PRESENTATION D'INTEROPS

	Nom	Organisme	Date
Rédaction	**GT Technique Interops**		
Validation			
Approbation			

Document applicable à compter du

Identification du document			
Direction			
Objet			
Domaine			
Nature			
N° d'ordre		Version	**3.0**
Nbre pages	**13**		
Référence			
Logiciel			

SOMMAIRE

Contexte et objet

Les organismes de la sphère sociale ont besoin de partager des informations, d'accéder aux systèmes d'informations de leurs partenaires et de coproduire des démarches administratives avec les usagers. Le standard Interops, initié par la DSS, publié dans sa première version en 2006, est aujourd'hui reconnu par la sphère sociale comme le standard de référence en matière d'interopérabilité. Il a pour objectif de spécifier les modalités d'interopérabilité des identités et des habilitations entre les systèmes d'information des OPS, dans une perspective de sécurisation des échanges.

La version 1 du standard INTEROPS a fait l'objet d'une demande de conseil à la CNIL et d'une réponse par courrier le 19 Août 2008 (Saisine n° 08016911). En avril 2012, le standard a évolué en version 2.

L'utilisation du standard INTEROPS par les organismes de protection sociale pour sécuriser leurs échanges est entérinée par la circulaire du directeur de la sécurité sociale du 7 juillet 2011 relative aux règles communes d'organisation des échanges dans le cadre des activités de protection sociale.

L'objet de cette note est de présenter à la CNIL les évolutions techniques de la version 2 du standard avant implémentation par les organismes. La présentation des conventions ne fait pas partie de cette note.

Documentation

Le standard est constitué d'un ensemble de documents fonctionnels, techniques et juridiques disponible à l'adresse http://www. interops.fr/.

Les principaux sont ceux listés dans le tableau ci-dessous :

	Référence	Titre	Auteur	Ver.	Date
[R1]	Standard Interops2.0_SpecificationsFonctionnelles	Spécifications fonctionnelles	Groupe de travail Interops	2.0	05/04/2012
[R2]	Standard Interops2.0_SpecificationsVI	Spécifications du Vecteur d'Identification	Groupe de travail Interops	2.0	05/04/2012
[R3]	Standard Interops-P2.0_SpécificationsDétaillées	Spécifications détaillées du mode « portail à portail »	Groupe de travail Interops	2.0	05/04/2012
[R4]	Standard Interops2.0_FormatEchangeTraces	Format d'échange des traces	Groupe de travail Interops	2.0	05/04/2012
[R5]	Standard Interops2.0_ConventionTechnique	Convention technique	Groupe de travail Interops	2.0	05/04/2012
[R6]	Standard Interops2.0_GuideMiseEnOeuvre-TransfertDeContexteApplicatif	Guide de mise en œuvre pour le transfert de contexte applicatif	Groupe de travail Interops	1.0	05/04/2012
[R7]	Standard Interops2.0_Glossaire	Glossaire du standard Interops	Groupe de travail Interops	2.0	05/04/2012

La liste des projets mis en œuvre en production et en qualification est disponible dans un espace protégé, à l'adresse suivante : https://espace-partenaires.interops.fr.

Cet accès est soumis à présentation d'un mot de passe, qui peut être obtenu sur demande au numéro suivant : 01-58-10-47-10.

Evolution du standard Interops

Les principaux points d'évolution sont les suivants:

- Les modes Interops-A et Interops-P ont évolué pour pouvoir être utilisés dans le cadre du Référentiel Général de Sécurité version 1.
- Des guides de mise en œuvre ont été rédigés, pour encadrer la mise en œuvre du transfert de contexte applicatif de l'échange et celle du transfert de pièces jointes.
- Un nouveau mode d'échange a été créé : le mode Interops-S « Sphère de confiance ». Celui-ci permet à tout utilisateur préalablement identifié et authentifié par un organisme appartenant à une sphère de confiance d'accéder directement, aux portails de plusieurs autres organismes appartenant à cette même sphère de confiance, sans avoir besoin de s'identifier ni de s'authentifier une nouvelle fois. Interops-S permet de mettre en relation n organismes au sein d'une sphère de confiance.
- Dans un souci de simplification de gestion, les modèles de conventions juridiques pour les modes Interops-A et Interops-P ont été fusionnés en une convention unique entre deux partenaires. La mise en œuvre de tous les nouveaux projets utilisant Interops est réalisée par la signature d'un avenant spécifiant le contexte applicatif et le mode d'échange Interops utilisé.
- Un modèle de convention juridique spécifique au mode Interops-S a été rédigé.

