

Le réseau interministériel de l'État : un vecteur de transition numérique au service de la modernisation de l'action publique

Hélène BRISSET

SCN RIE
39-43 quai André Citroën
75015 PARIS

Frédéric PACQUIER

SCN RIE
39-43 quai André Citroën
75015 PARIS

Pascal MARYNIAK

SCN RIE
39-43 quai André Citroën
75015 PARIS

Karim BOUDJEMAA

GIP RENATER
23-25 rue Daviel
75013 PARIS

Dominique LAUNAY

GIP RENATER
263 avenue du Général Leclerc
35042 RENNES

Ludovic ISHIOMIN

GIP RENATER
23-25 rue Daviel
75013 PARIS

Résumé

Le conseil des ministres du 25 mai 2011 a décidé la mise en place d'un « réseau interministériel sécurisé regroupant l'ensemble des réseaux des ministères et permettant la continuité de l'action gouvernementale en cas de dysfonctionnement grave d'Internet ». Ce réseau, élément essentiel de la transition numérique de l'action publique, permettra de renforcer encore la sécurité des systèmes d'information de l'État dans un contexte de menaces croissantes.

La conception du RIE a d'abord été confiée à une équipe projet interministérielle. Les travaux pluridisciplinaires ont abouti à la spécification d'une architecture souple et évolutive s'appuyant sur un cœur optique à haut débit reliant les principaux centres informatiques ministériels.

Initié lors d'échanges autour d'IPv6, le partenariat conclu avec le GIP RENATER a très vite mis en exergue l'intérêt économique d'une solution consistant à transporter les flux du RIE de manière indépendante sur les fibres de RENATER, par rapport à la construction d'une infrastructure dédiée. Ce principe, validé par le conseil d'administration du GIP en mars 2012, a de plus permis le déploiement très rapide d'un cœur de réseau sécurisé en technologie MPLS/IP à 10 Gbits/s, opérationnel depuis juillet 2013.

Les premiers sites pilotes seront raccordés au dernier trimestre 2013, et la grande majorité des 17000 sites ministériels

rallieront le RIE, de 2013 à 2016, via des réseaux de collecte opérés par des opérateurs de télécommunications.

Un service à compétence nationale rattaché au directeur interministériel des systèmes d'information, a pris dès sa création en décembre 2012 le relais de l'équipe projet initiale, et doit assurer la gestion, l'exploitation et la sécurité du RIE.

Mots-clefs

Infrastructure, Projet, Mutualisation

1 Contexte

1.1 Un contexte interministériel complexe

Le système d'information de l'État s'est construit progressivement, dans des organisations dites « en silo », en fonction des besoins propres et des contraintes de chaque administration, et sans la mise en place d'infrastructures communes d'échange et de partage des ressources. Il en résulte un patrimoine applicatif composé de milliers de systèmes hétérogènes partiellement interconnectés, et qui s'appuient sur des infrastructures multiples de réseaux et de production informatique réparties dans 130 salles principales.

Aussi, la transformation du système d'information de l'État à une échelle interministérielle apparaît comme une nécessité pour accompagner les réformes dans de nombreux domaines, notamment dans le développement de la relation numérique à l'utilisateur, pour anticiper l'évolution des technologies, optimiser les coûts et améliorer l'efficacité.

La première phase de cette transformation est la mutualisation des infrastructures et des services transverses dans laquelle s'inscrit la réalisation du réseau interministériel de l'État. Dans un contexte de menaces informatiques et cybernétiques croissantes, cette mutualisation des infrastructures de communication visera également à renforcer la résilience face à cette expansion des attaques. Enfin, elle accompagnera la réorganisation de l'administration territoriale, en offrant aux directions départementales interministérielles une infrastructure d'échange et de services communs.

1.2 Un projet interministériel d'ampleur décidé en conseil des ministres

Le conseil des ministres du 25 mai 2011 a décidé de la mise en place d'un « réseau interministériel sécurisé regroupant l'ensemble des réseaux des ministères et permettant la continuité de l'action gouvernementale en cas de dysfonctionnement grave d'Internet ».

