MODE OPERATOIRE JURIDIQUE
INTEROPS

	Nom	Organisme	Date
Rédaction			
Validation			
Approbation			

Document applicable à compter du

Identification du document			
Direction			
Objet			
Domaine			
Nature			
N° d'ordre		Version	**1.0**
Nbre pages	**18**		
Référence			
Logiciel			

Participants au Groupe de Travail Juridique INTEROPS

Claire ALBOUY-COSSARD	CNAMTS
Laëtitia APARICI	ACOSS
Monique BEUREY-LECONTE	GIP Info Retraite
Patricia BLOCH-MANIKOW	GIP-MDS
Virginie BOUTTEMY	CNAV
Florence CIROT	CDC
Isabelle DOMENECH	DSS
Christel HAGNERE	CNAMTS
Laure LE BRUN	CCMSA
Stéphanie LECOMTE	RSI
Sophie LHERAULT	CCMSA
Sophie MICHAS	AGIRC-ARRCO
William MORRICHON	AGIRC-ARRCO
Sébastien ROBELIN	GIP-MDS

SOMMAIRE

1. CONTEXTE

En 2004, le Ministère des Affaires Sociales a constaté un besoin croissant d'échanges entre les organismes de la sphère sociale dans de nombreux domaines. La direction de la sécurité sociale a lancé un projet d'étude inter organismes pour définir les règles communes d'interopérabilité des systèmes d'information, dirigé par un comité de pilotage et décliné au travers d'un groupe technique et d'un groupe juridique inter-organismes.

Les organismes de la sphère sociale ont besoin de partager des informations, d'accéder à leurs systèmes d'informations respectifs et de coproduire des démarches administratives avec les usagers. Ils le font dans le respect des dispositions de l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives[1] et de ses textes d'application.

Afin de répondre de façon pérenne à ces préoccupations, un standard d'interopérabilité entre les organismes de protection sociale, appelé INTEROPS, a été défini. Ce standard a vocation à être utilisé par tous les acteurs de la sphère sociale pour échanger des informations. Il ne peut évoluer qu'après validation du comité de pilotage INTEROPS.

La Circulaire Ministérielle n°DSS/4C/2011/273 du 7/7/2011[2] , publiée le 5 septembre 2011 sur le site « circulaires.gouv.fr » et relative aux règles communes d'organisation des échanges électroniques dans le cadre de l'activité des organismes de protection sociale, est venue préciser les règles d'organisation en matière d'échanges électroniques entre les organismes de protection sociale (OPS) d'une part et entre les OPS et leurs assurés d'autre part, et présenter les procédures de contrôle mises en œuvre pour garantir la qualité de ces échanges.

Cette circulaire précise que tout échange de données dématérialisées entre OPS, réalisé via un web service utilisant un standard d'interopérabilité, donne lieu à une procédure de contractualisation entre les OPS, sous la forme d'une convention interops.

Elle définit le web service comme une technologie permettant à des applications de dialoguer/ communiquer à distance de manière sécurisée, en s'appuyant sur un ensemble de protocoles d'échanges standards (notamment XML,http).

[1] Lien hypertexte de l'ordonnance : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000636232

[2] Lien hypertexte de la circulaire : http://www.sante.gouv.fr/fichiers/bo/2011/11-08/ste_20110008_0100_0148.pdf

Elle rappelle que le standard repose sur la confiance entre les organismes (notion de sphère de confiance), qu'il propose un système sécurisé de propagation des droits d'accès et des habilitations et qu'il garantit la traçabilité des actions ainsi que les principes retenus pour la mise en place du standard :

- la création d'un cercle de confiance entre les organismes ;
- l'authentification de l'utilisateur réalisée par l'organisme client ;
- l'attribution de l'habilitation par l'organisme client à ses utilisateurs selon les règles établies avec l'organisme fournisseur au moyen d'une convention propre à chaque échange ;
- la transmission de l'habilitation, de manière sécurisée, à l'organisme fournisseur par un vecteur d'identification ;
- la trace de toute création d'un vecteur d'identification afin d'en permettre le contrôle « a posteriori ».