Présentation Interops

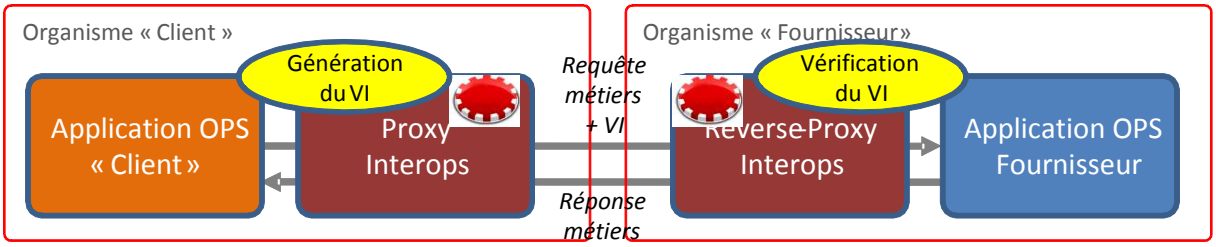
Principes

- Le modèle repose sur la confiance entre les organismes
- L'authentification de l'utilisateur n'est pas effectuée de bout en bout mais est réalisée par l'opérateur d'authentification
- Les habilitations sont attribuées par l'opérateur d'authentification en respectant les règles établies avec l'opérateur de service (Convention)
- L'habilitation est transmise à l'opérateur de service de manière sécurisée (par un Vecteur d'identification)
- Toute création et vérification de vecteur d'identification est auditable afin d'en permettre le contrôle « a posteriori »

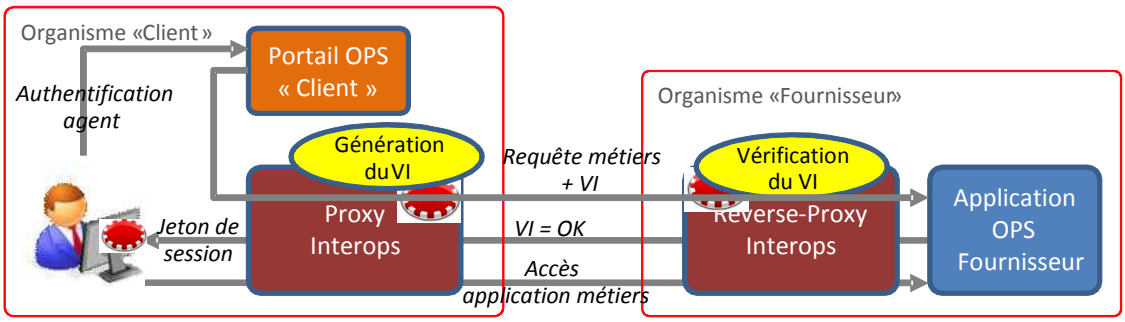
Interops A et P

Pour couvrir les différents cas d'usages, la version 1 du standard a spécifié deux modes d'échanges entre un organisme Client et un organisme Fournisseur (voir schéma ci-dessus) :

- Un mode « Application à Application » ou Interops-A qui permet à une application d'un organisme Client de communiquer avec une application située chez un organisme Fournisseur en utilisant les technologies Web Services. Pour chaque requête, un vecteur d'identification doit être transmis à l'application du fournisseur.



- Un mode « Portail à Portail » ou Interops-P qui concerne l'accès par un agent à une application web ou un portail situés dans un organisme distant (Fournisseur) avec un simple navigateur. Ce modèle est utilisé dans le cas de l'intégration d'applications d'un organisme fournisseur de services (applications distantes appartenant à un organisme fournisseur) à un portail d'accès d'un organisme client.



Interops-S

La version 2 du standard, a ajouté un mode « Sphère de confiance » ou Interops-S qui 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 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 (mécanismes de Web SSO entre un opérateur d'authentification et des opérateurs de service).

Interops-S définit les rôles suivants :

Opérateur d'identification : organisme chargé de réaliser l'identification de l'utilisateur.