Un travail interministériel soutenu a été conduit depuis juin 2011 afin de spécifier et de construire le réseau interministériel de l'État (RIE). Ce réseau viendra remplacer l'ensemble des réseaux ministériels existants, raccordant ainsi progressivement près de 17 000 sites entre 2013 et 2017.

Le RIE constitue un élément essentiel de la transition numérique de l'action publique. Il s'inscrit dans les orientations arrêtées lors du comité interministériel de la modernisation de l'action publique du 18 décembre 2012.

2 Conception et Architecture

2.1 Des travaux interministériels conduits depuis deux ans

Une équipe de projet interministérielle intégrée a été mise en place dès le début du projet en mai 2011, afin de prendre en compte l'ensemble des besoins ministériels, et de mutualiser les compétences et les expertises. Un cycle de réunions plénières mensuelles de l'équipe a été instauré, et les travaux de conception du réseau ont été structurés en 8 chantiers interministériels majeurs, dont les objectifs sont présentés ci-dessous.

- Adressage : constitution d'un plan d'adressage urbanisé pour raccorder à minima les ministères relevant du premier périmètre de déploiement.

- Architecture : analyse des points clés et propositions concernant les éléments structurants d'architecture.
- CCTP : élaboration des pièces contractuelles en vue des consultations pour la réalisation.
- Implémentation IPv6 : analyse et anticipation des impacts de la mise en œuvre d'IPv6 ; identification de scénarii de transition V4/V6 (LAN et WAN).
- Démonstrateur : identification d'un périmètre pertinent (cas d'usage, sites et infrastructures) ; préparation de la mise en place du démonstrateur.
- Sécurité : analyse des points clés concernant la sécurité du réseau (sécurisation des flux, cloisonnement éventuel, sondes de sécurité).
- Outils de gestion : analyse des outils de gestion existants (sites, liens, configurations, commandes...), étude des possibilités d'extension et/ou proposition d'un cahier des charges fonctionnel pour le futur outillage commun du RIE.
- Migration : préparation de la migration, identification des spécificités et contraintes ministérielles.

Ces travaux interministériels ont abouti à la conception d'une architecture souple et évolutive s'appuyant sur un cœur optique à haut débit, et dont les éléments sont détaillés au chapitre 3 du présent article. Les principaux points de raccordement au cœur de réseau sont ainsi hébergés dans des centres informatiques ministériels, qui disposent alors d'une connexion directe à très haut débit sur le RIE, facilitant l'accès aux applications ministérielles ou interministérielles. Les sites utilisateurs seront raccordés au cœur de réseau par l'intermédiaire de réseaux de collectes régionaux s'appuyant sur les infrastructures d'opérateurs de télécommunications.

2.2 Le choix stratégique d'un partenariat avec RENATER

Initié lors d'échanges autour de la technologie IPv6, un partenariat fort a été conclu avec le GIP « réseau national de télécommunications pour la technologie, l'enseignement et la recherche » (RENATER).

L'architecture initialement envisagée pour le RIE s'appuyait sur des fibres optiques « noires », c'est-à-dire brutes, sans service intégré d'opérateur de télécommunications. Ce choix permettait de répondre à des besoins en débit en très forte augmentation, en utilisant les larges capacités existantes déployées par des entités tierces tels que les autoroutiers et les transporteurs d'énergie, qui louent leur capacité aux opérateurs de télécommunication. Il nécessitait cependant une part importante d'investissement la première année à hauteur de 27,5 M€ TTC pour la seule infrastructure optique.

Le scénario retenu in fine consiste à transporter les flux du RIE de manière indépendante sur les fibres du réseau RENATER. Le transport des flux gouvernementaux sur cette infrastructure ne nécessite plus le déploiement d'une infrastructure propre sur l'ensemble du territoire mais uniquement la mise en œuvre de liens optiques complémentaires entre les datacenters ministériels hébergeant les équipements du RIE et le cœur de réseau RENATER.

