Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Ministère délégué au budget et à la réforme de l'Etat

Direction Générale de la Modernisation de l'Etat

Référentiel Général d'Interopérabilité

Interopérabilité Organisationnelle

Normes et recommandations

Références documentaires

<1> Ordonnance n°2005-1516 sur les échanges électr oniques du 8 décembre 2005,

(Journal Officiel du 9 décembre 2005).

<2> Introduction au Référentiel Général d'Interopérabilité. V1.4 du 26-02-2006.

<3> Référentiel Général d'Interopérabilité. Glossaire.

<4> Schéma Directeur Adèle.

Sommaire

Index des Règles d'Interopérabilité organisationnelle

Présentation générale et guide d'usage

Présentation

L'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives elle-même, s'inscrit dans la démarche globale du Gouvernement de réforme de l'Etat, plus précisément dans ses aspects de simplification des démarches des usagers et de facilitation de l'accès de ces derniers aux services publics.

Cette ordonnance introduit la notion de Référentiel Général d'Interopérabilité (RGI) dont l'objet est de fixer les règles permettant d'assurer l'interopérabilité de tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives.

Une des composantes du RGI concerne l'interopérabilité organisationnelle et le volet sécurité, ensemble de normes et de standards qui doivent être utilisés par les autorités administratives et dont le respect conditionne le développement de l'offre de services administratifs accessibles par voie électronique.

L'objectif du présent document est de traiter cette composante et de cibler plus particulièrement les chefs de projet, architectes et développeurs travaillant sur des projets relatifs à l'Administration électronique. Afin de renforcer son caractère opérationnel, il se matérialise sous la forme d'un ensemble de règles d'interopérabilité qui précise les normes, standards, recommandations, principes de mise en œuvre et composants à utiliser.

L'interopérabilité organisationnelle est la capacité d'identifier les acteurs et les procédures organisationnelles intervenant dans la fourniture d'un service spécifique d'administration en ligne et de parvenir à un accord entre ces acteurs et procédures pour structurer leur interaction. En d'autres termes, il s'agit de définir leurs « interfaces d'entreprise ».

L'interopérabilité organisationnelle concerne principalement la définition de processus qui sont mis en œuvre lors d'échanges entre administration ou avec les usagers.
Le but est de mettre à disposition des usagers des services disponibles, facilement identifiables, accessibles et centrés sur l'usager.

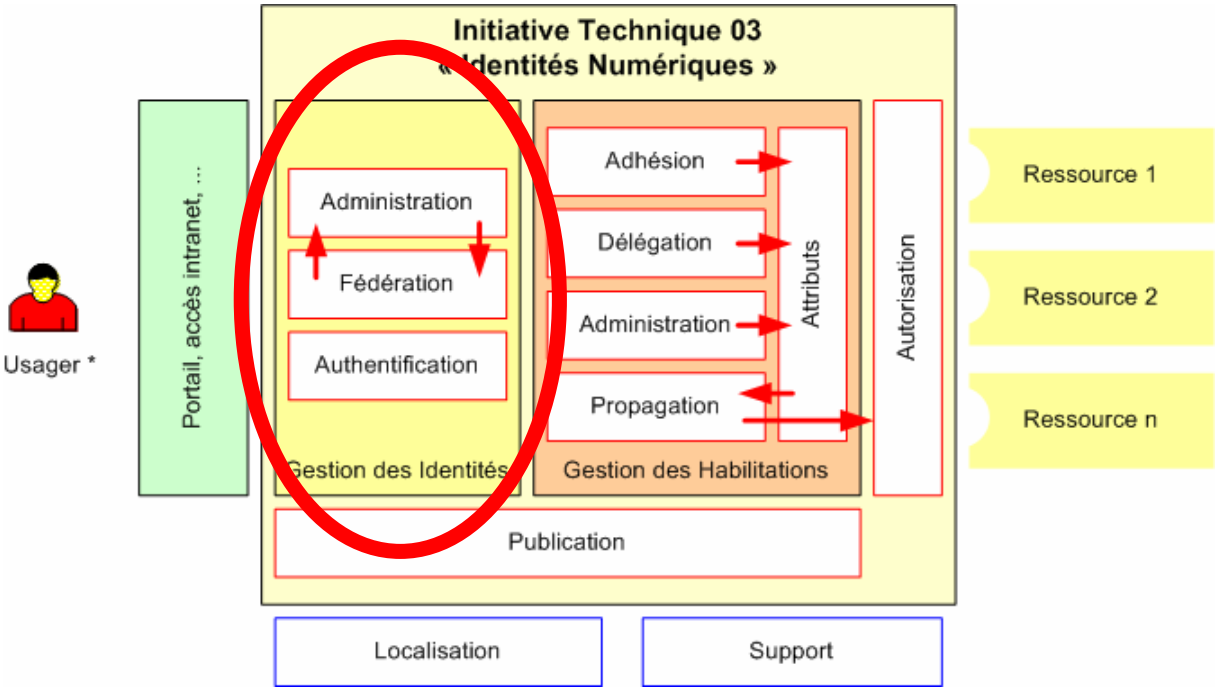
Ce document respecte les conditions d'élaboration, d'approbation, de modification et de publication fixées par décrets.

En application du principe de subsidiarité, ces règles ne s'appliquent qu'aux problématiques d'échange (pris au sens large) entre les usagers et l'Administration ainsi qu'entre les différentes autorités administratives. Pour leurs besoins internes, les administrations et les collectivités territoriales restent libres du choix des normes, principes et composants à utiliser.

1 - Gestionnaire d'Identités Numériques

Objectif	Dans le contexte de l'Administration Electronique, les besoins d'interopérabilité relatifs à la gestion des identités des agents publics concernent notamment la possibilité pour ces derniers d'accéder à des applications mises en place par d'autres administrations que la leur. Pour cela, il convient d'adopter des normes et des standards communs pour permettre une identification transverse des agents publics ainsi qu'une propagation de droits et rôles afin de mettre en place des mécanismes de type « Single Sign On ».
Domaine d'interopérabilité	• Intégration des services de sécurité • Accès aux services en ligne • Intégration entre portails, • Intégration entre portails et téléservices, • Intégration entre portails et services administratifs • Intégration entre téléservices.
Responsable	Bruno Deschemps

1.1 - Urbanisation fonctionnelle



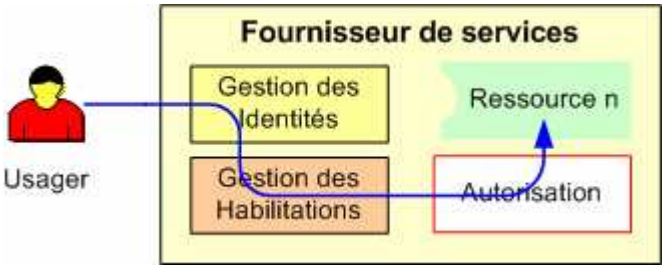
Le *Gestionnaire d'Identités* offre les services :

- de gestion du cycle de vie des comptes utilisateurs ;
- d'accès à ces comptes.

1.2 - Scenarii de mise en oeuvre

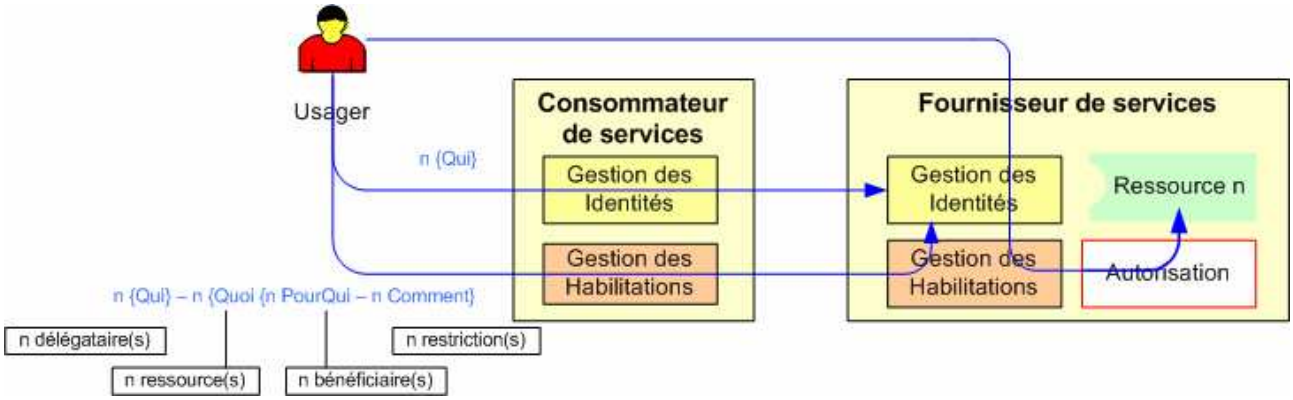
1.2.1 - Scénario n°1 :

Le *Consommateur de services* ne possède pas de *Gestionnaires d'Identités* et *d'Habilitations*. Il utilise ceux mis à disposition par le *Fournisseur de services* pour accéder aux ressources.



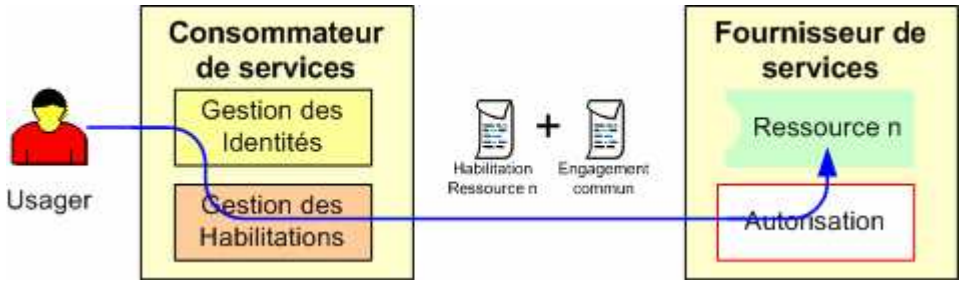
1.2.2 - Scénario n°2 :

L'usager possède un *Gestionnaire d'Identités & d'Habilitations* ; Il les utilise pour mettre à jour ceux mis à disposition par le *Fournisseur de services*. Il utilise ceux mis à disposition par le *Fournisseur de services* pour accéder aux ressources.



1.2.3 - Scénario n°3 :

L'usager possède un *Gestionnaire d'Identités & d'Habilitations* ; Il les utilise pour transférer ses droits et accéder aux ressource mises à disposition par le *Fournisseur de services*.



1.3 - Service « Administration des identités » (Agent)

1.3.1 - Description

Ce service consiste :

- à récupérer l'identifiant d'un *Agent* ;
- à construire son identité numérique ;
- à héberger cette identité numérique.

1.3.2 - Normes et standards

1.3.3 - Principe de mise en oeuvre

Seul le scénario n°3 est retenu.

RIO 0100	Il est OBLIGATOIRE que l'identité numérique d'un *Agent* soit construite depuis le SIRH de sa structure d'appartenance.

RIO 0101	Il est INTERDIT d'héberger l'identité numérique d'un *Agent* inconnu du Système d'Information des Ressources Humaines du *Fournisseur de services*.

RIO 0102	Il est OBLIGATOIRE que l'identifiant d'un *Agent* soit indépendant de données non pérennes.

L'appartenance d'un *Agent* à un service, une sous direction, ... n'étant pas pérenne, l'utilisation de ces identifiants est donc prohibée.

1.3.4 - Composants

1.3.5 - Exemples d'initiatives sectorielles

1.4 - Service « Administration des identités » (Professionnel)

1.4.1 - Description

Ce service consiste :

- à attribuer un identifiant à un usager *Professionnel* ;
- à construire son identité numérique ;
- à héberger cette identité numérique.

1.4.2 - Normes et standards

1.4.3 - Principes de mise en œuvre

Les scénarii 1, 2 & 3 sont retenus.

RIO 0105	Il est OBLIGATOIRE, pour accéder aux services nécessitant une reconnaissance ultérieure ou une sauvegarde de contexte, d'héberger l'identité numérique de l'usager *Professionnel.*

RIO 0107	Il est OBLIGATOIRE d'attribuer aux usagers *Professionnels* d'un Gestionnaire d'identités un identifiant unique.

Cet identifiant sera unique au sein du Gestionnaire d'Identités donnant accès à un collection « cohérente » de télé-services. La cohérence étant apportée par une offre « métier » ou « sectorielle ».

RIO 0103	Il est OBLIGATOIRE que l'identifiant de l'usager *Professionnel* soit indépendant de données non pérennes.

L'appartenance d'un usager *Professionnel* à un SIREN, SIRET, ... n'étant pas pérenne, l'utilisation de ces identifiants est donc prohibée.

RIO 0109	Il est INTERDIT de laisser la définition de l'identifiant à l'initiative de l'usager *Professionnel*.

1.4.4 - Composants

1.4.5 - Exemples d'initiatives sectorielles

1.5 - Service « Administration des identités » (Particulier)

1.5.1 - Description

Ce service consiste :

- à attribuer un identifiant à un usager *Particulier* ;
- à construire son identité numérique ;
- à héberger cette identité numérique.