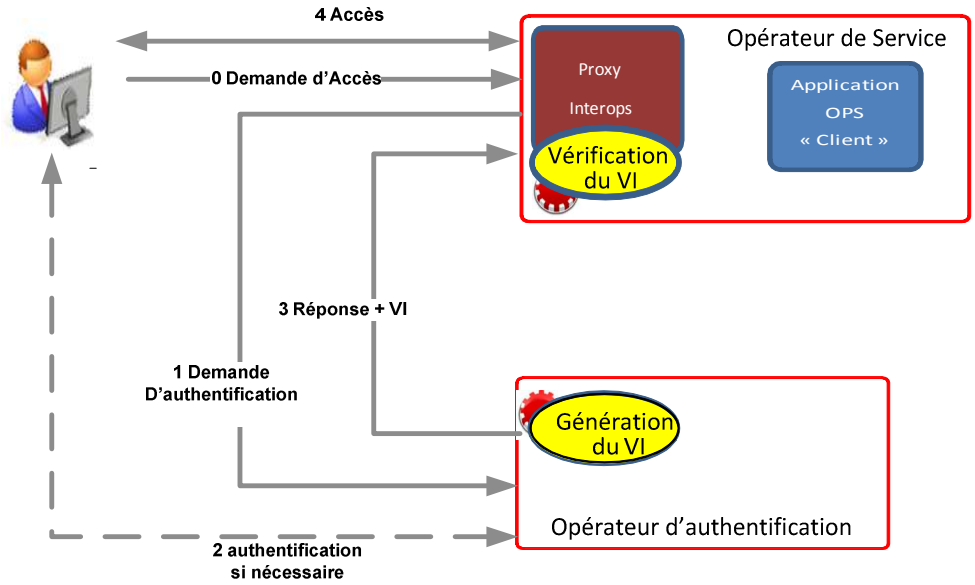
Opérateur d'authentification : organisme authentifiant l'utilisateur final. L'identifiant de l'utilisateur peut avoir été récupéré grâce à l'opérateur d'identification. Il est chargé de produire un VI. C'est l'équivalent de l'organisme client dans Interops-P ou du fournisseur d'identité dans SAML 2.0.

Opérateur de service : organisme hébergeant un service offert aux utilisateurs. Il vérifie et consomme le VI pour contrôler l'accès au service. C'est l'équivalent de l'organisme fournisseur dans Interops-P ou du fournisseur de service dans SAML 2.0.
Chaque organisme peut jouer plusieurs rôles en même temps vis-à-vis des autres organismes. Ainsi, dans le cas le plus ordinaire, le couple opérateur d'identification et d'authentification sont confondus

Connexion

Interops-S offre la possibilité de rediriger l'utilisateur vers son opérateur d'authentification à partir d'un opérateur de service. Interops-S permet de déterminer quel est l'opérateur d'authentification utilisé par un utilisateur à partir d'un opérateur de service de façon à initier une cinématique d'authentification.

Cinématique d'authentification :



0. L'utilisateur se connecte à l'opérateur de service et accède à une zone sécurisée nécessitant d'être authentifié. Si l'opérateur d'authentification est inconnu, alors il est possible de le déterminer grâce à la cinématique de récupération de l'opérateur d'authentification Si l'opérateur d'authentification reste indéterminé, alors l'opérateur de service peut remonter une erreur à l'utilisateur ou authentifier localement l'utilisateur.

1. L'opérateur de service émet une demande d'authentification signée à destination de l'opérateur d'authentification en précisant le service visé. L'opérateur de service transmet également toute information utile au suivi de la requête comme URL de l'application visée, etc.

2. L'opérateur d'authentification vérifie :

- Le format de la requête d'authentification
- La période de validité de la requête connaissant la date et l'heure de création de la requête et la durée de validité autorisée
- L'identifiant de la requête pour éviter un rejeu
- La signature de la requête d'authentification

Si l'utilisateur n'est pas déjà authentifié, l'opérateur d'authentification authentifie l'utilisateur.