Ce scénario d'adossement à RENATER, instruit avec les ministères et le GIP, a permis de dégager des économies significatives par rapport à la construction d'une infrastructure dédiée, avec une économie plus de 20 M€ TTC en investissement et de 140 k€ TTC annuels en récurrent.

Les schémas qui suivent représentent les liens à construire dans les différents scénarios. Dans le cas de l'infrastructure dédiée envisagée initialement, l'ensemble des liens auraient été à construire, soit près de 6 200 km avec le maillage représenté en figure 1. Dans le cas de l'adossement à RENATER, les liens à construire sont indiqués en rouge dans le schéma ci-dessous, soit environ 1 000 km avec le maillage représenté en figure 2. La figure 3 représente un zoom sur le raccordement d'un PIB à l'infrastructure RENATER.

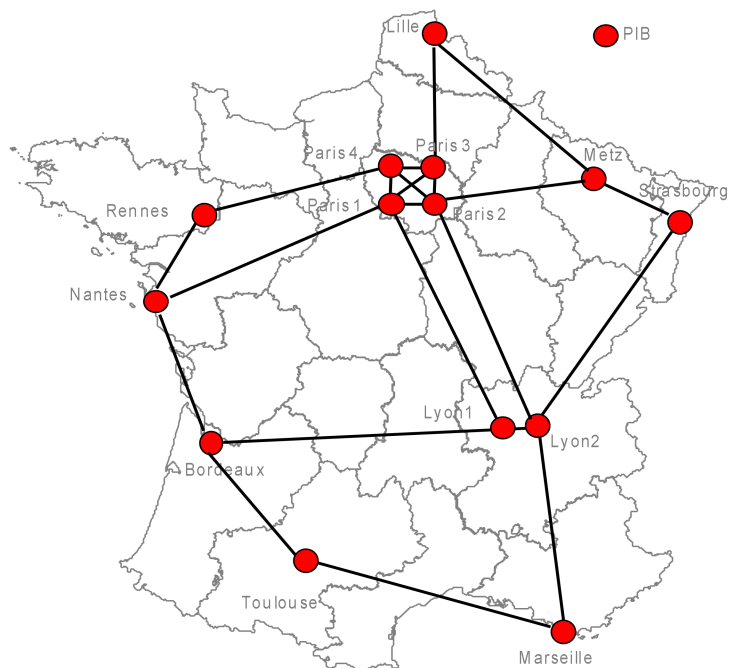


Figure 1 - Carte initiale du RIE
 Les cercles rouges représentent les Points d'Interconnexion au Backbone (PIB)
 Les traits noirs sont les liens à construire