Enfin, la circulaire définit le socle minimum de sécurité (physique et logique) et de traçabilité des échanges qui doivent être mises en place entre les OPS en conformité avec le Référentiel Général de Sécurité (RGS, approuvé par arrêté du 6 mai 2010[3])

[3] Lien hypertexte de l'arrêté du 6 mai 2010 relatif au RGS :
http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000022220429&dateTexte=vig

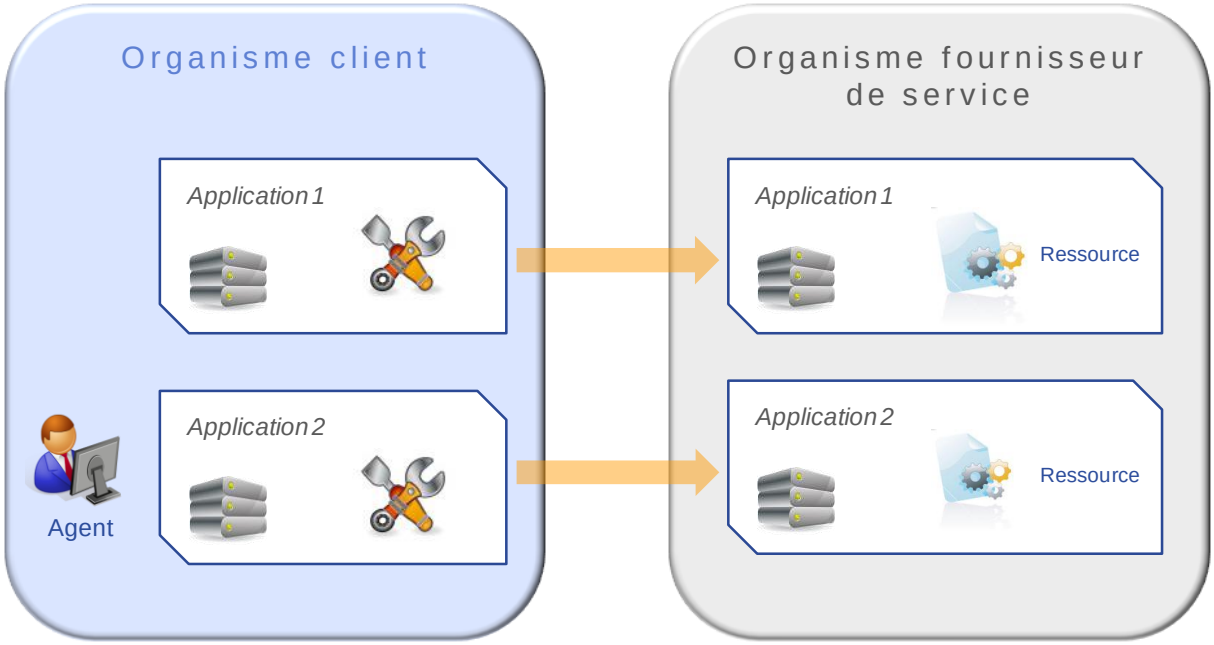
2. GENERALITES SUR LE STANDARD INTEROPS

Le standard INTEROPS se décline selon plusieurs modes de communication :

2.1 – INTEROPS-A : Mode « Application à Application »

Le mode « *application à application* » permet à une application d'un organisme client de communiquer avec des applications (ou services) d'un organisme fournisseur au travers de la mise à disposition par le fournisseur d'un web service au client.

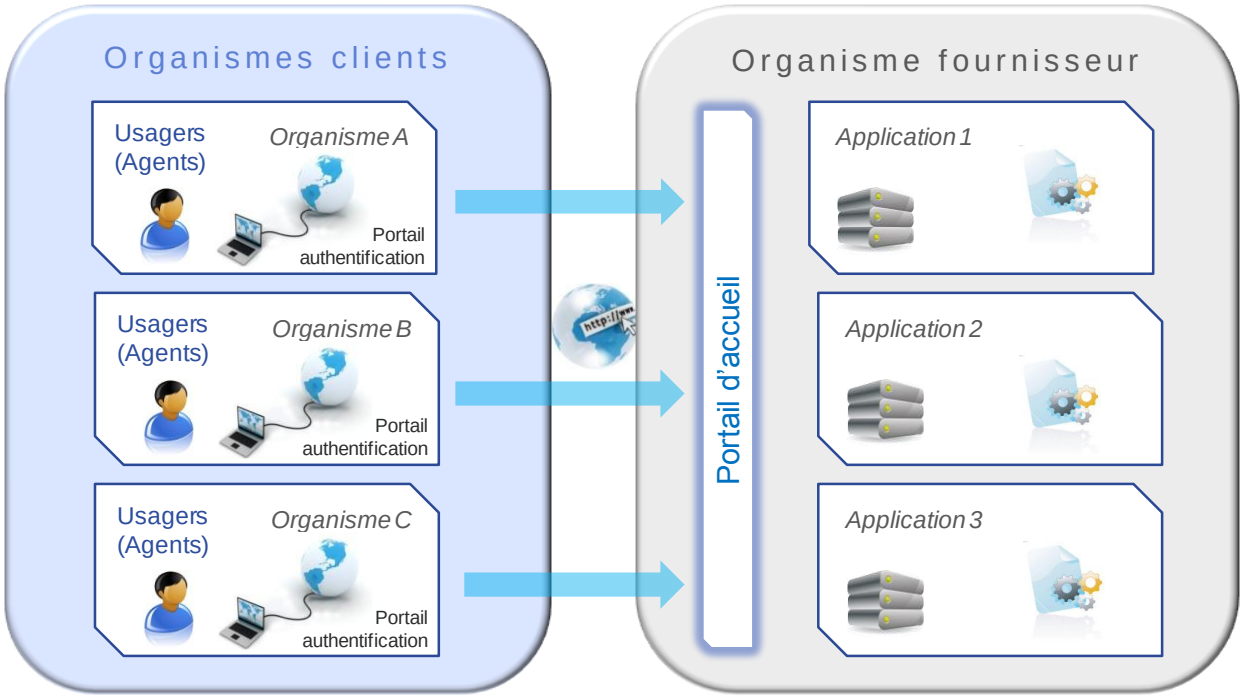
Dans le mode INTEROPS-A, chacun des organismes partie à la convention, a un rôle soit de client, soit de fournisseur. Le « client » est l'organisme accédant à des services offerts par un « fournisseur ».