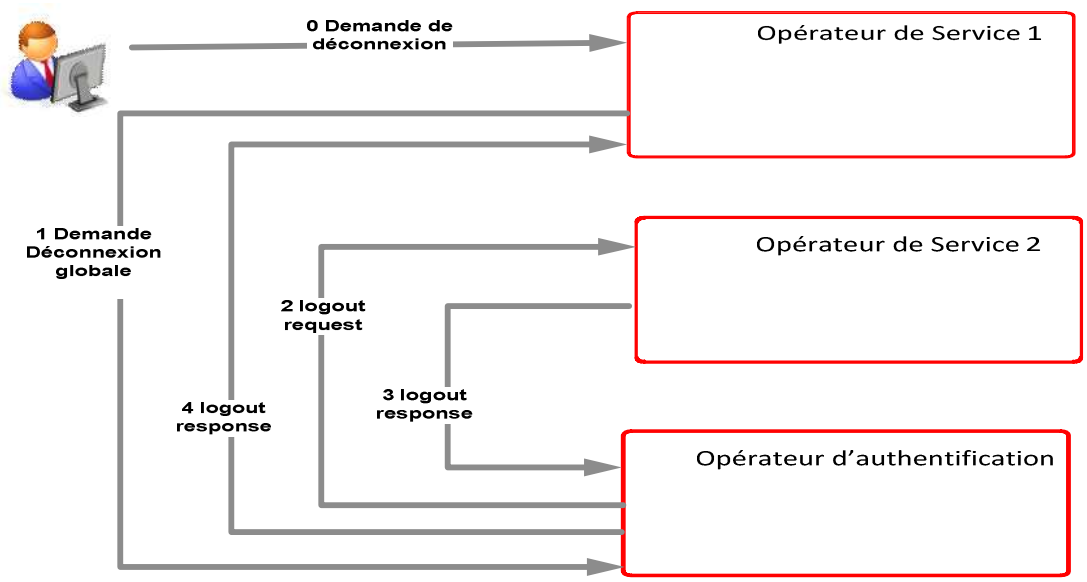
3. L'opérateur d'authentification retourne dans un formulaire auto-soumis à destination de l'opérateur de service une réponse contenant les informations d'authentification, c'est-à-dire le VI.

4. Apres création d'une session à partir du VI, l'utilisateur a accès aux pages demandées.

Déconnexion

Interops-S propose également un mécanisme de déconnexion globale (SLO) permettant de déconnecter un utilisateur sur l'opérateur d'authentification et l'ensemble des opérateurs de service sur lesquels il s'est connecté.

Cinématique de déconnexion :



0. L'utilisateur s'est authentifié sur l'opérateur d'authentification et connecté auprès des opérateurs de service 1 et 2. Il demande alors une déconnexion globale.

1. L'opérateur de service 1 invalide toute session ouverte pour le compte de l'utilisateur. Il génère une demande de déconnexion, la signe et la transmet à l'opérateur d'authentification. **Cette étape est optionnelle si l'utilisateur fait la demande de déconnexion globale directement auprès de l'opérateur d'authentification**.

2. L'opérateur d'authentification vérifie :

- Le format de la demande de déconnexion
- L'adéquation de la demande à l'utilisateur et à l'identifiant de session (égal à l'identifiant du VI)

- La période de validité de la requête connaissant la date et l'heure de création de la requête et la durée de validité autorisée
- L'identifiant de la requête pour éviter un rejeu
- La signature de la requête de déconnexion

L'opérateur d'authentification propage la demande de déconnexion globale en générant des <LogoutRequest> signées pour chacun des opérateurs de service auprès desquels l'utilisateur s'est authentifié, excepté l'opérateur de service émetteur de la demande. Dans notre cas, la demande est transmise uniquement à l'opérateur de service.
Le formalisme et le mécanisme de transmission de la requête sont identiques à l'étape précédente.

3. L'opérateur de service 2 vérifie la demande de déconnexion comme l'opérateur d'authentification à l'étape 2 et invalide toute session encore ouverte pour le compte de l'utilisateur et transmet une réponse à la demande de déconnexion sous forme de <LogoutResponse> signée. Si la session est déjà expirée, l'opérateur de service ne doit pas retourner d'erreur.

4. L'opérateur d'authentification vérifie :
Le format de la réponse de déconnexion

- L'identifiant de la réponse pour éviter un rejeu
- La période de validité de la réponse connaissant la date et l'heure de création de la réponse et la durée de validité autorisée
- La signature de la réponse

L'opérateur d'authentification invalide la session et redirige l'utilisateur vers l'opérateur de service1 avec un <LogoutResponse>.

