLES D'AUTHENTIFICATION.....</b>	<b>9</b>

## **1 PREAMBULE – RAPPEL DE L'OBJECTIF DU DOCUMENT**

Dans le cadre de l'application de la Loi Fillon relatif à l'information des personnes en matière de retraite, les régimes de retraite membres du Gip Information des actifs ont décidé de mettre en œuvre à compter du 2<sup>ème</sup> trimestre 2011, un service permettant aux assurés d'obtenir leur Relevé Individuel de Situation (RIS-e) via Internet.

Ce projet a nécessité la définition par les régimes concernés d'un niveau d'authentification à partir duquel chaque régime de retraite accepte de mettre à la disposition de la communauté des régimes les informations en sa possession nécessaires à la constitution du RIS-e.

Ce cahier des charges a pour objectif de décrire le niveau de sécurité à mettre en œuvre dans les systèmes d'information des institutions Agirc et Arcco, et particulièrement sur leur site Internet pour atteindre le niveau de sécurité défini par la Communauté.

Ces dispositions n'ont pas appelé d'objections de la part des services de la CNIL.

Elles couvrent les fonctionnalités suivantes :

- Identification de l'internaute,
- Authentification de son identité
- Mode de transmission des clés d'accès au portail
- Gestion du compte Internet de l'assuré et de la transaction
- Règles techniques d'accès au dispositif
- Reprise de l'existant

## **2 DOCUMENTS DE REFERENCE**

## **3 IDENTIFICATION DE L'INTERNAUTE POUR L'INSCRIPTION AU SERVICE DU RIS EN LIGNE**

L'identification des personnes peut être assurée par une des données suivantes :

- le NIR ou numéro de sécurité sociale avec sa clé,
- le numéro interne d'affiliation à l'institution,
- les autres éléments d'identité : nom de naissance, prénom, nom marital, date de naissance...

A l'occasion de cette inscription, l'institution doit récupérer une adresse e-mail valide dans sa forme (voir Circulaire Relevé Individuel de Situation électronique).

## **4 CONTROLE DE COHERENCE – PHASE D'AUTHENTIFICATION DE LA PERSONNE POUR L'INSCRIPTION AU SERVICE**

### **4.1 CONTROLE DE CONNAISSANCE DE L'ASSURE DANS LES BASES D'AFFILIATION DE L'INSTITUTION.**

L'institution doit mettre en œuvre un contrôle immédiat de connaissance de l'assuré dans ses bases de données "Participant" en contrôlant :

- la présence du NIR certifié du demandeur dans ses bases,
- la cohérence du NIR avec les autres éléments d'identification (nom de naissance, prénom, nom marital, date de naissance,...) déclarés par le demandeur avec les informations connues de son système d'information.

### **4.2 CONFRONTATION AVEC DES INFORMATIONS INSCRITES DANS LE SYSTEME D'INFORMATION.**

Il est recommandé de mettre en œuvre des contrôles d'authentification de deuxième niveau en comparant les données saisies par l'internaute avec des données différentes de celle du 4.1 et qui sont connues de son système d'information.

Ces contrôles peuvent être, en particulier, en cas d'utilisation du NIR ou des éléments de l'Etat civil, effectués :

- avec le numéro interne d'affiliation de la personne
- et/ou l'adresse préalablement connue du système d'information de l'institution
- et/ou l'adresse mail préalablement connue du système d'information de l'institution ou d'autres éléments (nom de la dernière entreprise par exemple).

La vérification dans les bases de données de l'institution que la personne n'est pas connue comme décédée peut être effectuée.

### 4.3 GESTION DES ECARTS

En cas de non-authentification de l'internaute à l'un de ces deux niveaux d'authentification, l'inscription au service doit être refusée et la personne doit être invitée à prendre contact avec un centre de contact qui sera chargé de l'identifier ou à partir d'autres éléments constitutifs de son dossier, lesquels restent à l'appréciation de chaque groupe selon sa procédure habituelle.

## 5 MODE DE TRANSMISSION DES CLES D'ACCES AU PORTAIL (IDENTIFIANT – MOT DE PASSE)

Les données d'identification nécessaires à l'accès au service peuvent être diffusées :

- à la suite de la demande de l'internaute au moment de son inscription,
- à titre exceptionnel au moyen d'opérations de diffusion massive, sous réserve que ce mode de diffusion soit limité dans le temps et sur une partie restreinte de la population susceptible d'accéder au service. Ce type de diffusion ne doit pas entraîner l'ouverture automatique d'un compte, lequel doit toujours se faire sur une demande expresse du participant.

Le mot de passe doit toujours être délivré après une demande expresse du participant. L'identifiant de l'internaute et son mot de passe ne doivent en aucun cas figurer sur le même support.

L'identifiant et le mot de passe peuvent être transmis en temps réel, par mail ou par courrier postal<sup>1</sup> aux adresses enregistrées au moment de l'inscription au service avec comme recommandation l'utilisation de deux canaux de distribution différents. Si le même canal de transmission est utilisé, les envois de l'identifiant et du mot de passe doivent être désynchronisés dans le temps.

Les documents ou mails doivent mentionner de façon visible un avertissement attirant la responsabilité de l'internaute au cas où il transmettrait à des tiers ces données d'accès au service, par exemple :

*"Votre responsabilité est engagée au cas où vous transmettriez ou laisseriez à la disposition de tiers les données vous identifiant et les mots de passe vous permettant d'accéder au service du RIS en ligne"*

---

<sup>1</sup> Pour la CNIL, la diffusion du mot de passe par courrier à l'adresse déjà connue par le système d'information de l'intéressé est le moyen le plus sécurisé de diffusion.