2.2 – INTEROPS-P: Mode « Portail à Portail »

Le mode « *portail à portail* » permet aux utilisateurs de l'organisme client, après s'être identifiés, authentifiés et avoir été habilités dans leur infrastructure locale, de venir consulter des applications web d'un organisme fournisseur par accès direct de l'organisme client au service de l'organisme fournisseur.

Dans le mode INTEROPS-P, chacun des organismes partie à la convention, a un rôle soit de client, soit de fournisseur. Le « client » est l'organisme accédant à des services offerts par un « fournisseur »,



2.3 – INTEROPS-S: Mode « Sphère de Confiance »

Le mode « *sphère de confiance* », permet à tout utilisateur préalablement identifié et authentifié par un organisme d'accéder directement, aux portails de plusieurs autres organismes de la même sphère de confiance, sans avoir besoin de se ré-identifier ni ré-authentifier[4].

Une sphère de confiance correspond à une relation entre n organismes dans laquelle les notions d'organisme client et d'organisme fournisseur n'existent plus.
Interops-S permet de mettre en relation n organismes au sein d'une sphère de confiance. L'objectif est de pouvoir assurer une navigation à un utilisateur sans réidentification ni réauthentification au travers de son navigateur entre les différents opérateurs de service dès lors qu'il s'est authentifié auprès d'un opérateur d'authentification.

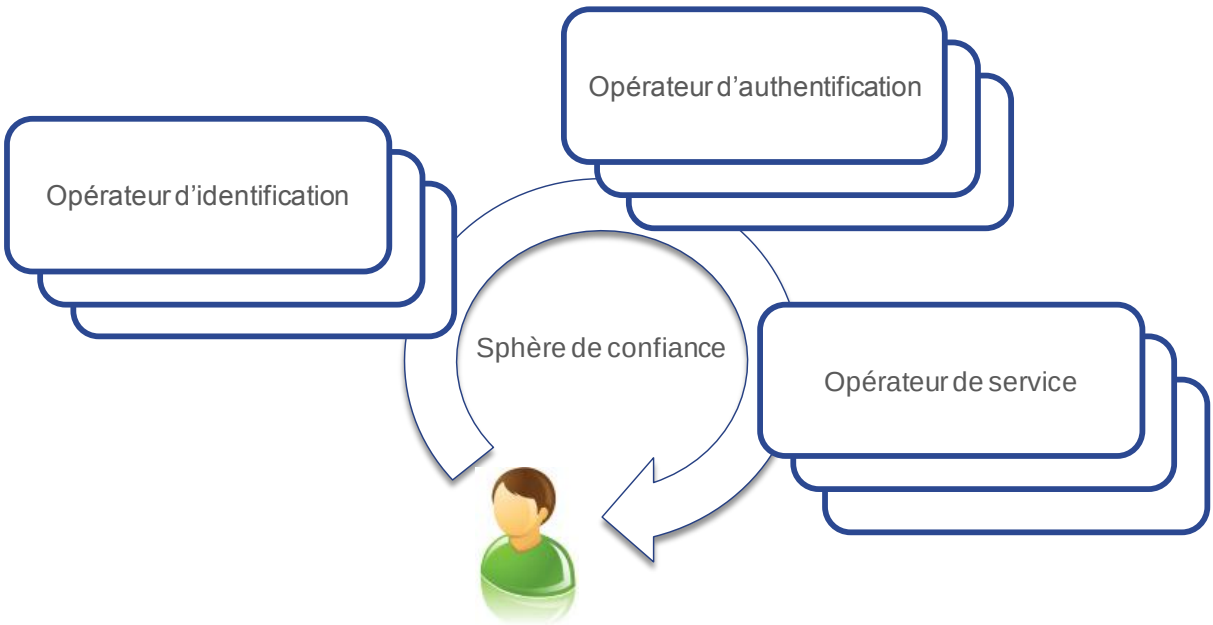
Interops-S définit les rôles d'organismes suivants, qui peuvent être cumulés :