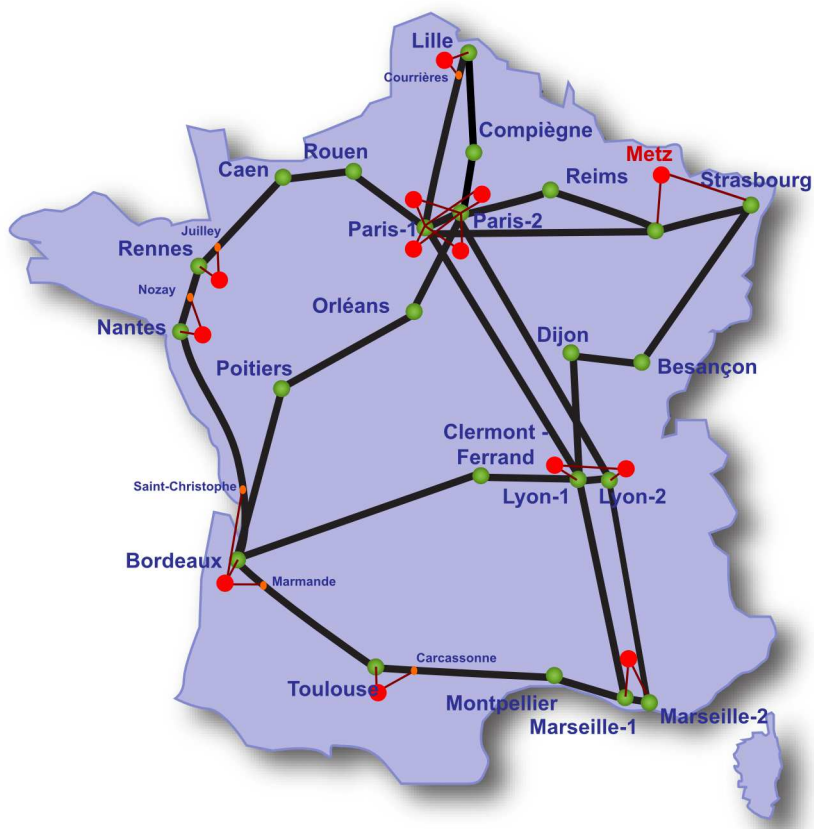


Figure 2 - Adossement du RIE à RENATER
 Les nouveaux liens à construire sont en rouge

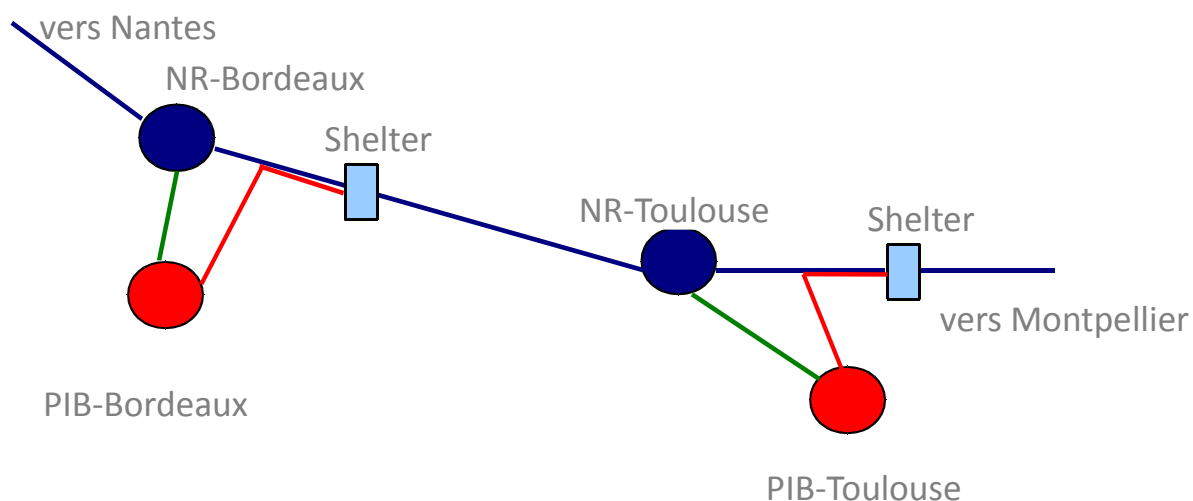


Figure 3 – Zoom sur le raccordement d'un PIB

L'architecture physique du backbone RIE s'appuie ainsi sur les fibres optiques de RENATER déployées et sur des équipements optiques gérés par l'infrastructure optique de RENATER. L'achat de fibres optiques noires (FON) reste cependant nécessaire pour relier les points d'interconnexion au backbone RIE (PIB) au réseau RENATER existant.

Afin de valider techniquement, économiquement et juridiquement ce scénario, des travaux ont été conduits en étroite collaboration entre le GIP RENATER et la direction interministérielle des systèmes d'information et de communication (DISIC).

Un conseil d'administration du GIP RENATER s'est tenu le 7 mars et a validé le principe d'adossement du RIE à ses infrastructures.

D'un point de vue administratif, les prestations confiées à RENATER font l'objet d'une convention de service, qui formalise les modalités de collaboration entre le GIP RENATER et la DISIC et d'utilisation privative partielle des infrastructures optiques de RENATER au profit du RIE.