1.5.2 - Normes et standards

1.5.3 - Principes de mise en œuvre

Seul le scénario n°1 est retenu.

RIO 0106	Il est OBLIGATOIRE, pour accéder aux services nécessitant une reconnaissance ultérieure ou une sauvegarde de contexte, d'héberger l'identité numérique de l'usager *Particulier.*

RIO 0108	Il est OBLIGATOIRE d'attribuer aux usagers *Particuliers* d'un Gestionnaire d'identités un identifiant unique.

RIO 0104	Il est OBLIGATOIRE que l'identifiant de l'usager *Particulier* dépende de données pérennes.

La possession d'une d'adresse électronique par un usager *Particulier* n'étant pas pérenne, l'utilisation de cet identifiant est donc prohibée.

RIO 0110	Il est DECONSEILLE de laisser la définition d'un identifiant à l'initiative de l'usager *Particulier*.

1.5.4 - Composants

1.5.5 - Exemples d'initiatives sectorielles

1.6 - Service « Authentification » (Agent)

1.6.1 - Description

Cf. IT05 « Sécurité des services »

1.6.2 - Normes et standards

Cf. IT05 « Sécurité des services »

1.6.3 - Principes de mise en œuvre

Seul le scénario n°3 est retenu.

RIO 0111	Il est OBLIGATOIRE que les usagers *Agents* s'authentifient auprès de leur structure d'appartenance.

1.6.4 - Composants

Cf. IT05 « Sécurité des services »

1.6.5 - Exemples d'initiatives sectorielles

Cf. IT05 « Sécurité des services »

1.7 - Service « Authentification » (Professionnel)

1.7.1 - Description

Cf. IT05 « Sécurité des services »

1.7.2 - Normes et standards

Cf. IT05 « Sécurité des services »

1.7.3 - Principes de mise en œuvre

Les scenarii 1, 2 & 3 sont retenus.

RIO 0112	Il est RECOMMANDE que l'usager Professionnel qui possède un Gestionnaire d'Identités s'authentifie auprès de celui-ci..

RIO 0114	Il est OBLIGATOIRE que l'usager Professionnel s'authentifie auprès du Fournisseur de service s'il ne possède pas de Gestionnaire d'Identités.

Le scénario n°3 sera recommandé. Une phase transitoire du type « scénario n°2 » permettra de respecter les politiques de gestion des identités et des habilitations des *Consommateurs de services*.

1.7.4 - Composants

Cf. IT05 « Sécurité des services »

1.7.5 - Exemples d'initiatives sectorielles

Cf. IT05 « Sécurité des services »

1.8 - Service « Authentification » (Particulier)

1.8.1 - Description

Cf. IT05 « Sécurité des services »

1.8.2 - Normes et standards

Cf. IT05 « Sécurité des services »

1.8.3 - Principes de mise en œuvre

Seul le scénario n°1 est retenu.

RIO 0113	Il est OBLIGATOIRE que les usagers *Particuliers* s'authentifient auprès du Gestionnaire d'Identités mis à disposition par le *Fournisseur de services*.

1.8.4 - Composants

Cf. IT05 « Sécurité des services »

1.8.5 - Exemples d'initiatives sectorielles

Cf. IT05 « Sécurité des services »

1.9 - Service « Fédération des identités » (Usagers)

1.9.1 - Description

Objectif	Ces règles ont pour objectif de définir les dispositifs à mettre en place pour fournir aux usagers des dispositifs de *Single Sign-On* (*SSO*) entre différents téléservices. Ces règles visent à garantir l'interopérabilité des dispositifs d'authentification et d'identification des usagers afin de rendre possible la mise en place de ces mécanismes de SSO dans des portails.
Domaine d'interopérabilité	• Accès aux services en ligne • Intégration entre portails et téléservices
Responsable	Benoît Boute

1.9.2 - Principe de fédération

La fédération entre différents systèmes consiste à partager des services de gestion des identités (authentification, échanges d'attributs, autorisation, etc...) entre différents systèmes (différentes entreprises ou au sein d'une même organisation) sans avoir à partager le même référentiel ni la même infrastructure de gestion des identités.

Dans l'objectif de fournir aux usagers des dispositifs leur permettant d'accéder à différents téléservices sur la base d'une authentification unique, la fédération d'identités est jugée comme le seul moyen technique permettant le respect des libertés individuelles. En effet :

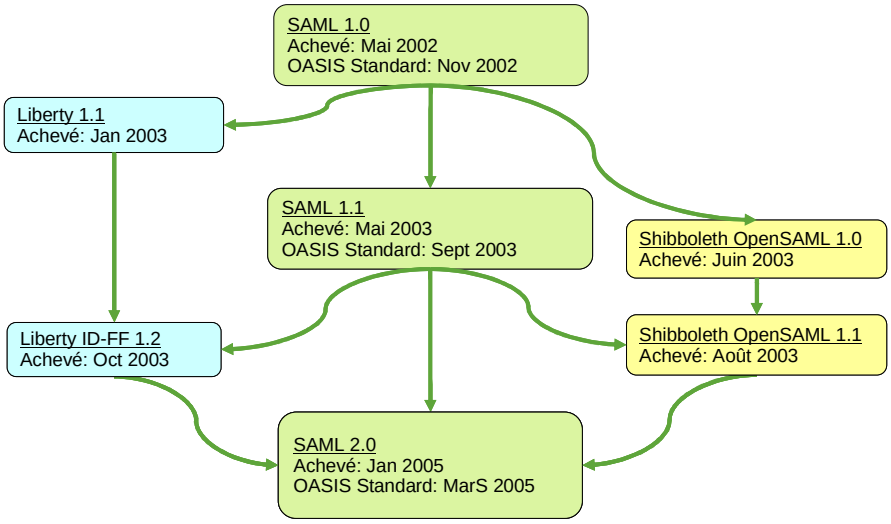
- elle permet à chaque administration de conserver sa propre gestion de l'identification des usagers en préservant les identifiants sectoriels ;
- elle permet d'éviter la mise en place d'un identifiant unique commun à plusieurs administrations ;
- elle évite de constituer une base nationale et centrale de correspondance entre les identifiants sectoriels de chaque individu.

RIO 0154	Il est OBLIGATOIRE d'utiliser un système de fédération d'identité pour la mise en place de systèmes d'authentification unique des usagers dans des téléservices dépendant de différentes administrations.

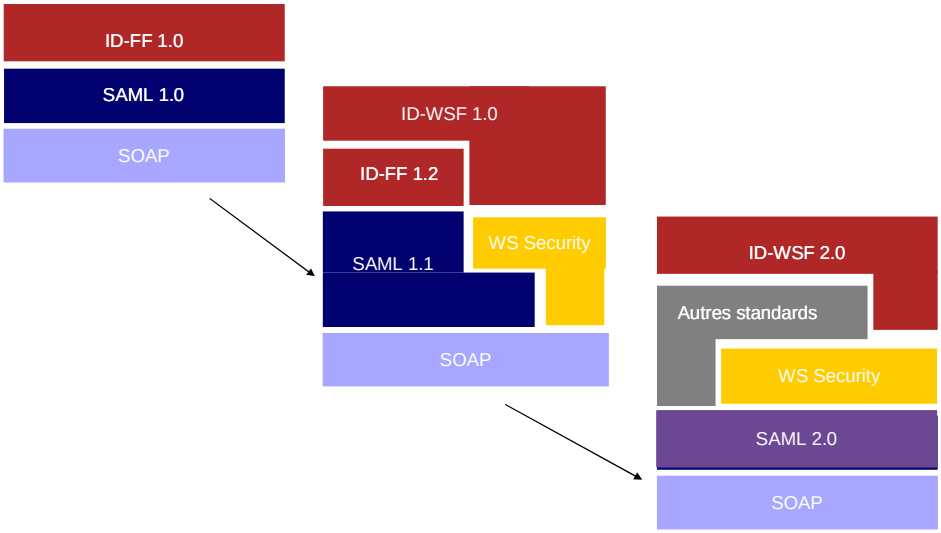
1.9.3 - Normes et standards

SAML 2.0 (OASIS) et ID-FF (Liberty Alliance)

Les travaux sur le protocole d'assertion SAML sont menés par l'OASIS. Ceux-ci se sont menés en parallèle des travaux menés par le consortium Liberty Alliance. Ce consortium, initié par Sun en septembre 2001 et soutenu par plus de 150 entreprises ou organismes internationaux (dont AOL, HP, France Telecom, IBM, Nokia…), spécifie en particulier un système d'authentification distribué qui permet à un internaute navigant sur plusieurs sites se faisant confiance de s'authentifier une seule fois selon le principe du *single sign on* (Id-FF). Cette spécification (Id-FF 1.2) a été intégrée dans le standard d'assertion de sécurité **SAML 2.0**. Des principes complémentaires (Id-WSF) permettent aussi de transporter des attributs liés à l'identité.



Interactions Liberty Alliance / ID-FF et SAML



Evolutions Liberty Alliance / ID-FF et SAML

Nom + Version	Spécification	Etat	Date
SAML 2.0	http://www.oasis-open.org/specs/index.php#samlv2.0	OASIS Standard	Mars 2005
Id-FF 1.2	http://projectliberty.org/resources/specifications.php#box1	Liberty Alliance Final Specification	Oct 2003
Id-WSF 1.1	http://projectliberty.org/resources/specifications.php#box2a	Liberty Alliance Final Specification	?

Les composants principaux d'une fédération d'identités sont :

- **Fournisseur d'identités (IdP)** : c'est une entité qui gère les informations relatives à l'identification et à l'authentification, sans gérer l'identité. Il porte l'ensemble des fédérations pour l'usager pseudonyme.
- **Fournisseur de services (SP)** : C'est une entité qui fournit des services (ou des biens) à l'usager et utilise le fournisseur d'identité pour l'authentification.
- **Fédération** : C'est une relation établie entre plusieurs entités, se faisant confiance, à l'initiative de l'usager. Elle permet l'accès direct à un téléservice.
- **Cercle de confiance (CoT)** : C'est un ensemble d'entités amenées à partager et à échanger de l'information. Il est formé d'un portail s'appuyant sur un fournisseur d'identité et l'ensemble des fournisseurs de services. Un cercle de confiance est défini par un (ou n) fournisseurs d'identité.

- **Clé de fédération** : Les différents fournisseurs de service ne peuvent communiquer directement entre eux à propos de l'identité d'un utilisateur. Ils ne peuvent échanger des informations le concernant qu'avec le fournisseur d'identité. Cela permet d'obtenir l'assurance du respect de la vie privée ; afin de garantir l'intégrité et la non-révocabilité de l'échange, une tierce partie de confiance (IdP) émet un jeton de sécurité qui identifie la session, mais pas l'utilisateur, (certificats X.509, clé Kerberos). Ceci, afin de préserver son anonymat.

Il existe d'autres spécifications traitant de la fédération des identités (exemple de WS-Federation basée sur la pile protocolaire WS-*) mais les spécifications SAML et Id-FF sont les plus généralisées parmi les spécifications ouvertes et libres de droit.

Utilisation des standards Liberty Alliance pour la constitution de cercles de confiance

RIO 0156	Il est RECOMMANDÉ d'utiliser SAML 2.0 ou ID-FF 1.2 pour fédérer des services sur un cercle de confiance inter administrations

RIO 0157	Il est RECOMMANDÉ d'utiliser ID-WSF 1.1 pour échanger des attributs entre des services fédérés sur un cercle de confiance inter administrations..

1.9.4 - Principes de mise en œuvre

Principes de constitution et d'interopérabilité des cercles de confiance

Dans l'objectif de développer des portails de services sectoriels et/ou locaux, il est nécessaire de pouvoir créer une fédération depuis l'un de ces portails vers tous les téléservices nationaux ou locaux.
L'existence de portails locaux et de téléservices locaux qui fonctionnent sur un modèle de fédération d'identité (pour permettre notamment l'authentification mutualisée entre ces services) passe par la mise en place de plateformes.
Chaque plateforme devra constituer un cercle de confiance en gérant un fournisseur d'identité et en agrégeant autour de celui-ci des portails locaux d'accès et des téléservices.
Des principes d'interopérabilité devront être respectés par les différents acteurs pour permettre :

- à l'usager de choisir son portail parmi l'offre proposée, de fédérer l'ensemble des téléservices existants et à venir et de s'y retrouver dans une relation de confiance avec ces nouveaux usages,
- aux différentes administrations de développer les téléservices avec un seul modèle de fédération d'identité et d'éviter de gérer plusieurs intégrations avec différents portails d'accès,
- de créer les conditions pour que différentes plates-formes de service puissent concentrer et organiser cette offre de portails.

L'idée est de pouvoir regrouper les téléservices dans des cercles de confiance suivant une certaine logique. Un cercle de confiance étant défini par un ensemble d'opérateurs de téléservices ayant noué entre eux des relations contractuelles dans l'objectif de construire un bouquet de services cohérent et accessible par l'usager sur la base d'une authentification unique.