- **Opérateur d'identification** : organisme chargé de réaliser l'identification de l'utilisateur (sur la base d'une carte SESAM-Vitale, etc.)
- **Opérateur d'authentification** : organisme authentifiant l'utilisateur final. L'identifiant de l'utilisateur peut avoir été récupéré grâce à l'opérateur d'identification. Il est chargé de produire un vecteur d'identification.

[4] cf. annexe 1 : description d'INTEROPS-S

- **Opérateur de service** : organisme hébergeant un service offert aux utilisateurs. Il vérifie et consomme le vecteur d'identification pour contrôler l'accès au service.

Chaque organisme peut jouer plusieurs rôles en même temps vis-à-vis des autres organismes. Ainsi, dans le cas le plus ordinaire, les opérateurs d'identification et d'authentification sont confondus. De même un opérateur de service peut être opérateur d'authentification.



2.4 – Caractéristiques techniques communes aux trois modes du standard INTEROPS.

Le standard Interops se base sur plusieurs standards reconnus : SOAP, WS-Security, SAML, XML Signature

Il intègre plusieurs fonctions de sécurité : authentification mutuelle des partenaires, authentification et transmission des habilitations du demandeur via un vecteur d'identification, sécurisation de l'échange au niveau transport et signature des jetons, génération des traces via :

- une interconnexion sécurisée (par SSL) avec le partenaire
- la génération ou vérification des jetons (vecteur d'identification et assertions signées)
- la gestion du cycle de vie des jetons (respectivement côté client et côté fournisseur)
- l'intégration des jetons aux requêtes métiers
- la gestion des traces de sécurité Interops

3. DISPOSITIF CONVENTIONNEL INTEROPS

3.1 – Principes généraux

Tout projet INTEROPS doit impérativement être fondé sur une convention juridique et ne peut démarrer qu'une fois cette convention signée.[5]

Une convention juridique s'appuie sur la dernière version du standard publiée sur le site interops.fr au moment de sa signature.

Toutes les versions successives du standard INTEROPS, ainsi que les documents complémentaires aidant à la mise en œuvre et les documents juridiques, sont disponibles sur le site interops.fr

Il existe des modèles de conventions juridiques et d'annexes types, élaborés par l'ensemble des OPS, au travers de Groupes de Travail dédiés. Ces modèles ont été présentés à la CNIL en même temps que le standard INTEROPS. Il est donc très vivement conseillé de se baser sur ces modèles pour établir ses conventions juridiques INTEROPS.

3.2 – Historique du processus de conventionnement

- A l'origine, le GT juridique a élaboré un modèle type de convention juridique entre OPS (convention + annexes), reprenant les principes généraux énumérés ci-dessus pour le respect du standard INTEROPS. Cette convention unitaire, contenant des clauses contractuelles minimales, applicables à tous les échanges, devait être adaptée à chaque type de projet. Elle concernait les modes d'échange INTEROPS-A et INTEROPS-P.

- Or, les projets entre les différents partenaires de la sphère sociale utilisant INTEROPS ont été amenés à se multiplier et dans ce contexte, il a été constaté que l'ensemble des informations techniques (convention technique, convention réseau, engagement de service, gestion des traces, etc.) étaient identiques, ce qui a amené le groupe à réfléchir à une possibilité de simplification des échanges contractuels entre les partenaires.

  Il est ressorti des réflexions qu'une convention générique INTEROPS avec chaque partenaire concerné permettrait de mettre en œuvre tous les nouveaux projets INTEROPS en ne signant qu'un avenant spécifiant le contexte applicatif du projet avec ledit partenaire.