Note : La transmission des requêtes et des réponses de déconnexion décrites aux étapes 2 et 3 peuvent être conduites en parallèle sur l'ensemble des opérateurs de service en fonction des implémentations.

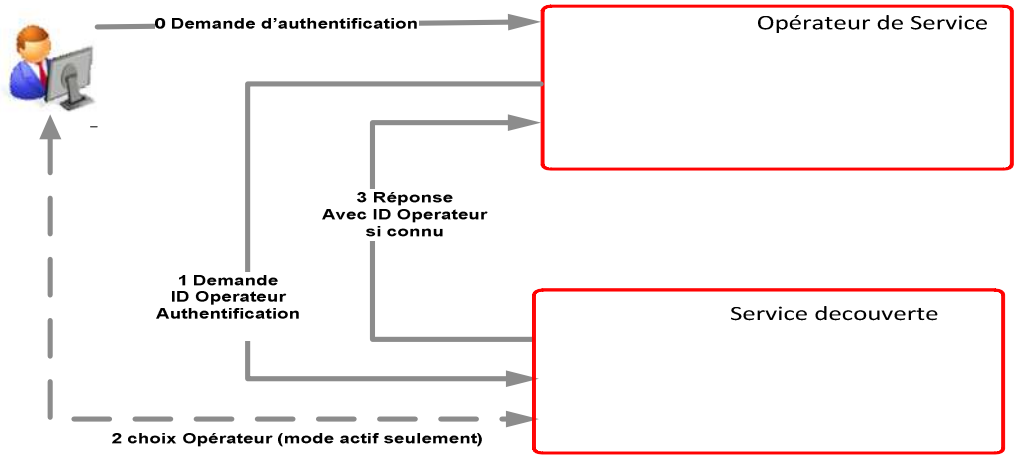
Service de découverte

L'opérateur de service peut chercher à connaître l'opérateur d'authentification auquel est affilié l'utilisateur afin de faire une demande d'authentification. Pour cela il utilise un service de découverte. La cinématique est décrite sur le schéma ci-dessous :
Le service de découverte doit permettre de :

- Sauvegarder l'opérateur d'authentification de l'utilisateur
- Déterminer l'opérateur d'authentification de l'utilisateur pour tout opérateur de service de la sphère de confiance.

La sauvegarde de l'opérateur d'authentification se fait au travers d'un cookie sur le navigateur de l'utilisateur contenant un identifiant du ou des opérateurs d'authentification ayant procédé à l'authentification.

Cinématique service de découverte :



0. L'utilisateur se connecte à l'opérateur de service. L'utilisateur n'est alors pas authentifié. L'opérateur de service cherche à connaître l'opérateur d'authentification de l'utilisateur.

1. L'opérateur de service redirige l'utilisateur vers le service de découverte pour demander l'identifiant de l'opérateur d'authentification en précisant dans la requête :

- L'identifiant de l'opérateur de service
- Le comportement attendu par le service de découverte (mode passif/actif, ne retourne qu'un seul identifiant ou tous, etc.)
- L'URL de retour

2. Le service de découverte lit le cookie partagé et récupère l'identifiant de l'opérateur d'authentification. Si le cookie est inexistant ou si aucun opérateur d'authentification n'est présent, deux comportements sont possibles en fonction du mode choisi :

- Passif : il n'existe aucune interaction entre le service de découverte et l'utilisateur en dehors des redirections. Le service de découverte redirige l'utilisateur vers l'opérateur de service avec en réponse un opérateur d'authentification vide
- Actif : si aucun cookie n'existe ou si aucun identifiant correspondant n'est trouvé, le service de découverte présente une page avec une liste d'opérateurs d'authentification avec lesquels il existe une convention et pour lesquels l'opérateur joue le rôle d'opérateur de service. Ainsi, l'utilisateur peut préciser son opérateur d'authentification. Le service de découverte sauvegarde le choix de l'utilisateur dans le cookie avant de rediriger l'utilisateur vers l'opérateur de service avec cet identifiant d'opérateur d'authentification en paramètre

3. Le service de découverte redirige l'utilisateur vers l'opérateur de service en retournant dans l'URL les informations de l'opérateur d'authentification si elles sont connues.