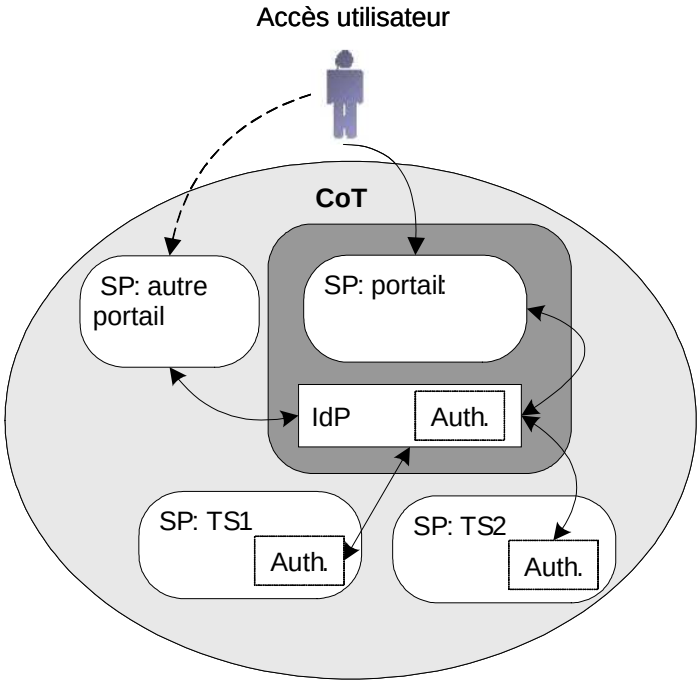
A titre d'exemple, on pourra trouver différents types de cercles de confiance, comme le cercle de confiance constitué par le portail *mon.Service-Public.fr* et ses partenaires, des cercles de confiance structurés autour de portails de communes ou communautés de communes, des cercles de confiances thématiques (santé, éducation, etc…).

Des principes sont préconisés afin d'apporter une homogénéité dans la constitution des cercles de confiance :

- Un cercle de confiance (CoT) est défini par un et un seul fournisseur d'identité (IdP)
- Au sein d'un cercle de confiance il peut y avoir plusieurs portails

Par ailleurs on ne rend pas visible à l'utilisateur la distinction entre le portail et fournisseur d'identité. La notion d'identité numérique n'étant pas intuitive pour l'usager, la seule notion présentée à l'usager est le compte portail ; d'où la notion de Portail « référent ». Pour un usager, le portail référent est celui qui « porte » l'identité de cet usager dans ce cercle de confiance (CoT). C'est le portail du cercle de confiance par lequel un utilisateur donné devra accéder s'il veut bénéficier de tous les services associés à sa fédération d'identités.

Cercle de confiance unique

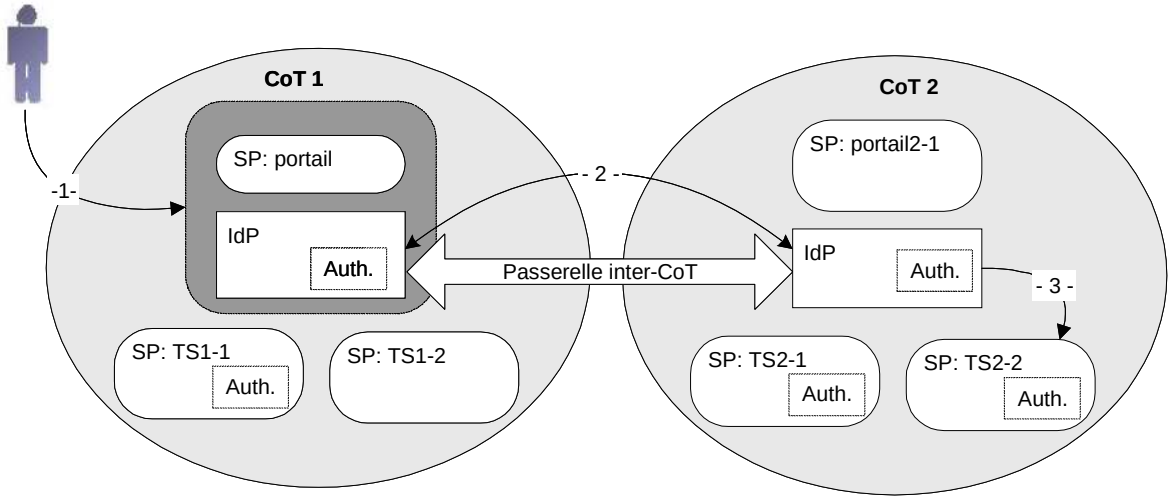


Un cercle de confiance (CoT) est un ensemble d'entités (IdP – identity provider, TS – télé-service, portail…) qui ont établi un rapport de confiance et qui vont être amenées à partager des accès et à échanger de l'information concernant l'usager.
Voici les pré-requis retenus :

- Il existe un seul IdP au sein d'un CoT
- Un seul service d'authentification est associé à un IdP.
- Il peut exister plusieurs portails « fédérateurs » au sein d'un même CoT.
- Il existe par définitions plusieurs télé-services (TS) au sein d'un même CoT.
- D'un point de vue Utilisateur, le portail, l'IdP et le service d'authentification ne forment qu'une seule entité. Un usager ne pouvant pas comprendre la notion d'IdP mais uniquement celle du portail, les deux notions sont liées de son point de vue.

Interconnexion de cercles de confiance

L'utilisation du « modèle de fédération lié » est préconisée : plusieurs cercles de confiance indépendants liés entre eux par des passerelles au niveau de l'IdP.



Un des processus d'invocation d'un télé-service par un usager hors du cercle de confiance de son portail référent est le suivant :

1. Authentification de l'usager auprès de son portail référent.
2. Utilisation de la passerelle inter-CoT et de la fédération entre les IdP.
3. Propagation de l'authentification (si la fédération IdP – TS2-2 existe pour cet usager) auprès du télé-service demandé et accès au service.

Bien entendu, les autres cas sont aussi possibles : invocation à partir d'un accès direct au SP:portail2-1 avec ou sans authentification préalable à son portail référent.

RIO 0155	Il est RECOMMANDÉ d'utiliser un modèle de fédération reposant sur une passerelle inter fournisseurs d'identité pour construire une authentification unique des usagers sur des services appartenant à des cercles de confiance différents.

Il est RECOMMANDÉ d'utiliser un modèle de fédération reposant sur une passerelle inter fournisseurs d'identité pour construire une authentification unique des usagers sur des services appartenant à des cercles de confiance différents.

L'interopérabilité de ces cercles de confiance sera d'autant plus aisée que ceux-ci s'appuieront sur les mêmes technologies de fédération. C'est pourquoi il est recommandé d'utiliser SAML 2.0 ou ID-FF 1.2 quel que soit le cercle de confiance constitué.

Exemple de mise en œuvre : ***mon.Service-Public.fr***

Le projet *mon.service-public.fr* sous le pilotage de la DGME/MINEFI mettra en place un cercle de confiance entre téléservices de plusieurs administrations en vue d'offrir aux usagers un accès « unifié » à l'ensemble de leurs services administratifs.

Pour ce faire, **le cercle de confiance *mon.service-public.fr* s'appuiera une fédération d'identités respectant le protocole SAML 2.0 et des échanges d'attributs conformément à ID-WSF 1.1**.

Dans la mesure où de nombreux partenaires fédéreront leurs services avec ce portail, les services offerts par ces partenaires pourront être accessibles dans le cadre d'une authentification unique pour n'importe quel autre cercle de confiance avec lequel le projet *mon.service-public.fr* aura bâti une interconnexion d'IdP.

Le portail existe déjà en version pilote déployée sur ID-FF 1.1 et ID-WSF 1.0. La version industrielle sera déployée au printemps 2007.

1.9.4.1. Composants associés : Kit d'intégration MSP

Toolkit d'intégration *mon.Service-Public.fr* (MINEFI / Direction Générale de la Modernisation de l'Etat)

Attention : ce toolkit d'intégration sera conçu dans le cadre du projet mon.service-public.fr ; il devrait être mis à disposition au quatrième trimestre 2006

Pour simplifier la tâche technique d'intégration des services partenaires au portail *mon.Service-Public.fr*, un kit d'intégration (toolkit) porteur des fonctions de gestion d'accès au travers de la fédération d'identité ainsi que des fonctions relatives à la communication et à l'espace de données sera mis à leur disposition. Ceci permettra aussi de normaliser le comportement vu de l'utilisateur lors de l'accès, de la fédération, mais aussi lors du pré-remplissage de formulaires.

Ce kit d'intégration comprendra :

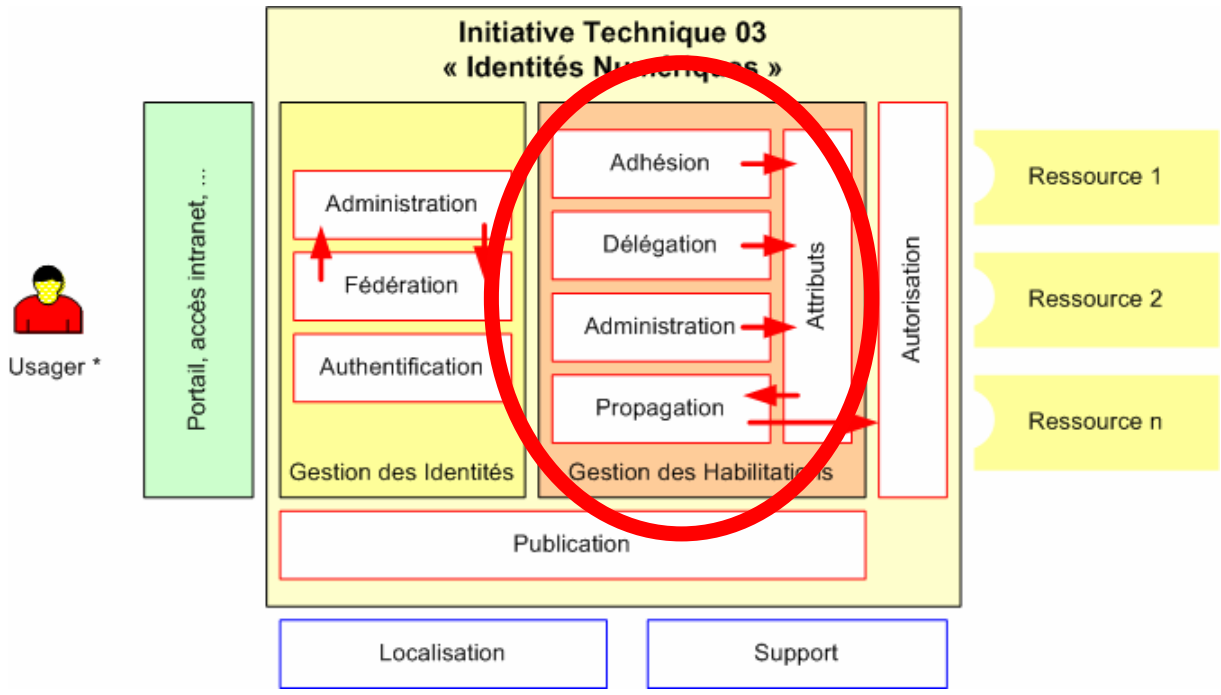
- un ensemble d'objets et de fonctions permettant de prendre en charge tous les échanges avec la brique de gestion de l'identité (création, utilisation, suppression de fédérations).
- un ensemble de technologies permettant d'assurer le transfert d'information entre l'espace de données et les formulaires mais aussi les fonctions de routage de messages pour injecter des informations dans le tableau de bord *mon.Service-Public.fr*.
- une implémentation de référence qui démontre la mise en œuvre de l'ensemble des fonctions du toolkit et le séquencement standard de l'accès au dossier de suivi dont chaque SI Partenaire pourra dériver son implémentation.
- une implémentation de référence qui démontre la mise en œuvre d'un téléservice factice (contact et formulaire) assurant les échanges de données relatifs à l'envoi de messages dans le tableau de bord et à l'utilisation ou la production d'informations dans l'espace de données dont chaque SI Partenaire pourra dériver son implémentation.
- le jeu de bouchons nécessaires aux partenaires pour réaliser et tester de manière exhaustive l'intégration de ce kit avec d'une part, leur système d'information, d'autre part, le système bâti dans le cadre du présent marché (gestion de l'identité, espace de données, routeur de messages…).

Le code et les spécifications de ce kit seront ouverts et libres de droit de manière à en faciliter l'appropriation et la modification par les partenaires et la communauté. Ce kit d'intégration sera donc mis à la disposition de la communauté (code source, documentations...) dans la forge « Admisource ».
Enfin, s'il s'agit d'un ensemble d'APIs, il sera développé dans une technologie connue des partenaires du projet et communément répandue, vraisemblablement dans des technologies Java.