[5] Cf. Annexe 2 : Lettre de la CNIL du 19 août 2008.

Cette convention générique, concernant les modes d'échanges INTEROPS-A et INTEROPS-P, est le modèle à privilégier à ce jour.

- En parallèle, un nouveau mode d'échange, basé sur INTEROPS-S, est apparu. Un modèle de convention juridique spécifique à INTEROPS-S a donc été rédigé.

3.3 – Architecture de la convention juridique générale pour INTEROPS-A ou INTEROPS-P.

L'architecture juridique en vigueur entre deux partenaires pour les projets basés sur INTEROPS-A ou INTEROPS-P est la suivante :

- Une convention générale
- L'annexe 1, « Conditions de fonctionnement et d'utilisation du service », est commune à tous les projets entre deux partenaires.
- L'annexe 2, « Spécifications d'une interconnexion réseau pour INTEROPS », est commune à tous les projets entre deux partenaires.
- L'annexe 3, « Liste des projets utilisant le standard INTEROPS et fiches projets déclinées par projet », regroupe l'ensemble des projets entre deux mêmes partenaires. Elle comprend les annexes 3.1 (« fiche projet n°1 »), 3.2 (« fiche projet n°2 »), etc. qui précisent les spécificités de chaque projet, le contexte, la qualité de fournisseur ou de client des partenaires.

En outre, l'article 3 de la convention (« Documents conventionnels ») dispose que la signature de celle-ci « *vaut adhésion aux spécifications définies dans les documents de référence du standard INTEROPS (publiés sur le site http://interops.fr)* » qui incluent les spécifications fonctionnelles, les spécifications détaillées portail à portail **et** application à application (en fonction du mode utilisé par les services), les spécifications du Vecteur d'Identification, les spécifications du jeton de contexte et les spécifications du format d'échange des traces.

Le standard INTEROPS est un support d'échange ; chaque type d'échange de données est à considérer comme un projet, selon le mode d'interopérabilité (A/P) et le rôle des organismes (client / fournisseur).
Exemple : Un projet met en œuvre les trois types d'échanges suivants :

1. INTEROPS-A : Organisme 1 Client et Organisme 2 Fournisseur
2. INTEROPS-A : Organisme 2 Client et Organisme 1 Fournisseur
3. INTEROPS-P: Organisme 1 Client et Organisme 2 Fournisseur.

Chacun des trois types d'échanges est considéré comme un projet distinct, et fait donc l'objet d'annexes 3.x spécifiques.

Une fois la convention générique signée pour un premier projet entre deux partenaires, tout nouveau projet entre ces deux mêmes partenaires fera l'objet de la signature d'un avenant, modifiant la convention par ajout de nouvelles fiches dans l'annexe 3 de la convention (dénommées « annexe 3.1, 3.2…»).

De même, il peut être mis fin à tout projet par un avenant, sans remettre en cause la convention générique. Cet avenant devra modifier les fiches de l'annexe 3 relatives au projet venu ainsi à terme.

3.4 –Architecture de la convention juridique INTEROPS-S.

L'architecture juridique en vigueur entre plusieurs partenaires pour les projets basés sur INTEROPS-S est la suivante :

- Une convention INTEROPS-S
- L'annexe 1, « Organisation de la sphère de confiance », qui mentionne les qualités des parties, les opérateurs d'identification, les opérateurs d'authentification, les opérateurs de services et les interlocuteurs désignés par les parties.
- L'annexe 2, « Spécifications d'une interconnexion réseau pour INTEROPS ».

En outre, l'article 4 de la convention (« Documents conventionnels ») dispose que la signature de celle-ci « *vaut adhésion aux spécifications définies dans les documents de référence du standard INTEROPS (publiés sur le site http://interops.fr)* » qui incluent les spécifications fonctionnelles, les spécifications détaillées « sphère de confiance », les spécifications du Vecteur d'Identification, les spécifications du jeton de contexte et les spécifications du format d'échange des traces.

Les particularités d'une convention juridique INTEROPS-S sont les suivantes :

- La convention peut être multipartite.
- Une fois la convention signée, toute nouvelle entité souhaitant devenir partie à la convention devra être acceptée par l'ensemble des parties et se conformer à la convention sans pouvoir en modifier les termes. Dans ce cas, un avenant sera signé, dont un modèle est disponible sur le site http://interops.fr.
- La convention s'appuie sur un Comité de Pilotage.
- Il peut être mis fin à la convention par avenant portant dénonciation de la convention signé par l'ensemble des parties et dont un modèle est disponible sur le site http://interops.fr.