Vecteur d'identification VI

Chacun de ces modes s'appuie sur l'échange d'un vecteur d'identification permettant d'authentifier l'origine des messages et de transporter des informations sur l'identité de l'utilisateur et son Profil Applicatif Générique Métier (PAGM). La liste des PAGM disponibles pour une application ou un ensemble d'applications est déterminée par les organismes propriétaires d'applications et est rendue disponible aux organismes clients en fonction du contenu de la convention bipartite.

Le Vecteur d'Identification doit contenir à minima les éléments suivants :

- Le numéro de version pour le format du vecteur d'identification
- L'identifiant de vecteur unique pour tous les organismes
- L'identifiant de l'Organisme Client
- L'identifiant de l'utilisateur ou de l'application cliente, éventuellement dépersonnalisé
- La date de création
- La durée de vie de l'habilitation
- L'identifiant de l'Organisme Fournisseur de service
- Le service visé (sous forme d'URI sans partie locale)
- La liste des PAGM valides pour l'utilisateur ou l'application cliente
- Les attributs optionnels facultatifs concernant l'identification de l'utilisateur ou de l'application cliente (indication géographique, localisation, niveau de sécurité,…). Ces attributs ne doivent pas contenir de données applicatives.
- Niveau d'authentification initiale (moyen ou niveau de moyen avec lequel l'authentification initiale de l'utilisateur ou de l'application cliente est réalisée)
- Signature numérique délivrée par l'organisme de départ

.

Note : Les organismes de la sphère de confiance partagent un format de VI commun, dont le format d'identifiant et la liste d'attributs de l'utilisateur. L'identifiant échangé entre les organismes peut être différent de l'identifiant utilisé pour authentifier l'utilisateur. La valeur de cet identifiant est partagé par tous les organismes de la sphère de confiance et établi de manière implicite : aucun processus impliquant l'utilisateur n'est nécessaire pour le définir.

Le standard Interops implémente les standards du marché comme SOAP, WS Security, SAML pour le format du VI, sa sécurisation et son mode de transmission.

Sécurité des échanges

Utilisation de certificats électroniques

Les échanges Interops sont sécurisés par l'utilisation de certificats électroniques X509. Chaque organisme est à même de vérifier que :

- La date de validité du certificat est correcte
- Le certificat a été émis par une chaîne de certification de confiance
- Le certificat n'a pas été révoqué
- L'usage du certificat correspond bien à l'emploi qui en est fait

Sécurisation des flux entre l'utilisateur et différents composants

Toutes les communications entre le navigateur et les différents composants devront être protégées par TLS avec authentification serveur. Les communications seront alors protégées en confidentialité et en intégrité.

Sécurisation des flux Interops-A/P entre les différents composants serveurs

Les échanges entre les infrastructures sont sécurisés par une authentification mutuelle des serveurs et par chiffrement des canaux.

Une architecture de « coupure » des flux applicatifs échangés entre les OPS (composants proxy côté client et reverse proxy côté serveur) permet de contrôler les flux et de gérer les traces de manière centralisée.

Traçabilité / Auditabilité

Les principes de sécurité et d'auditabilité sont élargis aux nouveaux mécanismes. La convention Interops passée entre le client du service et le fournisseur du service définit de manière forte la traçabilité attendue des échanges et l'auditabilité de ces traces.

Chaque partenaire stocke et archive, pour chaque échange, les traces propres à son système d'information ainsi qu'un numéro d'opération unique lié à cet échange (Cette clé correspond à l'identifiant du VI). Ces traces sont à un format pivot défini dans la convention.

En cas de besoin, les traces des deux organismes sont appareillées grâce à l'identifiant du VI et permettent de retracer l'ensemble de l'opération.

La durée de conservation des traces est fixée dans la convention.

Conformité RGS

Interops a fait l'objet de réunions de travail avec la DGME et l'ANSSI pour assurer sa conformité RGS, qui est confirmée. Les moyens cryptographiques utilisés devront suivre les préconisations du RGS V1, en particulier, les tailles de clés, les algorithmes et les profils de certificats.

Conformité RGI

Ce projet respecte les exigences et recommandations du RGI. Des travaux sont en cours conjointement avec la DISIC pour que le standard Interops soit intégré aux recommandations du RGI « V2 ».