2 - Gestionnaire d'Habilitations

Objectif	Dans le contexte de l'Administration Electronique, les besoins d'interopérabilité relatifs à la gestion des droits d'accès des agents publics concernent notamment la possibilité pour ces derniers d'accéder à des applications mises en place par d'autres administrations que la leur. Pour cela, il convient d'adopter des normes et des standards communs pour permettre une administration simplifiée et une propagation sécurisée de droits et rôles
Domaine d'interopérabilité	• Intégration des services de sécurité • Accès aux services en ligne • Intégration entre portails, • Intégration entre portails et téléservices, • Intégration entre portails et services administratifs • Intégration entre téléservices.
Responsable	Bruno Deschemps

2.1 - Urbanisation fonctionnelle & scenarii de mise en oeuvre



Le *Gestionnaire d'Habilitations* offre les services :

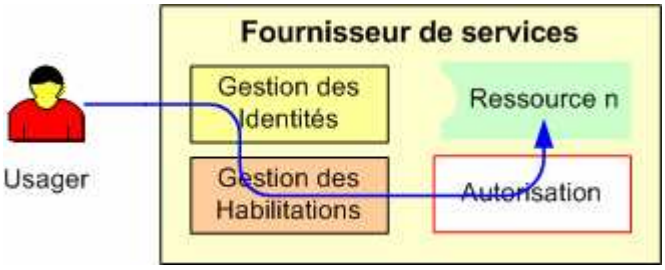
- de gestion du cycle de vie des droits d'accès ;
- d'attribution des droits d'accès ;
- d'élaboration des droits d'accès ;

- de transfert de ses droits d'accès vers les ressources mises à disposition par le Fournisseur de services.

2.2 - Scenarii de mise en oeuvre

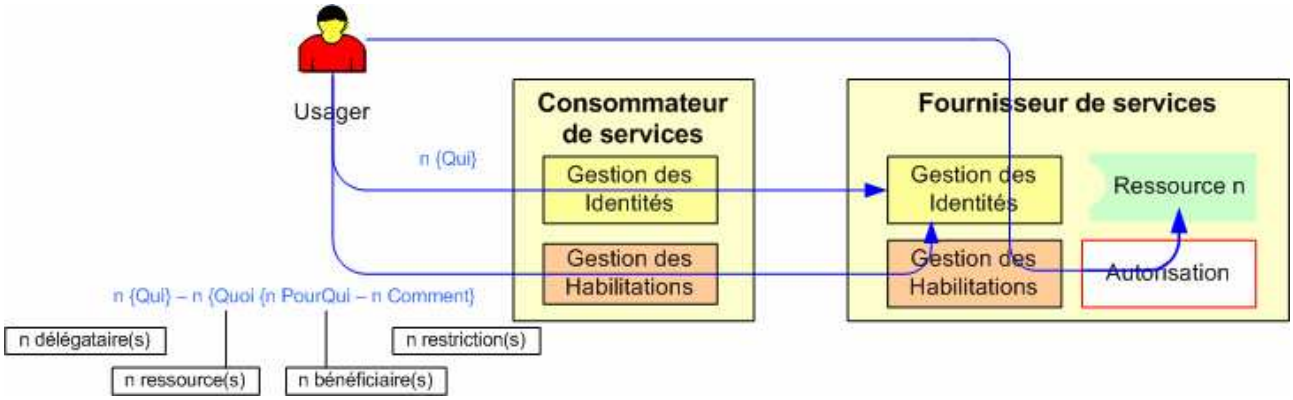
2.2.1 - Scénario n°1 :

Le *Consommateur de services* ne possède pas de *Gestionnaires d'Identités* et *d'Habilitations*. Il utilise ceux mis à disposition par le *Fournisseur de services* pour accéder aux ressources.



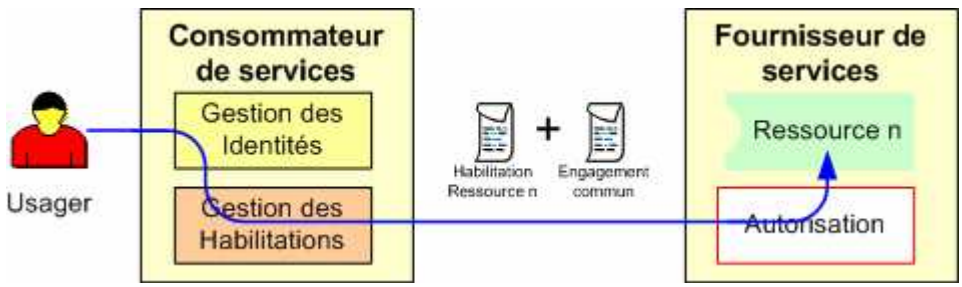
2.2.2 - Scénario n°2 :

L'usager possède un *Gestionnaire d'Identités & d'Habilitations* ; Il les utilise pour mettre à jour ceux mis à disposition par le *Fournisseur de services*. Il utilise ceux mis à disposition par le *Fournisseur de services* pour accéder aux ressources.



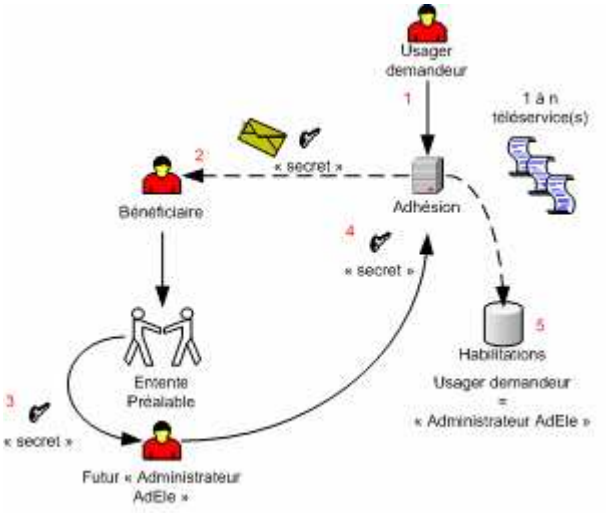
2.2.3 - Scénario n°3 :

L'usager possède un *Gestionnaire d'Identités & d'Habilitations* ; Il les utilise pour transférer ses droits et accéder aux ressource mises à disposition par le *Fournisseur de services*.



2.2.4 - Scénario A :

L'usager demandeur doit prouver qu'il est mandaté par le *Bénéficiaire* des ressources. Cela se matérialise par la présentation d'un « secret ». Ce « secret », envoyé ou en possession préalable du *Bénéficiaire*, est délivré par le *Bénéficiaire* à la personne qu'il désiré mandater. Cet échange a lieu au cours de la phase « d'Entente Préalable ».

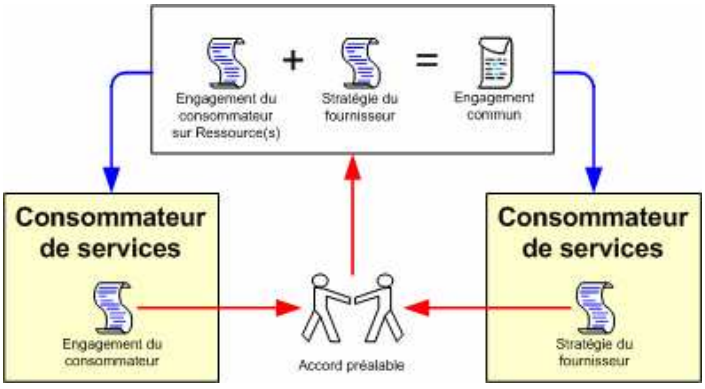


Remarques:

- Ce processus s'applique aux usagers *Professionnel* & *Particulier* ;
- Dans le scénario usager *Particulier*, l'usager demandeur est identique au *Bénéficiaire* ;
- Dans le scénarion usager *Professionnel*, si l'usager demandeur peut alléguer sa qualité professionnelle, celle-ci peut se substituer au « secret » (cas des usagers agissant dans le cadre d'une profession reglementée).

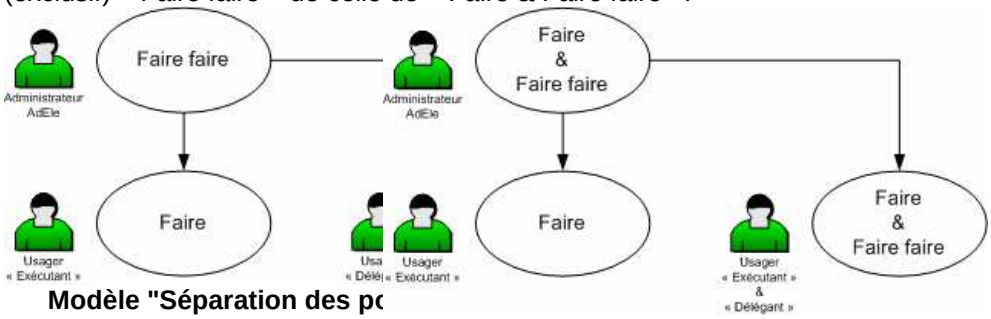
2.2.5 - Scénario B :

Un « Engagement commun » – négociation élaborée entre le *Consommateur de services* et le *Fournisseur de services* – contient les modalités d'accès aux ressources mises à disposition par le *Fournisseur de services*. Les demandes d'accès aux ressources mises à disposition par le *Fournisseur de services* font référence à cet « Engagement commun ».



2.2.6 - Scénario C :

L'attribution de droits d'accès devra offrir la possibilité de distinguer l'aptitude pour un usager de « Faire » ou (exclusif) « Faire faire » de celle de « Faire & Faire faire ».



Modèle "Séparation des pc

Modèle "cumulation des pouvoirs"

2.3 - Service « Adhésion » (Agent)

2.3.1 - Description

Ce service consiste à attribuer à un usager *Agent* une collection de droit d'accès pour le compte d'un *Bénéficiaire.*

2.3.2 - Normes et standards

2.3.3 - Principes de mise en œuvre

Seul les scenarii n°3 & B sont retenus.

RIO 0115	Il est OBLIGATOIRE de conditionner les modalités techniques et fonctionnelles d'accès aux services d'un *Fournisseur de services* par l'élaboration d'une convention reflétant « l'Engagement commun » *Consommateur de services* / *Fournisseur*.

RIO 0116	Il est RECOMMANDE de privilégier un accès aux ressources d'un *Fournisseur de services* se basant sur le rôle de l'usager *Agent* en lieu et place de son identifiant.

2.3.4 - Composants référencés

2.3.5 - Exemples d'initiatives sectorielles

2.4 - Service « Adhésion » (Professionnel)

2.4.1 - Description

Ce service consiste à attribuer à un usager *Professionnel* une collection de droit d'accès pour le compte d'un *Bénéficiaire.*

Le *Bénéficiaire* est une Personne Physique Représentant Légal d'une Personne Morale.

2.4.2 - Normes et standards

2.4.3 - Principes de mise en œuvre

- Dans le cas d'un scénario 1 ou 2 associé au scénario A & C :

RIO 0119	Il est RECOMMANDE de présenter un secret "technique" afin de prouver sa légitimité à utiliser une collection de télé-services pour le compte du Représentant Légal d'une entreprise bénéficiaire.

RIO 0120	Il est OBLIGATOIRE que le secret « technique » soit indépendant de toutes données gérées par un télé-service.

RIO 0121	Il est RECOMMANDE que le secret « technique » présenté véhicule la volonté (ou non) du Représentant Légal de l'entreprise bénéficiaire de choisir une organisation des chaînes de délégation de droits d'accès avec séparation des pouvoirs.

RIO 0122	Il est RECOMMANDE que le secret « technique » soit à usage limité dans le temps.

RIO 0123	Il est OBLIGATOIRE d'envoyer le secret "technique" au Représentant Légal de l'entreprise bénéficiaire de la collection de télé-services.

RIO 0124	Il est OBLIGATOIRE que l'échange du secret "technique" entre le Représentant Légal de l'entreprise bénéficiaire et l'usager *Professionnel* qu'il choisit de mandater pour l'utilisation des télé-services, se fasse au cours de la phase dite d'« *Entente Préalable* ».

RIO 0125	Il est OBLIGATOIRE d'attribuer le rôle "Administrateur AdEle" aux usagers *Professionnels* présentant un secret "technique" valide. L'usager *Professionnel* possédant ce rôle « est » ou « est mandaté par » le Représentant Légal auprès de l'Administration.

RIO 0126	Il est RECOMMANDE d'attribuer les droits d'accès à un nouveau télé-service aux usagers *Professionnels* possédant préalablement le rôle "Administrateur AdEle". L'usager *Professionnel* possédant ce rôle « est » ou « est mandaté par » le Représentant Légal auprès de l'Administration.

La mise à disposition d'un nouveau télé-service enrichira la collection d'habilitations des usagers *Professionnel* possédant le rôle « Administrateur Adèle »; on parlera d'adhésion « implicite » (par opposition à l'adhésion « explicite » nécessitant la présentation d'un secret « technique »).

RIO 0118	Il est RECOMMANDE d'archiver une trace des événements associés au processus d'adhésion attribuant des droits d'accès.

Cette trace sera générée, qu'il s'agisse d'une adhésion « implicite » (attribution de droits d'accès du à la possession d'une qualité, d'un rôle, ...) ou d'une adhésion « explicite » (attribution de droits d'accès suite à la présentation et validation d'un secret « technique » prouvant que l'usager est mandaté par le Représentant Légal de l'entreprise bénéficiaire des télé-services).