3.5 –Mise en œuvre d'une convention juridique INTEROPS.

- Pour tout projet de type INTEROPS-S, une convention basée sur la convention type INTEROPS-S doit être signée.

- Pour tout nouveau projet de type INTEROPS-P ou INTEROPS-A, une convention générique doit désormais être signée, y compris si des conventions unitaires préexistent entre les deux partenaires. Tous les projets INTEROPS suivants feront l'objet d'un avenant à cette convention générique, comme précisé dans le paragraphe 3.3.

- La convention générique ne vient pas en remplacement de conventions existantes. Ainsi, si une ou plusieurs conventions unitaires INTEROPS avaient d'ores et déjà été signées entre les deux partenaires, ces dernières demeurent valables en l'état, jusqu'à leur terme ou leur résiliation. En cas de modification de cette convention unitaire (corps et/ou annexes), un avenant à cette convention doit être signé par les parties.

3.6 – Recommandations de mise en œuvre d'une convention juridique INTEROPS issues du retour d'expérience des OPS.

Dans le cas de projets utilisant INTEROPS-P ou INTEROPS-A, il est préférable que l'organisme fournisseur soit à l'initiative de la convention juridique.

- Il convient d'identifier le responsable du projet.
- Les aspects juridiques relatifs aux projets INTEROPS doivent être étudiés par des juristes.
- Les annexes doivent être rédigées par des services techniques, sous la coordination du responsable du projet.
- Il appartient à chacun des organismes de gérer la vie et le suivi de ses conventions juridiques.
- L'ensemble des conventions et des avenants doit être archivé par chaque organisme dans des conditions permettant leur conservation.

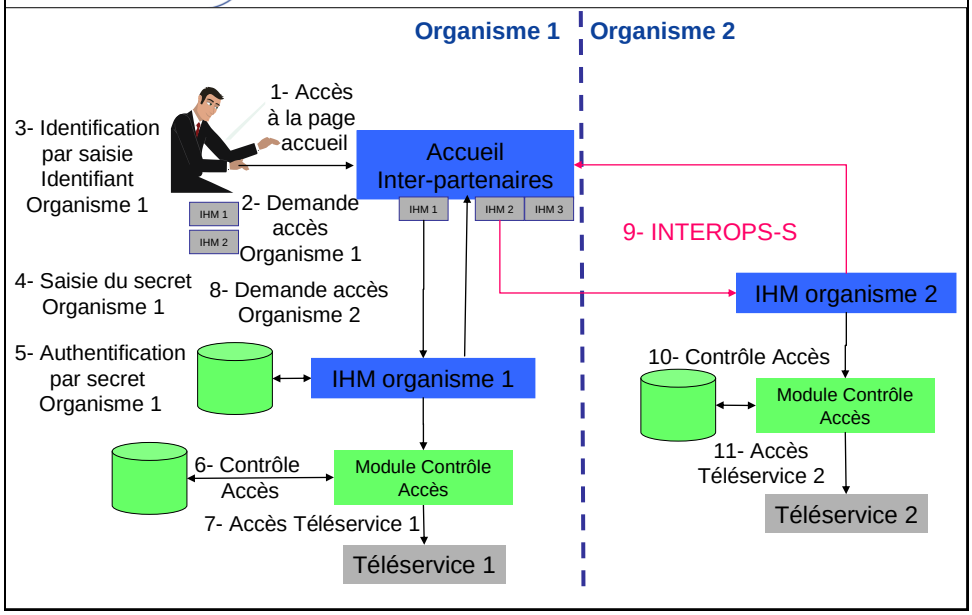
4. ANNEXE 1 : DESCRIPTION D'INTEROPS-S

Principes généraux

- Un individu (utilisateur agent ou non agent) doit pouvoir disposer de services individuels proposés par plusieurs OPS, sans se ré-identifier ni ré-authentifier auprès de chaque OPS.
- Le premier OPS consulté identifie et authentifie l'individu et transmet de manière sécurisée l'identification de l'individu et le fait qu'il l'a authentifié aux OPS consultés par la suite (jeton INTEROPS-S).
- Les OPS suivants font confiance au premier OPS qui a réalisé l'identification et l'authentification.
- Appelons « rebond » le passage d'utilisateur d'un site OPS à un autre

9 septembre 2010 1

Principes généraux



IHM : Interface Homme / Machine

Principes généraux

- INTEROPS-S est dérivé d'INTEROPS-P.
- Le nombre de partenaires peut être supérieur à deux (« rebond »).
- Le nombre de partenaires et les services disponibles peuvent changer en cours de vie du projet
  - intégration à la sphère de nouveaux partenaires et/ou de nouveaux services en cours de projet
- Chaque partenaire peut être tour à tour client et fournisseur de services identiques ou différents.