## **6 GESTION DU COMPTE DE L'INTERNAUTE**

### **6.1 IDENTIFIANT POUR ACCEDER AU SERVICE**

L'identifiant utilisé par les institutions pour accéder au service peut être le NIR ou numéro de sécurité sociale<sup>2</sup> ou tout autre numéro interne dans le Groupe (numéro d'affiliation, ...).

### **6.2 GESTION DES MOTS DE PASSE**

Le mot de passe envoyé par l'institution doit être au minimum un mot de passe de 8 caractères alphanumériques.

Ce mot de passe doit être modifié par l'utilisateur à la première connexion en exigeant de l'internaute qu'il respecte également la règle minimale de 8 caractères alpha numériques.

Il est demandé de mettre en place un contrôle vérifiant que le mot de passe créé par l'intéressé ne contient pas des données correspondant à son nom ou à sa date de naissance.

Dans ces conditions, le mot de passe peut avoir une durée de vie illimitée.

A l'inverse, si ces contrôles ne sont pas mis en œuvre le mot de passe doit avoir une durée de vie limitée.

Il est recommandé également de signaler à l'internaute la date à laquelle sa dernière connexion a été effectuée avec le mot de passe.

Par ailleurs, une jauge ou tout autre symbolisme permettant de visualiser la solidité du mot de passe choisi par l'internaute peut être mise en place et affiché sur la page Internet.

### **6.3 GESTION DU COMPTE**

Avant la première authentification, le mot de passe doit avoir une durée de vie limitée à :

- 5 jours ouvrés si le mot de passe provisoire est transmis par mail,
- 30 jours s'il est transmis par courrier.

Après la première authentification, le compte a une durée de vie illimitée.

Le compte de l'internaute doit être bloqué en cas de 5 tentatives infructueuses cumulées. Cette notion de cumul s'entend quelque soit l'intervalle de temps entre les tentatives. Au delà, il doit être demandé à l'internaute de se réinscrire au service.

La session doit être désactivée en cas d'inactivité durant 30 minutes, l'internaute devant passer par une phase d'authentification avant de pouvoir utiliser à nouveau le service.

La page de gestion du service doit comporter un bouton visible de déconnexion volontaire.

---

<sup>2</sup> Attention, la possibilité d'utilisation du NIR doit s'entendre ne peut être utilisé dans des services commerciaux

## **6.4 PROCEDURE EN CAS DE PERTE DU MOT DE PASSE**

En cas de perte du mot de passe ou de verrouillage, un nouveau mot de passe à modifier dès réception peut être renvoyé à l'intéressé :

- au terme d'une nouvelle procédure d'inscription (procédure conseillée par la CNIL),
- au terme d'une procédure particulière d'identification auprès d'une hot line,
- au terme d'une réponse positive à une question secrète.

Dans ce dernier cas, le mot de passe devra être obligatoirement renvoyé par courrier postal (recommandation CNIL).

S'il y a une question secrète, elle doit être systématiquement et obligatoirement renseignée au cours de l'inscription. Deux réponses erronées à la question secrète doivent entraîner le blocage du compte et l'obligation pour l'intéressé de se réinscrire.

## **7 ELEMENTS TECHNIQUES**

### **7.1 LIAISON HTTPS OBLIGATOIRE**

La mise en place d'une liaison https entre l'internaute et le service de RIS en ligne est obligatoire.

### **7.2 GESTION DES TRACES**

Les institutions doivent s'assurer obligatoirement de conserver les traces des transactions d'accès au service du RIS en ligne. La durée de conservation sera précisée ultérieurement ou la forme de celles-ci seront précisées ultérieurement.

Il est conseillé également de gérer des systèmes et une architecture permettant de se prémunir des demandes d'accès faits en masse.

## **8 POLITIQUE DE REPRISE DU PASSE**

Dans le cadre de la mise en place du RAP en ligne, les institutions ont été amenées à délivrer des codes d'accès (identifiant, mot de passe) pour accéder à ce service. La mise en place du service du Ris en ligne soulève la question de la reprise du stock des identifiants ne répondant pas aux critères de qualité requis par ce nouveau service.

Il a été décidé que :

- Qu'à partir de la date d'ouverture du service du RIS-e, les personnes sollicitant le service du RAP ou du RIS-e pour la première fois devaient se voir attribuer un niveau d'authentification respectant les exigences de ce cahier des charges ;
- Que les personnes ayant reçu avant cette date une authentification dans le cadre du service du RAP peuvent continuer à utiliser les règles d'authentification actuelles à charge pour les Groupes de les faire basculer progressivement dans les nouvelles règles, selon un plan d'actions restant sous leur responsabilité.

## **9 SUIVI DE MISE EN ŒUVRE DES REGLES D'AUTHENTIFICATION**

Il est rappelé que seuls les portails présentant le niveau requis de sécurité pourront être utilisés pour véhiculer les demandes et fournir des Ris-e.

Dans le cadre du déploiement du RIS-e dans les Groupes, un suivi sera effectué auprès de chaque Groupe pour mesurer le niveau de mise en œuvre de ces règles et suivre, si nécessaire, les plans d'actions nécessaires pour assurer le niveau requis.