- Dans le cas du scénario n°3 associé au scénario B :

RIO 0115	Il est OBLIGATOIRE de conditionner les modalités techniques et fonctionnelles d'accès aux services d'un *Fournisseur de services* par l'élaboration d'une convention reflétant l'engagement commun *Consommateur de services / Fournisseur*.

RIO 0117	Il est RECOMMANDE de privilégier un accès aux ressources d'un *Fournisseur de services* se basant sur le rôle de l'usager *Professionnel* en lieu et place de son identifiant.

2.4.4 - Composants référencés

2.4.5 - Exemples d'initiatives sectorielles

2.5 - Service « Adhésion » (Particulier)

2.5.1 - Description

Ce service consiste à attribuer à un usager *Particulier* une collection de droit d'accès pour son propre compte.

2.5.2 - Normes et standards

2.5.3 - Principes de mise en œuvre

Seul les scenarii n°1 & A sont retenus.

RIO 0127	Il est RECOMMANDE de présenter un secret « métier » afin de prouver sa légitimité à utiliser une collection de télé-services.

RIO 0128	Il est OBLIGATOIRE que le secret « métier » soit une donnée reconnue par la sphère sectorielle.

RIO 0129	Il est OBLIGATOIRE d'attribuer le rôle "Administrateur AdEle" aux usagers *Particuliers* présentant un secret « métier » valide.

RIO 0130	Il est RECOMMANDE d'attribuer les droits d'accès à un nouveau télé-service aux usagers *Particuliers* possédant préalablement le rôle « Administrateur AdEle ».

La mise à disposition d'un nouveau télé-service enrichira la collection d'habilitations des usagers *Particulier* possédant le rôle « Administrateur Adèle »; on parlera d'adhésion « implicite » (par opposition à l'adhésion « explicite » nécessitant la présentation d'un secret « métier »).

RIO 0118	Il est RECOMMANDE d'archiver une trace des événements associés au processus d'adhésion attribuant des droits d'accès.

Cette trace sera générée, qu'il s'agisse d'une adhésion « implicite » (attribution de droits d'accès du à la possession d'une qualité, d'un rôle, ...) ou d'une adhésion « explicite » (attribution de droits d'accès suite à la présentation et validation d'un secret « métier » prouvant que l'usager est légitime).

2.5.4 - Composants référencés

2.5.5 - Exemples d'initiatives sectorielles

2.6 - Service « Délégation » (Agent)

2.6.1 - Description

Ce service consiste à attribuer tout ou partie de ses propres droits d'accès à des tiers.

2.6.2 - Normes et standards

2.6.3 - Principes de mise en œuvre

RIO 0131	Il est RECOMMANDE d'archiver une trace des événements associés au processus de délégation de droits d'accès.

RIO 0132	Il est OBLIGATOIRE que *l'Agent* délégataire de droits d'accès possède une identité numérique.

RIO 0134	Il est OBLIGATOIRE que *l'Agent* délégant possède le plein usage de son droit de délégation pour attribuer les droits d'accès aux délégataires.

- Cas du scénario C « séparation des pouvoirs (SOX) » :

RIO 0136	Il est INTERDIT qu'un *Agent* puisse cumuler l'aptitude à « faire » et « faire faire » ;

- Cas du scénario C « cumulation des pouvoirs » :

RIO 0138	Il est INTERDIT de déléguer des droits d'accès recouvrant un périmètre supérieur au sien.

2.6.4 - Composants référencés

2.6.5 - Exemples d'initiatives

2.7 - Service « Délégation » (Professionnel)

2.7.1 - Description

Ce service consiste à attribuer tout ou partie de ses propres droits d'accès à des tiers.

2.7.2 - Normes et standards

2.7.3 - Principes de mise en œuvre

RIO 0131	Il est RECOMMANDE d'archiver une trace des événements associés au processus de délégation de droits d'accès.

RIO 0133	Il est OBLIGATOIRE que l'usager *Professionnel* délégataire de droits d'accès possède une identité numérique.

RIO 0135	Il est OBLIGATOIRE que l'usager *Professionnel* délégant possède le plein usage de son droit de délégation pour attribuer les droits d'accès aux délégataires.

- Cas du scénario C « séparation des pouvoirs (SOX) » :

RIO 0137	Il est INTERDIT qu'un usager *Professionnel* puisse cumuler l'aptitude à « faire » & « faire faire » ;

- Cas du scénario C « cumulation des pouvoirs » :

RIO 0138	Il est INTERDIT de déléguer des droits d'accès recouvrant un périmètre supérieur au sien.

2.7.4 - Composants référencés

2.7.5 - Exemples d'initiatives

2.8 - Service « Propagation » (Agent)

2.8.1 - Description

2.8.2 - Normes et standards

2.8.3 - Principes de mise en œuvre

Seule l'association des scenarii n°3 & B est retenu e.

RIO 0139	Il est RECOMMANDE d'archiver une trace des événements associés au demandes d'accès des *Agents* aux ressources mises à disposition par le *Fournisseur de services*.

RIO 0142	Il est OBLIGATOIRE que les demandes d'accès des *Agents* aux ressources fassent référence à « l'Engagement commun » *Consommateur de services / Fournisseur*.

RIO 0144	Il est RECOMMANDE que les demandes d'accès des *Agents* aux ressources mises à disposition par le *Fournisseur de services* véhiculent une identification de l'utilisateur, du *Bénéficiaire*, de la ressource invoquée ainsi que des restrictions d'accès sur cette ressource.

2.8.4 - Composants référencés

2.8.5 - Exemples d'initiatives

2.9 - Service « Propagation » (Professionnel)

2.9.1 - Description

2.9.2 - Normes et standards

2.9.3 - Principes de mise en œuvre

RIO 0140	Il est RECOMMANDE d'archiver une trace des événements associés aux demandes d'accès des *Professionnels* aux ressources mises à disposition par le *Fournisseur de services*.

RIO 0145	Il est RECOMMANDE que les demandes d'accès des *Professionnels* aux ressources mises à disposition par le *Fournisseur de services* véhiculent une identification de l'utilisateur, du *Bénéficiaire*, de la ressource invoquée ainsi que des restrictions d'accès sur cette ressource.

- Cas du scénario n°3 associé au scénario B :

RIO 0143	Il est OBLIGATOIRE que les demandes d'accès des Professionnels aux ressources fassent référence à « l'Engagement commun » *Consommateur de services / Fournisseur*.

2.9.4 - Composants référencés

2.9.5 - Exemples d'initiatives

2.10 - Service « Propagation » (Particulier)

2.10.1 - Description

2.10.2 - Normes et standards

2.10.3 - Principes de mise en œuvre

Seule l'association des scenarii n°1 & A est retenu e.

RIO 0141	Il est RECOMMANDE d'archiver une trace des événements associés aux demandes d'accès des *Particuliers* aux ressources mises à disposition par le *Fournisseur de services*.

RIO 0146	Il est RECOMMANDE que les demandes d'accès des *Particuliers* aux ressources mises à disposition par le *Fournisseur de services* véhiculent une identification de l'utilisateur, du *Bénéficiaire*, de la ressource invoquée ainsi que des restrictions d'accès sur cette ressource.

2.10.4 - Composants référencés

2.10.5 - Exemples d'initiatives sectorielles

2.11 - Eléments documentaires

Les travaux engagés sur ce sujet par un groupe de projet interministériel vont se poursuivre en 2006 dans le cadre de l'Initiative Identité numérique du Schéma directeur.

Une première version d'un Référentiel de gestion des habilitations et des droits d'accès à fait l'objet d'un appel à commentaires

Ce référentiel regroupe un ensemble de règles, procédures, données et modèles d'architectures fonctionnelles et techniques associées à la problématique de gestion des habilitations et/ou des droits d'accès d'un usager.

Nom + Version	**Spécification**	**Etat**	**Date**
Référentiel de gestion des habilitations v0.92	http://vitamin2.adae.gouv.fr/ministeres/projets_adele/adele_121_gestion_de/public/	Appel à commentaires	Août 2005
«Standard d'interopérabilité inter-organismes » de la sphère sociale	Etude publiée par la Direction de la Sécurité sociale du ministère de la santé http://vitamin2.adae.gouv.fr/ministeres/projets_adele/adele_121_gestion_de/public/		Juillet 2005

3 - Archivage électronique

Objectif	Un système d'archivage électronique sécurisé a pour objectif de conserver aux Archives leur force juridique originelle tant en terme de preuve que de légalité. Cet objectif s'applique également aux Archives à valeur patrimoniale.
Domaine d'interopérabilité	• Archivage • Intégration des services de sécurité
Responsable	Gabriel Ramanantsoavina

3.1 - Finalités

L'archivage électronique est un moyen. Comme tout archivage, il doit répondre aux finalités suivantes :

- conserver des actes juridiques servant de titres et/ou pièces justificatives (pièces comptables, justificatifs fiscaux, par exemple) ;
- permettre la production d'actes pouvant valoir preuve pour la reconnaissance de droits en cas de litiges ;
- constituer une source d'informations pour l'organisme, correspondant à sa « *mémoire* » (la gestion de la production, la planification et la commercialisation des produits en seront directement dépendantes),
- préserver le patrimoine culturel et la mémoire collective

Les deux premières ont une dimension juridique, répondant à une contrainte légale (archivage obligatoire imposé par un texte) ou à une fonction juridique de confort (prouver ses droits), les deux dernières répondent à une finalité patrimoniale.

3.2 - Acteurs de l'archivage

Le décret n°79-1037 du 3 décembre 1979 relatif à l a compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques définit les règles de gestion des documents d'archives publiques au long de leur cycle de vie.

- *Le Service d'archives*

Le Service d'archives est l'entité destinataire du transfert et assurant la gestion des Archives transférées par les Services versants et destinées à être communiquées aux Producteurs, et, dans le respect des délais de communicabilité, aux demandeurs d'archives.

- *Le Service versant*

Le Service versant désigne l'entité qui transfère un ensemble de données à un service d'archives.

- *Le Service producteur*

Le Service producteur désigne l'entité qui a produit les archives, c'est-à-dire qui les a créées ou reçues dans le cadre de son activité.

- Le Service de contrôle

Certains messages ne sont émis qu'après validation par un service de contrôle.
Dans le secteur public en France, ce service de contrôle exerce le contrôle scientifique et technique sur les archives (Direction des Archives de France et notamment l'Inspection générale des Archives de France, directeurs des Archives départementales).

- Le Demandeur d'archives

Le terme Demandeur d'archives désigne toute personne physique ou morale qui souhaite consulter les Archives conservées par le service d'archives dans le respect de la législation applicable en matière de communication des Archives.

Cette typologie est valable pour l'archivage interne à une entité et pour l'archivage externe faisant intervenir des entités indépendantes.

- Le Tiers archiveur

Le tiers archiveur est une personne physique ou morale en charge, pour le compte de tiers, de la réception, de la conservation et de la restitution de documents électroniques dont il doit garantir l'intégrité.

Les services de l'Etat peuvent, dans des cas particuliers et sous certaines conditions, confier à des sociétés privées d'archivage la conservation d'archives intermédiaires qui seront détruites à terme. Cette faculté n'existe pas pour les collectivités territoriales (article L. 212-6 du code du patrimoine). Les établissements de santé peuvent faire héberger leurs dossiers médicaux électroniques dans des conditions prévues par décret.

RIO 0147	Il est RECOMMANDE que soient précisés par voie contractuelle, conventionnelle ou par note de service le rôle et responsabilités respectifs du Service versant et du Service d'archives, ainsi que les conditions techniques de mise en œuvre de l'archivage

3.3 - Définition et cycle de vie des archives

Le code du patrimoine définit les **archives** comme "*l'ensemble des documents, quels que soient leur date, leur forme et leur support matériel, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité*" (article L. 211-1) et les **archives publiques** comme "*les documents qui procèdent de l'activité de l'Etat, des collectivités territoriales, des établissements et entreprises publics ; les documents qui procèdent de l'activité des organismes de droit privé chargés de la gestion des services publics ou d'une mission de service public ; les minutes et répertoires des officiers publics ou ministériels*" (article L. 211-4).

Les documents sont d'abord conservés par les services qui les ont produits tant qu'ils leur servent régulièrement. Ils sont alors qualifiés d' "**archives courantes**".

Ensuite, lorsque leur utilisation devient exceptionnelle mais qu'ils gardent une utilité de preuve, ils restent conservés suivant des modalités diverses soit dans le service producteur, soit dans un dépôt dit de préarchivage, ou enfin dans un service public d'archives. Ils sont alors qualifiés d' "**archives intermédiaires**".

A l'issue de cette période, un tri est effectué entre les documents présentant un intérêt pour l'histoire ("**archives définitives**"), qui sont versés dans les services publics d'archives (Archives nationales, archives régionales, archives départementales, archives municipales), et les autres, qui sont détruits.