9 septembre 2010 4

Principes : identification et authentification

- Interops distingue trois types d'opérateurs qui peuvent ou non être les mêmes.
  - Opérateur d'identification : établit l'identité de l'utilisateur
  - Opérateur d'authentification : vérifie que l'utilisateur est bien le bon
  - Opérateur de service : fournit le service applicatif
- L'affectation de ces opérateurs est :
  - Soit statique (défini initialement)
  - Soit dynamique (défini au moment de l'accès au service)

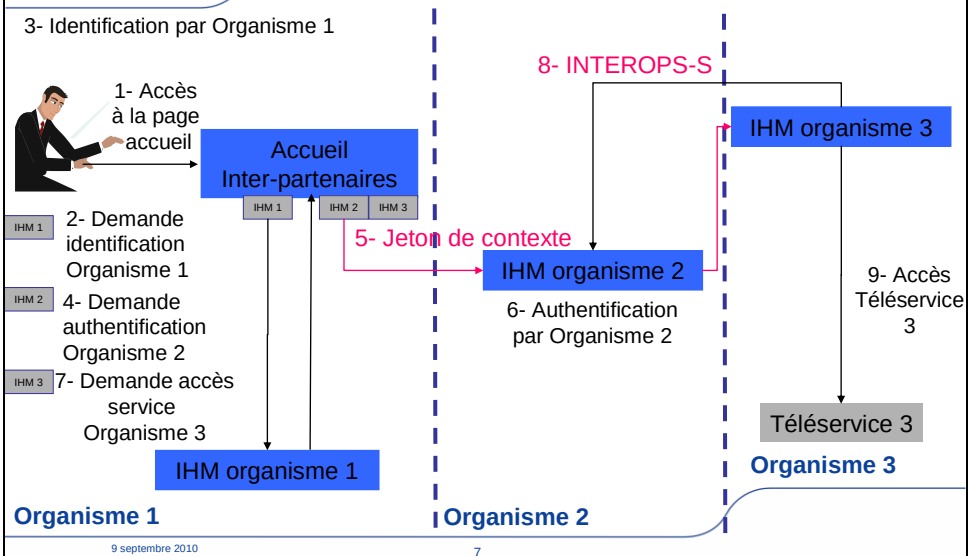
9 septembre 2010 5

Principes : identification et authentification

- L'OPS qui identifie un individu n'est pas forcément le même que celui qui l'authentifie (mais peut l'être).
- Lorsque ces OPS ne sont pas les mêmes, l'OPS qui a identifié un individu s'engage sur cette identité en produisant un jeton de contexte signé.
- Les OPS qui identifient et/ ou authentifient un individu ne sont pas forcément les mêmes que celui qui propose le service (fournisseur de service) (mais peuvent l'être).