Durée : Pour chaque type de documents, la durée de ces périodes est définie par accord entre l'administration productrice et l'administration des archives (article 15 du décret n°79-1037)
Contrôle : A chaque étape de leur cycle de vie, la conservation des documents d'archives publiques est contrôlée par l'administration des archives (article 2 du décret n°79-1037).
Elimination : En particulier, l'élimination de documents par un service producteur ne peut se faire sans le visa de l'administration des archives (article 16 du décret n° 79-1037 et article R. 1421-3 du code général des collectivités territoriales). De même, l'élimination de documents par un service public d'archives ne peut se faire sans le visa de l'administration productrice (article 16 du décret n° 79-1037 et article L. 212-14 du code du patrimoine).
Bordereau descriptif : Lors du transfert des documents d'archives dans un dépôt de préarchivage ou dans un service public d'archives, il est établi un bordereau descriptif par les soins du service qui effectue le versement (article 18 du décret n°79-1037).
Accès : Par la suite, le service versant peut avoir à tout moment accès aux documents qu'il a versés, sauf s'il s'agit de bases de données nominatives. La consultation par le public est également possible, selon des délais définis notamment par la loi n°78-753 du 17 juillet 1978 sur l'accès aux documents administratifs et par le code du patrimoine (articles L. 213-1 à L. 213-4).

Les archives étant définies sans distinction de date, de forme et de support, l'ensemble des règles qui précèdent s'appliquent aussi bien aux documents "traditionnels" papier qu'aux données électroniques (bases de données, documents bureautiques, documents numérisés gérés dans des systèmes de GED, documents échangés dans le cadre de téléservices, messages électroniques, etc.). Leur mise en oeuvre peut cependant différer.

3.4 - Exigences juridiques et fonctionnelles

RIO 0148	Il est OBLIGATOIRE, pour que l'archivage électronique remplisse sa finalité juridique, que les modalités mises en place permettent de garantir que le document archivé peut être lu et intelligible, imputable à un auteur identifié et qu'il est fiable et intègre jusqu'au terme du délai durant lequel des droits y afférents peuvent exister.

Pour conférer et conserver la valeur probante, exigence *ad probationem* (ou validité, *ad validatem*) à un document, son archivage doit être ***fiable et sécurisé*.** Il doit répondre aux exigences suivantes d'identification, d'intégrité, de confidentialité, d'accès et pérennité de l'information

3.4.1 - Identification

Cela implique

- une identification des documents concernés :
  - Respect des opérations de sélection, de tri et d'élimination
  - Evolution du statut du document avec sa durée de conservation
  - Conditions de communication et d'accès au document
- une identification du domaine juridique dans lequel s'inscrit le document :
  - Durée et modalité de conservation
  - Finalité (légalité, preuve, …)
  - Formalisme connexe (LRAR, double exemplaire,…)

3.4.2 - Intégrité

Le document doit être établi et conservé dans des conditions de nature à en garantir l'intégrité, à défaut le juge pourra douter de la fiabilité de l'écrit électronique et donc de sa valeur juridique, que ce soit à titre de preuve ou de légalité.
Cette exigence fonctionnelle suppose :

- que toute altération ou modification dans le contenu d'un document soit immédiatement détectable
- la traçabilité des archives (tout événement affectant l'archive est conservé)
- une fiabilité du processus d'archivage

RIO 0149	Il est RECOMMANDE, pour que l'archivage électronique soit regardé comme fiable d'un point de vue juridique, que les procédures mises en place soient précisément décrites et mises en œuvre.

3.4.3 - Confidentialité

La confidentialité est nécessaire selon la nature des documents archivés :

- Identifier la nature de l'archive en amont
- Définir son caractère communicable ou non au public ou aux seules personnes intéressées
- Prévoir un archivage permettant de prendre en compte l'évolution du degré de confidentialité de l'archive

RIO 0150	Il est RECOMMANDE pour assurer la confidentialité que le service d'archivage mette en place un service sécurisé par un contrôle d'accès et, si nécessaire, un chiffrement des données.

- Contrôle d'accès (login/mot de passe)
  - seules les personnes autorisées doivent pouvoir accéder aux archives et au système

- les documents devront être classés, identifiés et indexés selon un processus permettant la recherche des documents

- Recours à la cryptologie/chiffrement des données

  la cryptologie permet une sécurité des échanges et des systèmes d'information (dans le cadre des flux et du stockage des données sur un disque)

3.4.4 - Accès et pérennité

L'accès et la pérennité de l'information doivent être assurés. Ils renvoient aux notions de :

- Durée de la conservation

  La distinction est à faire entre délais de conservation obligatoires des documents archivés et délais de prescription relatifs aux droits et obligations y afférents (qui peuvent être interrompus)

- Durabilité/ fiabilité

  Il s'agit de la conservation des informations qui pourront être aisément consultées pendant un laps de temps adapté et assurant la reproduction à l'identique des informations stockées

3.4.5 - Traçabilité

L'ensemble des opérations affectant l'archive doit être tracé.

RIO 0151	Il est OBLIGATOIRE d'enregistrer et d'archiver une trace des opérations et des événements concernant les archives et les documents archivés.

A cet effet des procédures devront être définies en tenant compte des prescriptions applicables à l'archivage en général (DUA, bordereau de versement, opération de tri, bordereau d'élimination, …) et des règles relatives à la consultation et à la communication des documents archivés (accès réservé, liberté de communication, …).

L'archivage électronique devra être auditable tout au long du cycle de vie du document électronique.

RIO 0152	Il est OBLIGATOIRE de créer des métadonnées associées à l'archive électronique, au plus tard lors du versement, afin de permettre son identification et sa traçabilité

3.4.5.1. Normes et standards sur les métadonnées

Nom + Version	Spécification	Etat	Date
« Preservation Metadata: Implementation Strategies (PREMIS) » *v1.0*	*Dictionnaire des données* http://www.loc.gov/standards/premis/	publié	Mai 2005
MOREQ – Commission européenne 2001	*Model Requirements for the management of electronic records* http://europa.eu.int/idabc/en/document/2631/5585	publié	2001

Le dictionnaire PREMIS vise à établir, à partir du modèle OAIS, une liste des métadonnées de préservation, c'est-à-dire « l'information qu'un dépôt utilise dans le processus de conservation numérique ».
L'objet principal en est la gestion de la conservation.

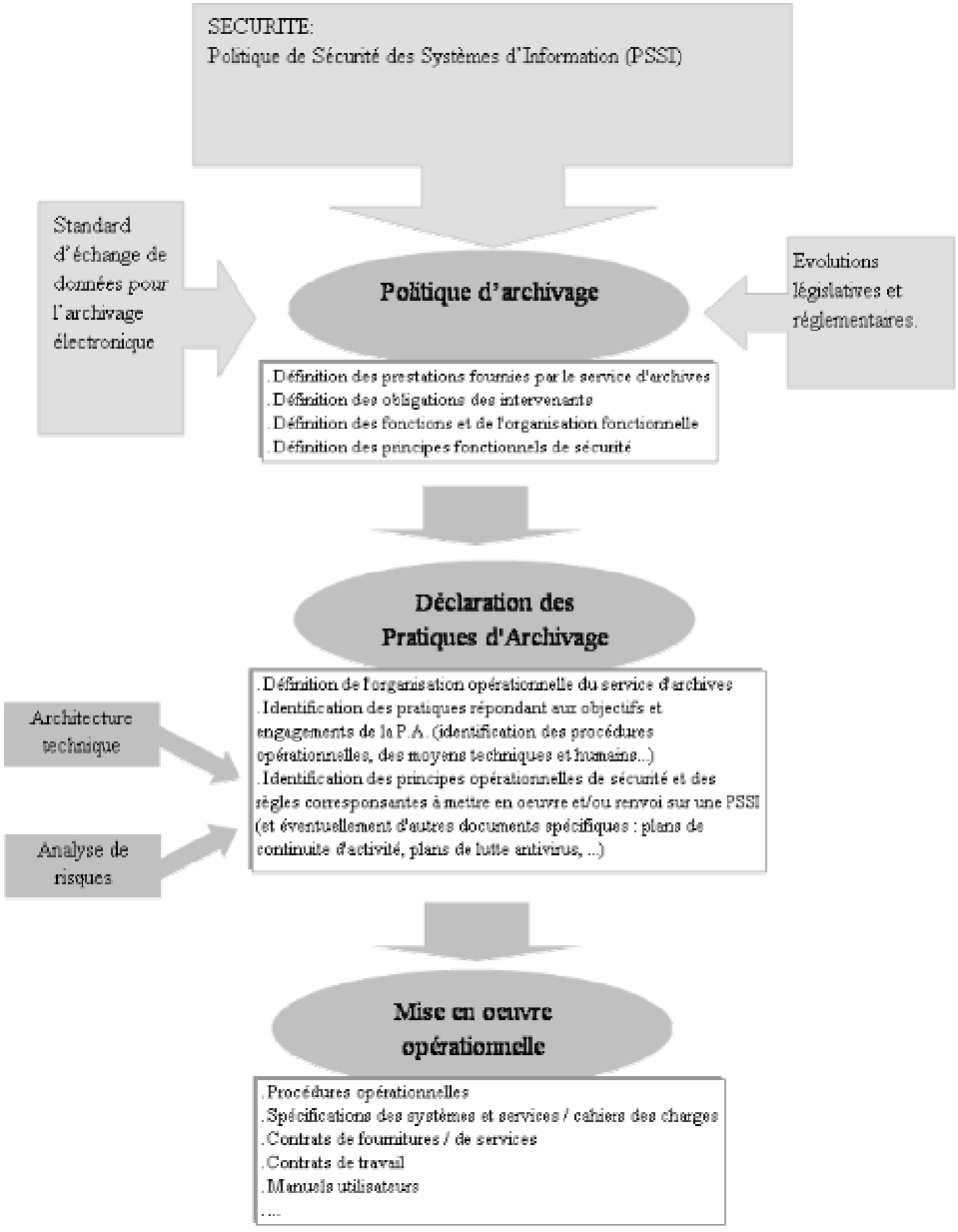
3.4.6 - Archivage sécurisé

RIO 0153	Il est RECOMMANDE d'établir une « politique d'archivage » avant toute mise en œuvre d'un système d'archivage électronique.

Il s'agit d'un document posant les règles de base en matière de sécurité pour un archivage électronique sécurisé. **Cette Politique d'archivage doit définir les contraintes juridiques, fonctionnelles, opérationnelles et techniques à respecter par les différents acteurs afin que l'archivage électronique mis en place puisse être regardé comme fiable**. Ce document, en l'absence de textes précisant les critères de fiabilité de l'archivage électronique, permettra, le cas échéant, de rapporter devant le juge la preuve de la fiabilité du procédé et des procédures mis en œuvre et par là-même de l'archivage électronique réalisé.

L'ensemble des messages échangés par réseau entre le service d'archives et ses partenaires extérieurs (service versant, service producteur, demandeur d'archives, service de contrôle) est sécurisé par l'utilisation de protocoles adéquats pour s'assurer que l'ensemble des données échangées parvient bien dans son intégralité à son destinataire.

Voir RGI Interopérabilité technique Protocoles



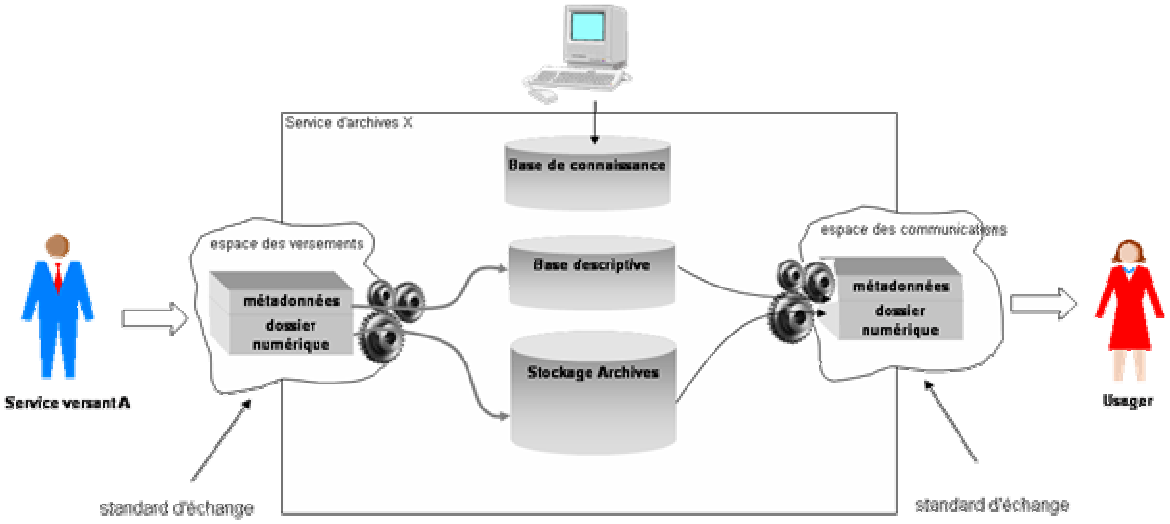
3.5 - Service d'archivage électronique SAE

Un service d'archivage électronique SAE est opératoire pour les archives intermédiaires et les archives définitives. Il a pour fonction de gérer la description des archives et la gestion de leur conservation, la gestion des informations et données échangées entre les différents acteurs.

La **base descriptive** contient des informations sur les archives et met à disposition des critères de recherche (exemples : description du contenu d'un dossier, nom du service producteur, délai de communicabilité d'un document, format du document, etc.).
Voir RGI Interopérabilité technique : les Formats de données et Formats de documents

La **base de connaissance** contient des données relatives au cadre d'exécution du processus d'archivage (exemple : informations sur les applications sources faisant l'objet de versements, contrats de service, plans d'assurance qualité, documentation technique, informations de représentation, etc.).

Le **système de stockage** gère les supports contenant les données.
Voir RGI Interopérabilité technique : les supports d'archivage.



Le **standard d'échange** s'intéresse aux formats des informations échangées, au format de l'enveloppe des objets et non au format de pérennisation des objets eux-mêmes.

Voir RGI Interopérabilité sémantique : Méthodologie d'élaboration :de données et documents RGI Interopérabilité technique.

3.6 - Loi et règlements

Loi n°78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public, articles 1er, 2 et 4.

Loi n°79-18 du 3 janvier 1979 sur les archives.

Ordonnance n°2004-178 du 20 février 2004 relative à la partie législative du code du patrimoine

Décret n°79-1037 du 3 décembre 1979 relatif à la compétence des services d'archives publics et à la coopération entre les administrations pour la collecte, la conservation et la communication des archives publiques

Décret n°79-1038 du 3 janvier 1979 relatif à la communicabilité des documents d'archives publiques

Décret n°79-1040 du 3 décembre 1979 relatif à la s auvegarde des archives privées présentant du point de vue de l'Histoire un intérêt public

4 - Standard d'échanges de données pour l'archivage

Objectif	Le standard d'échange de données pour l'archivage vise à faciliter l'interopérabilité entre le système d'information d'un service d'archives et les systèmes d'informations de ses partenaires (producteurs, utilisateurs...). Il fournit un modèle pour les différentes transactions qui peuvent intervenir : transfert, communication, destruction..
Domaine d'interopérabilité	• Archivage • Standard d'échanges entre partenaires
Responsable	Gabriel Ramanantsoavina

4.1 - Public visé

Le standard d'échange s'adresse plus particulièrement :

- aux producteurs d'archives publiques tels les ministères, les services déconcentrés de l'Etat, les collectivités territoriales, les établissements publics ;
- aux services publics d'archives, en vue de normaliser la réception et la communication d'archives numériques et de favoriser ainsi les portails de consultation multi-sites ;
- aux éditeurs de logiciels qui souhaiteraient se conformer à un cadre normatif pour le développement de leur module d'archivage ;
- aux éditeurs de logiciels de gestion et de description des archives papiers ;

Le standard peut également être utile aux entreprises, pour leurs besoins d'archivage, et aux sociétés prestataires de services d'archivage. Des éléments optionnels permettent de couvrir la diversité des besoins entre le secteur public et le secteur privé.

RIO 0158	Il est OBLIGATOIRE que les services publics d'archives et leurs partenaires qui veulent mettre en place des échanges informatisés se réfèrent au « standard d'échanges de données pour l'archivage » élaboré par la Direction des Archives de France du Ministère de la culture et de la communication et le SDAE de la DGME du Ministère des finances.

http://www.vitamin2.adae.gouv.fr/ministeres/projets_adele/a103_archivage_elect/public/standard_d_echange_d/folder_contents

4.2 - Description

La modélisation réalisée s'applique à la gestion et à la description des archives aussi bien papiers qu'électroniques. De même, il est opérant qu'il s'agisse de la gestion des archives intermédiaires ou des archives définitives.
Le standard se limite aux informations échangées entre les différents acteurs et ne concerne pas l'organisation interne de leurs systèmes d'information.

Ce travail de normalisation se traduit par des diagrammes d'activités et des modèles de données selon le formalisme UML, et par la définition de messages suivant des schémas XML. Les situations couvertes sont la demande de transfert et le transfert, la communication, l'élimination, l'avis de modification ou la restitution de documents ou données électroniques entre service versant, service d'archives et tierces entités. Sont définis le format, la structure et le contenu informationnel échangés.

Le standard défini est générique et adaptable à tous types de documents et de données, électroniques ou papier. Aussi, lors de la prise en compte d'un processus dans la chaîne de l'archivage, les éléments génériques devront être précisés par des règles de description spécifiques aux documents ou données versées

Le standard apporte des éléments utiles pour la construction des applications en amont et en aval des messages. Il indique en particulier les données nécessaires à prévoir dans ces systèmes. Ces données seront utilisées pour générer les messages, par mapping entre le modèle des bases applicatives et les schémas XML des transactions prévues dans le présent standard.

Voir aussi RGI Interopérabilité sémantique : Modélisation UML - Données communes des téléservices – Méthodologie d'élaboration de modèle d'échange

4.3 - Normalisation des métadonnées d'archivage

Comme les documents papier, les documents électroniques ne peuvent pas être conservés s'ils ne sont pas accompagnés, au moment de leur transfert aux archives, d'informations descriptives, autrement appelées métadonnées.

Ces métadonnées comprennent les mêmes informations que les bordereaux de versement de documents papier, et notamment : administration versante, date de versement, description du contenu des documents, dates des documents (métadonnées fonctionnelles), communicabilité, durée de conservation, traçabilité (métadonnées de suivi).

Mais il est capital de donner en outre des informations sur le format des documents versés et des indications sur l'environnement logiciel voire matériel nécessaire à la lecture et à la présentation des bits d'information (métadonnées techniques).

Par ailleurs, il est souhaitable que ce bordereau de versement sous forme électronique se présente de manière très normalisée. Il pourra ainsi accompagner les archives électroniques versées par réseau et pourra faire l'objet de traitements automatiques, notamment en vue d'être intégré dans le système d'information des archives.

4.4 - Normalisation des formats de documents

A la différence des documents papier, lisibles immédiatement, les documents électroniques se présentent sous la forme de fichiers composés de bits, selon des formats divers, dont la lecture requiert des logiciels particuliers, qui peuvent devenir obsolètes.
Il est donc indispensable de choisir dès l'origine des formats considérés comme pérennes et d'effectuer, en temps voulu, les conversions nécessaires pour maintenir la lisibilité des données.

Voir RGI Interopérabilité technique : Formats de données – Formats de documents

4.5 - Normes et standards

Le standard prend en compte ces deux normes liées :

Nom + Version	Spécification	Etat	Date
ISO 14721: 2003	Systèmes de transfert des informations et données spatiales -- Système ouvert d'archivage de l'information -- Modèle de référence, connue sous le nom de modèle OAIS (Open Archival Information System) http://ssdoo.gsfc.nasa.gov/nost/wwwclassic/documents/pdf/CCSDS-650.0-B-1.pdf. Traduction française, en cours de normalisation,: http://vds.cnes.fr/pin/documents/projet_norme_oais_version_francaise.pdf.	Norme publiée	2003

Norme ISAD(G)	General International Standard on Archival Description) du Conseil international des archives http://www.ica.org/ .		
MOREQ – Commission européenne 2001	Model Requirements for the management of electronic records http://europa.eu.int/idabc/en/document/2631/5585	publié	2001
« Preservation Metadata: Implementation Strategies (PREMIS) » *v1.0*	*Dictionnaire des données* http://www.loc.gov/standards/premis/	publié	Mai 2005

Norme ISO 14721:2003

Cette norme conceptuelle, mise au point par les principaux centres d'études spatiales du monde dont le CNES (Centre National d'Etudes Spatiales), définit les objets d'information, les métadonnées nécessaires à leur préservation et l'organisation à mettre en place pour leur archivage, leur conservation et leur communication.

Elle a été prise en compte pour définir les acteurs, les échanges et les objets d'informations échangés.

La Norme ISAD(G) définit les règles à suivre et les éléments nécessaires pour la description des documents archivés. En complément avec la DTD EAD (Encoded Archival Description), qui en est une implémentation, elle a été prise en compte dans le présent standard pour définir les éléments nécessaires à la description des données échangées.

Les métadonnées prévues par Moreq ont été prises en compte dans le standard d'échange.

Le dictionnaire PREMIS
L'objet principal en est la gestion de la conservation, non les échanges entre un service d'archives et ses partenaires. Il est donc assez différent de la perspective du standard d'échange de données pour l'archivage. PREMIS a été utilisé pour vérifier qu'aucune information de pérennisation importante à fournir par le service versant n'avait été oubliée.

4.6 - Synoptique des échanges

Cinq principaux cas d'utilisation interviennent entre le service d'archives et ses partenaires :
- le transfert
- la communication
- la modification d'archives
- l'élimination
- la restitution

Chaque échange a été modélisé, le diagramme des séquences établi : ils ont permis de définir un message à utiliser pour chaque séquence de communication.

Exemples :

Séquence	Message à utiliser
Demande de transfert d'archives	
Demande de transfert d'archives	ArchiveTransferRequest
Accusé de réception de demande de transfert	ArchiveTransferRequestReply
Acceptation de transfert d'archives	ArchiveTransferRequestReply
Refus de transfert d'archives	ArchiveTransferRequestReply
Accusé de réception de refus de transfert	ArchiveTransferRequestReplyAcknowledgement
Transfert d'archives	
Transfert d'archives	ArchiveTransfer
Accusé de réception de transfert d'archives	ArchiveTransferReply
Notification d'acceptation d'archives	ArchiveTransferAcceptance

Avis d'anomalie de transfert d'archives	ArchiveTransferReply
Accusé de réception d'avis d'anomalie	ArchiveTransferReplyAcknowledgement
Etc.	

4.7 - Modèle de données des messages et des objets échangés

La conception des messages s'est appuyée sur des composants de données créés en s'appuyant sur les types de composants communs normalisés.

Chaque message est un assemblage de composants spécifiques au message, dont son en-tête, et de composants réutilisables qui sont identiques dans de nombreux messages. Ces composants réutilisables, souvent des entités métier, sont regroupés en « packages » manipulables modélisés avec tous leurs attributs sous forme de diagramme de classes: une archive avec sa description de contenu, le document qui est inclus, une signature, une empreinte …..

Chaque message précédemment identifié au niveau des séquences d'échange est structuré et représenté par un **diagramme de classes**.
Ce diagramme de classe permet d'élaborer ensuite le **schéma XML**

L'ensemble des composants et leurs attributs peuvent également être présentés sous forme de dictionnaires ou tableau de données ou se retrouvent les entités métiers et métadonnées normalisées.

Ces définitions correspondent à celles de la norme ISO 14721 (modèle OAIS).

L'Archive comporte obligatoirement une description du contenu, constituée du contenu de données et des informations de représentation et peut comporter des documents joints. Elle peut être subdivisée en Objets d'archives, dotés de propriétés similaires.

L'Archive possède un identifiant, un intitulé (obligatoire), une indication du niveau de description (obligatoire), ainsi que les attributs suivants :
- accord d'archivage (Archival Agreement) : accord (convention, contrat) ou texte réglementaire servant de cadre aux relations entre le service versant et le service d'archives ;
- type d'archive (Archival Profile) : règles de constitution de l'archive en fonction du type de documents ou d'application concernée ;
- langue de la description (Description Language) - obligatoire ;
- niveau de service (Service Level) : niveau de service demandé (disponibilité, sécurité...), en référence aux différents niveaux prévus par le contrat ou la convention passée entre le service versant et le service d'archives.

4.8 - Composants du standard d'échanges

Il comprend

Une description très détaillée notamment sur les données et objets échangés : Archives, objets d'archive et documents.

L'étude des échanges à partir des cas d'utilisation précités.

Les diagrammes de classes des composants communs : entités métiers réutilisables

Les diagrammes de classes des composants communs : entités métiers réutilisables

Description de chaque message sous forme de modèle / diagramme de classe.

Le tableau des données, attributs, cardinalités, définitions et commentaires sur les ressources référentielles

Les schémas XML des messages

Les tables de codification (nomenclatures) à utiliser pour certaines des métadonnées

- Liste des schémas fournis avec le standard d'échange de données pour l'archivage :

Fichier	**Description**
CoreComponentTypesSchemaModule_0.3.4.xsd	CoreComponentType UN/Cefact
xades.xsd	schéma des attributs Xades
xmldsig-core-schema.xsd	schéma de la signature XMLDsig

archives_echanges_v0-1_archive.xsd	Description du contenu des archives
archives_echanges_v0-1_signature.xsd	Description de la Signature
archives_echanges_v0-1_organization.xsd	Description d'une organisation (contact, adresse)
archives_echanges_v0-1_hashcode.xsd	Description des Condensats (HashCode)
archives_echanges_v0-1_archivemodification.xsd	Messages liés a la modificationd'archives
archives_echanges_v0-1_archivetransfer.xsd	Messages liés au transfert d'archive
archives_echanges_v0-1_archivedestruction.xsd	Messages liés à la destruction d'archive
archives_echanges_v0-1_archiverestitution.xsd	Messages liés à la restitution d'archive
archives_echanges_v0-1_archivetransferrequest.xsd	Messages liés à la demande de transfert
archives_echanges_v0-1_archivedelivery.xsd	Messages liés à la communicationd'archive
MessagesIdentifiants. PD	Description des schémas et des messages associés

4.9 - Exemples sectoriels

- Schéma XML du transfert d'un dossier de marché public transfert d'un dossier de marché public au service d'archivage.