9 septembre 2010 6

Principes : identification et authentification



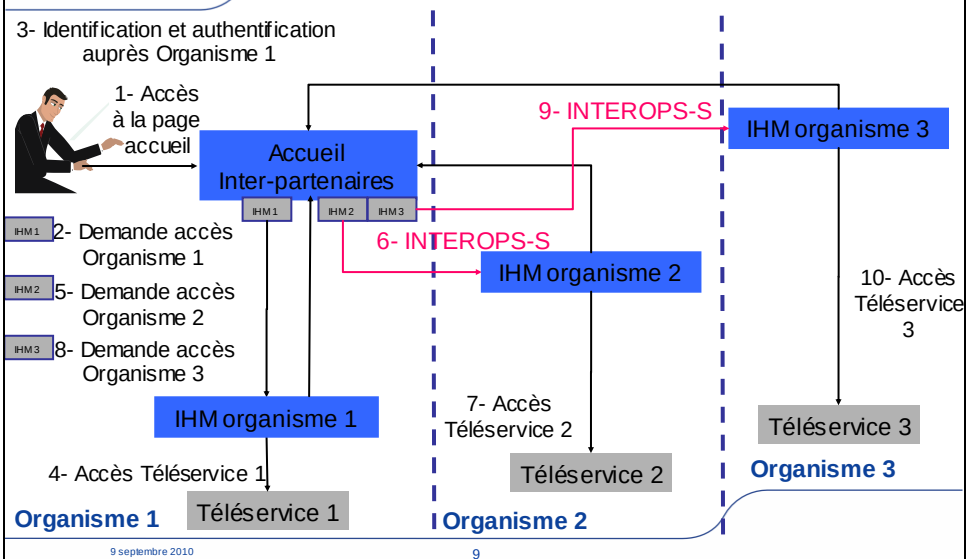
9 septembre 2010 7

Principes : rebond

- A chaque service présenté par un nouvel OPS, l'OPS ayant authentifié l'individu initialement génère un jeton INTEROPS-S s'engageant sur l'identification et l'authentification de cet individu (et ce même si c'est un autre OPS qui l'a identifié).
- Pour pouvoir produire ce jeton, un OPS doit donc avoir authentifié l'individu (après l'avoir identifié ou avoir reçu l'assurance de son identification par un autre OPS : jeton de contexte).
- A chaque "rebond", un nouveau jeton INTEROPS-S est généré.
- Chaque entité doit garder les traces qui permettront de suivre tout le parcours d'un individu.

9 septembre 2010 8

Principes : rebond



9 septembre 2010 9

5. ANNEXE 2 : LETTRE DE LA CNIL DU 19 AOUT 2008

CNIL.

Le Président,

Direction de la Sécurité Sociale
- 1 SEP. 2008
S/D.GSI / DSI
n°

Monsieur le Directeur de la sécurité sociale
~~MINISTERE~~ DU TRAVAIL DES RELATIONS SOCIALES ET DE LA SOLIDARITE
~~39/43 QUAI ANDRE CITROEN~~
~~75902 PARIS CEDEX 15~~

Instruction du dossier :
Paul HEBERT
Daniela PARROT
Alain PANNETRAT

Paris, le 19 AOUT 2008

N/Réf : AT/YPA/SVT/SN/GDP/DP/PHT/SA081402
Saisine n° 08016911
(à rappeler dans toute correspondance)

Monsieur le Directeur,

Vous avez souhaité prendre conseil auprès de la Commission nationale de l'informatique et des libertés, tant sur les spécifications techniques du standard « Interops » que sur le montage juridique envisageable pour simplifier l'instruction des dossiers.

Ce standard doit permettre de garantir l'intégrité et la sécurité des échanges d'informations entre organismes de protection sociale et a vocation à être utilisé par l'ensemble des partenaires de la « sphère sociale[1] ». Il définit les règles techniques et fonctionnelles d'interopérabilité que chaque organisme s'engage à respecter dans le cadre d'échanges d'informations. A titre d'information, une liste des organismes qui envisagent d'utiliser ce standard sera adressé à la CNIL.

Je note que l'établissement d'une convention entre l'organisme « client » (utilisateur des données ou de l'application) et l'organisme « fournisseur » (fournisseur de données ou de services) est un préalable indispensable à l'ouverture d'échanges en mode Interops comme indiqué lors de la réunion avec mes services en date du 1er juillet 2008.

L'analyse du référentiel technique Interops n'appelle pas d'observations particulières de la part de la Commission hormis le fait que le mode d'authentification des utilisateurs repose sur une confiance mutuelle entre les organismes échangeant des données. Ainsi, la gestion des habilitations est déléguée à l'organisme client dans le respect de la convention signée avec le fournisseur. Les opérations de gestion des habilitations doivent être tracées selon une méthode normalisée et auditable. La convention apparaît donc comme un outil majeur de sécurité.

[1] GIP Info retraite, CNAMTS : déclaration d'accidents du travail, RNCPS (lutte contre la fraude)....

Cette convention sera adaptée pour chaque traitement de données à caractère personnel. Elle comporte en annexe les documents techniques relatifs au standard Interops qui constituent un référentiel invariable que chaque organisme s'engage à respecter.

S'agissant de la procédure à suivre en cas d'utilisation du standard Interops, je prends acte du fait que la Commission sera systématiquement destinataire de la convention spécifique à chaque traitement signée entre les organismes concernés.

Ainsi, pour les nouveaux traitements, le dossier de formalité préalable devra être accompagné de la convention Interops signée et la mention de la version de chaque document du référentiel utilisée.

Pour les traitements déjà existants, la Commission devra être informée de l'utilisation du standard Interops et une copie de la convention lui sera transmise. L'utilisation du standard Interops n'entraînera pas de modification de l'acte réglementaire si aucune autre modification n'est apportée au traitement initial.

Toute évolution du référentiel utilisé devra être présentée à la CNIL préalablement.

Je vous prie, Monsieur le Directeur, d'agréer l'expression de mes salutations distinguées.

Alex TÜRK