Il présente la structure générale des messages et les entités manipulées : Archive, Organization, Signature, HashCode. Il illustre également l'utilisation des tables de codes génériques et spécifiques à une application. Il montre enfin l'utilisation des condensats (HashCode) pour garantir l'intégrité des documents transférés et de la signature PKCS7.

- .Schéma XML de la communication d'une délibération d'un conseil municipal (Acte).

Il montre l'usage d'une signature Xades et l'encapsulation du document transmis encodé en Base 64.

- Schéma XML demande de transfert préalable au versement d'une base de données issue de la Nouvelle Chaîne Pénale et réponse.

5 - Conservation des données et documents numériques

Objectif	La conservation des données courantes telles que les documents bureautiques, courriers électroniques … Sont l'une des préoccupations prioritaires des chantiers de l'administration électronique. La prise en compte de cette problématique quelle que soit l'étape dans le cycle de vie du document est à l'origine de nombreuses questions. La perte d'informations peut si l'on y prend garde se transformer en une perte de mémoire pour l'administration avec toutes les conséquences que cela induit. Les règles relatives à ce domaine portent notamment sur les formats des documents mais il sera également nécessaire de définir des règles la traçabilité et sur la mise en œuvre des système de gestion des droits (notamment DRM : digital right managment)
Domaine d'interopérabilité	• Démarches administratives dématérialisées • Echanges inter administrations
Responsable	Pascal Souhard

5.1 - Formats des documents

Voir RGI Interopérabilité Technique

En cours de rédaction

6 - Protection des données personnelles

Objectif	Sensibiliser au respect des obligations légales concernant la protection des données à caractère personnel, indispensables dans les échanges des usagers avec les administrations et inter-administrations avec la progression de l'interopérabilité des systèmes d'informations. Ces données ont vocation à être enregistrées dans l'espace de stockage individuel autorisé par l'ordonnance du 8 décembre 2005, devant faciliter les démarches administratives dématérialisées
Domaine d'interopérabilité	• Accès aux services en ligne • Conservation et archivage • Intégration entre portails et services administratifs • Echanges inter administrations
Responsable	Pascal Souhard

6.1 - Données à caractère personnel

Les données collectées auprès des usagers et transmises aux autorités administratives dans le cadre de l'administration en ligne sont pour une grande part des données personnelles. Toutes ne sont pas confidentielles, mais sont généralement des informations nominatives ce qui les rend sensibles. La protection de ces données à caractère personnel ainsi que la protection des individus concernés par les transferts et traitements sur ces données est encadrée par la loi "Informatique et Libertés" du 6 janvier 1978 modifiée par la loi du 6 août 2004.

Il appartient à tout individu et aux autorités administratives de participer à la protection de la vie privée et des libertés individuelles (déontologie administrative). La CNIL quant à elle a pour mission d'informer et de répondre aux demandes d'avis et conseil, de garantir aux individus l'exercice de leur droits, de recenser les fichiers, de contrôler le respect des obligations et sanctionner si nécessaire, de réglementer afin de faciliter la mise en œuvre des règles et formalités.

Nombre de procédures administratives, d'enquêtes et traitements statistiques sont concernés.

6.1.1 - Rappel de l'article 2 de la loi :

Constitue **une donnée à caractère personnel** toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.
Constitue **un traitement de données à caractère personnel** toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.
Constitue un **fichier de données à caractère personnel** tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

6.2 - Obligation de déclaration

Les responsables de sites Web, de téléprocédures, de fichiers et traitements de données à caractère personnel sont tenus de les déclarer auprès de la CNIL sauf en cas d'exonération.
Tous les éléments sur les différents régimes de déclaration – déclaration de site Web, déclaration de conformité, déclaration normale – sont en ligne sur le site de la CNIL.
http://www.cnil.fr/

RIO 0159	IL EST OBLIGATOIRE de ne collecter et enregistrer que les informations adéquates, pertinentes et non excessives au regard de la finalité du fichier. Les informations doivent être déterminées, légitimes et correspondre aux missions de l'autorité administrative.

RIO 0160	IL EST OBLIGATOIRE que les agents des autorités administratives amenés à créer de leur propre initiative des fichiers en informer leur hiérarchie et que cette obligation faite aux agents leur soit rappelée à intervalles réguliers.

La liste de données autorisées est strictement définie. La CNIL est particulièrement attentive aux questions d'interconnexion et d'identifiants, et limite l'usage du numéro NIR d'immatriculation au Répertoire national d'identification des personnes physiques (RNIPP).

RIO 0161	IL EST OBLIGATOIRE que les logiciels proposés aux autorités administratives soient adaptés à leurs besoins réels et paramétrables simplement afin de permettre l'enregistrement des seules données réellement nécessaires.

6.3 - Obligation d'information

Lorsque ces traitements sont en exploitation et ouverts aux usagers,

RIO 0162	IL EST OBLIGATOIRE d'afficher une information claire et précise (obligation légale d'information) visant à instaurer un climat de transparence et de confiance entre les usagers et les services mis en œuvre par les autorités administratives.

RIO 0163	IL EST OBLIGATOIRE de s'assurer que la finalité des fichiers et les éventuelles transmissions d'informations sont clairement définies, les dispositifs de sécurité précisément déterminés et l'information des usagers correctement diffusée.

Les pages « d'Informations légales » des procédures de type « traitement de données personnelles » doivent fournir ces indications et l'accès aux déclarations qu'il s'agisse

- d'un Engagement de conformité à une norme simplifiée, d'une Déclaration de conformité à une autorisation unique de la CNIL, d'un Engagement de conformité à un acte réglementaire unique
- ou même d'un Engagement de conformité à Engagement de conformité à une Méthodologie de référence

Les durées de conservation des données doivent également être explicitées.

6.4 - Exercice des droits des usagers

Droit d'opposition

RIO 0164	IL EST OBLIGATOIRE de permettre à l'usager le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel le concernant soient enregistrées dans un fichier informatique sauf si celui-ci présente un caractère obligatoire.

L'usager doit pouvoir exercer ce droit avant la procédure, mais aussi après en s'adressant au responsable du fichier.

Limite : Le droit d'opposition n'existe pas pour de nombreux fichiers du secteur public : ceux des services fiscaux, de la justice, de la sécurité sociale ….

Droit d'accès à ses données personnelles

Droit de modification ou de rectification

Droit de suppression

RIO 0165	IL EST OBLIGATOIRE de permettre à tout usager de demander à l'autorité administrative détenant un fichier de lui communiquer toutes les informations le concernant contenues dans ce fichier, il a également le droit de faire rectifier ou supprimer les informations erronées.

Les Contacts et modalités à suivre sont à indiquer dans les « Informations légales ». La CNIL veille à ce que les modalités n'entravent pas l'exercice de ce droit et peut, pour les fichiers touchant à la sûreté de l'Etat, à la défense et la sécurité publique, demander accès pour le compte de l'usager.

Le maintien d'erreurs, inexactitudes, ou données interdites dans les fichiers du secteur public ou privé peut porter préjudice et l'usager a la possibilité de porter plainte auprès de la CNIL.

De façon complémentaire, un Engagement explicite peut être demandé à l'usager concernant la prise de connaissance des informations, la véracité des ses réponses, la confidentialité de son mot de passe.

6.5 - Confidentialité et sécurité

RIO 0166	IL EST OBLIGATOIRE que les responsables des autorités administratives veillent à ce que leurs personnels mettent en oeuvre et appliquent, de manière effective, les mesures de confidentialité et sécurité concernant les données personnelles.

- article 34 de la loi 78-17 du 6 janvier 1978 : *Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.*
- article 226-17 du code pénal : *Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesure prescrites à l'article 34 de la loi 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.*

RIO 0167	IL est RECOMMANDE que les mots de passe permettant aux usagers et aux agents d'accéder aux informations comportent au moins 8 caractères, dont au moins une lettre minuscule, une lettre majuscule, un chiffre, un caractère non-alphanumérique. Ils doivent être changés au moins tous les deux mois.

RIO 168	IL est INTERDIT que plusieurs personnes au sein d'un même service partagent même mot de passe.

6.6 - Correspondant Informatique et Libertés CIL

Le correspondant informatique et libertés a été introduit, dans les secteurs public et privé, avec la réforme de la loi de 1978. Il a vocation à être un interlocuteur spécialisé dans la protection des données à caractère personnel auprès du responsable des traitements concernés, et dans les rapports de celui-ci avec la CNIL (décret du 20 octobre 2005).

Allégement des formalités :

La désignation d'un correspondant CIL, interne ou externe, est facultative et se fait sans agrément de la CNIL. Elle permet l'exonération de déclaration préalable pour les traitements ordinaires et courants. Seuls les traitements identifiés comme sensibles, demeureront soumis à formalités et autorisations.

Aide et conseil au responsable du traitement

Il est chargé de suivre la légalité de déploiement des projets informatiques, la gestion des données personnelles, la prise en compte de la protection des libertés dans le contexte du développement des nouvelles technologies de l'information et de la communication. Il aura à rechercher des solutions concrètes conciliant l'intérêt des professionnels et la protection des libertés individuelles.

6.6.1 - Normes et standards

.

Nom + Version	**Spécification**	**Etat**	**Date**
CNIL	Loi 78-17 relative à l'informatique, aux fichiers et aux libertés. http://www.cnil.fr/	Publiée et amandée	6 jan 1978
Conseil de l'Europe	Traité STCE no. : 108 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. http://conventions.coe.int/treaty/Commun/QueVoulezVous.asp?NT=108&CM=8&CL=FRE	Ratifié	01 oct 1985
ONU Haut Commissariat aux droits de l'homme Résolution 45/95	Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel. http://www.unhchr.ch/french/html/menu3/b/71_fr.htm	Adoptée	14 déc 1990
Commission européenne	Directive relative à la protection des données 95/46/CE http://europa.eu.int/comm/justice_home/fsj/privacy/index_fr.htm		24 oct 1995
CEPD	Contrôleur européen de la protection des données http://www.edps.eu.int/01_fr_presentation.htm		2002

7 - Les aspects Sécurité

7.1 - Services de gestion d'infrastructure à clés publiques

7.1.1 - Description

Objectif	
Domaine d'interopérabilité	Intégration entre services techniques
Responsable	

7.1.2 - Normes et standards

Avec l'accroissement du nombre d'applications, de solutions techniques et d'utilisateurs faisant appel à des certificats numériques, il peut devenir nécessaire de mettre en place des outils techniques et des procédures organisationnelles afin de gérer le cycle de vie des certificats numériques à grande échelle et d'instaurer véritablement la confiance inhérente à leur utilisation. C'est précisément le rôle d'une ICP (Infrastructure à Clefs Publiques) appelée en Anglais (*Public Key Infrastructure : PKI*). On entend parler aussi de IGC (Infrastructure de Gestion de Clés).

Les fonctionnalités offertes par une ICP via ses différentes composantes permettent d'assurer la gestion du cycle de vie d'un certificat. Une ICP s'articule généralement au minimum autour des trois composants de base suivants :

- L'Autorité de Certification (AC) qui génère et signe les certificats. L'AC est le tiers de confiance dont la signature apparaît sur le certificat. Elle est responsable du processus de certification dans sa globalité.
- Une ou plusieurs Autorités d'Enregistrement (AE) qui enregistrent et valident les demandes de certificats.
- Un dépôt qui stocke les certificats et les listes de certificats révoqués (CRL : Certificate Revocation List).

Le sujet de l'ICP étant largement par ailleurs, nous nous contenterons ici d'évoquer les quelques évolutions des standards sur lesquels elle s'appuie.

Nom + Version	RFC	Spécification	Etat	Date
PKI	2510 2511	Protocole et format de message pour une demande de création de certificat à une AC	Proposé standard	Mars 1999
	2559	Utilisation de LDAPv2 dans une PKI	Proposé standard	Avr 1999
	2560	OCSP	Proposé standard	Juin 1999
	2585	Utilisation de FTP et HTTP afin de récupérer un certificat ou une CRL	Proposé standard	Mai 1999
	2587	Schéma LDAPv2 pour une PKI	Proposé standard	Juin 1999
	2985	PKCS #9 v2.0 (RSA)	Information	Nov 2000
	3279	Algorithmes et identifiants pour le profil des certificats et des CRL	Proposé standard	Avr 2002
	3280	Profil des certificats et des CRL	Proposé standard	Avr 2002
	3281	Profil de certificat d'attribut pour l'autorisation	Proposé standard	Avr 2002

7.1.3 - Principes de mise en œuvre

Il n'existe pas encore d'élément référencé.

7.1.4 - Composants référencés

Il n'existe pas encore d'élément référencé.

7.1.5 - Exemples d'initiatives sectorielles

Il n'existe pas encore d'élément référencé.