Sur le plan juridique, une saisine préalable de services juridiques ministériels et de l'ARCEP a également permis de vérifier que le support du réseau RIE ne modifie pas les missions du GIP RENATER et que le RIE constitue bien un réseau privé.

Une vigilance particulière a également été portée sur la sécurité de cette alternative : l'utilisation d'une longueur d'onde spécifique empêche tout couplage de flux et garantit ainsi une étanchéité des flux du RIE vis à vis d'autres flux pouvant transiter sur le réseau RENATER.

Par ailleurs, l'analyse de sécurité globale menée sur le RIE intègre notamment les périmètres de prestations confiées à RENATER. En complément, une vérification de la sécurité physique des nœuds de raccordement RENATER auxquels sont rattachés les PIB du RIE a été réalisée et a permis l'engagement des premiers travaux d'infrastructure nécessaires.

2.3 Des choix techniques partagés

L'utilisation du protocole IP s'avère indispensable, du fait de son universalité dans les systèmes et réseaux de communication. Le déploiement initial du RIE est prévu dans la version IPv4, mais les saturations d'adresses aujourd'hui constatées dans cette version imposent également la gestion native d'IPv6 dès le démarrage du projet.

La technologie MPLS, ainsi que l'utilisation de la HQoS (Hierarchical Quality of Service) permettent d'assurer un cloisonnement des flux entre les différentes communautés ministérielles, et une gestion globale et hiérarchique de la qualité de service, sur la même infrastructure physique de communication.

Enfin, en matière de transmission, le choix de la technologie DWDM offre des débits initiaux très importants de l'ordre de 10 Gbits/s, et permet de disposer d'un potentiel d'accroissement de la bande passante du cœur de réseau, jusqu'à 100 Gbits/s. La technologie DWDM déployée sur RENATER permet de multiplexer 32 longueurs d'onde sur une fibre optique. Un groupe de 8 a été mis à disposition du RIE.

3 Réalisations

3.1 Point d'avancement sur le déploiement opérationnel du RIE

Au 11 juillet 2013, l'ensemble des douze centres informatiques ministériels, PIB, sont raccordés au cœur de réseau à très haut débit. Ce cœur s'appuie ainsi sur les fibres de RENATER.

3.1.1 Infrastructure optique

La construction de l'infrastructure optique a fait l'objet de plusieurs marchés. Une première consultation menée par la DISIC a porté sur la construction des fibres optiques noires permettant de raccorder un PIB à un NR ; elle a été découpée en lots géographiques dans le cadre d'un appel d'offres ouvert, notifiés en octobre 2012 à la société SFR. Le déploiement des tronçons s'est terminé en juillet 2013.

Les fibres optiques permettant de raccorder un shelter d'amplification optique à un PIB (cf schéma de la figure 3) ont fait l'objet de marchés établis et notifiés fin 2012 par RENATER aux opérateurs titulaires de ses FON : SFR pour les PIB de Rennes, Nantes, Bordeaux et Toulouse, et VIATEL pour le PIB de Lille. Les livraisons des tronçons sont intervenues d'avril à août 2013.

Enfin, l'acquisition et le déploiement du matériel optique DWDM a fait l'objet de marchés notifiés par le GIP à ses deux sous-traitants, Alcatel-Lucent, pour la fourniture des équipements permettant l'intégration du PIB de Lille, et CIENA pour la fourniture des équipements liés à tous les autres PIB. La première lambda entre les deux PIB lyonnais a été mise à disposition en avril, la dernière lambda qui fermait la boucle ouest du RIE a été déployée dans la foulée du dernier tronçon de FON livré en août.

Au total, près de 25 shelters ou NRs ont fait l'objet d'une intervention, parfois de nuit, pour déployer les lambdas du RIE. La figure 4 fait état de ces modifications. Le déploiement de ces nouvelles lambdas a pu se faire sans impact notablement significatif pour les utilisateurs RENATER.

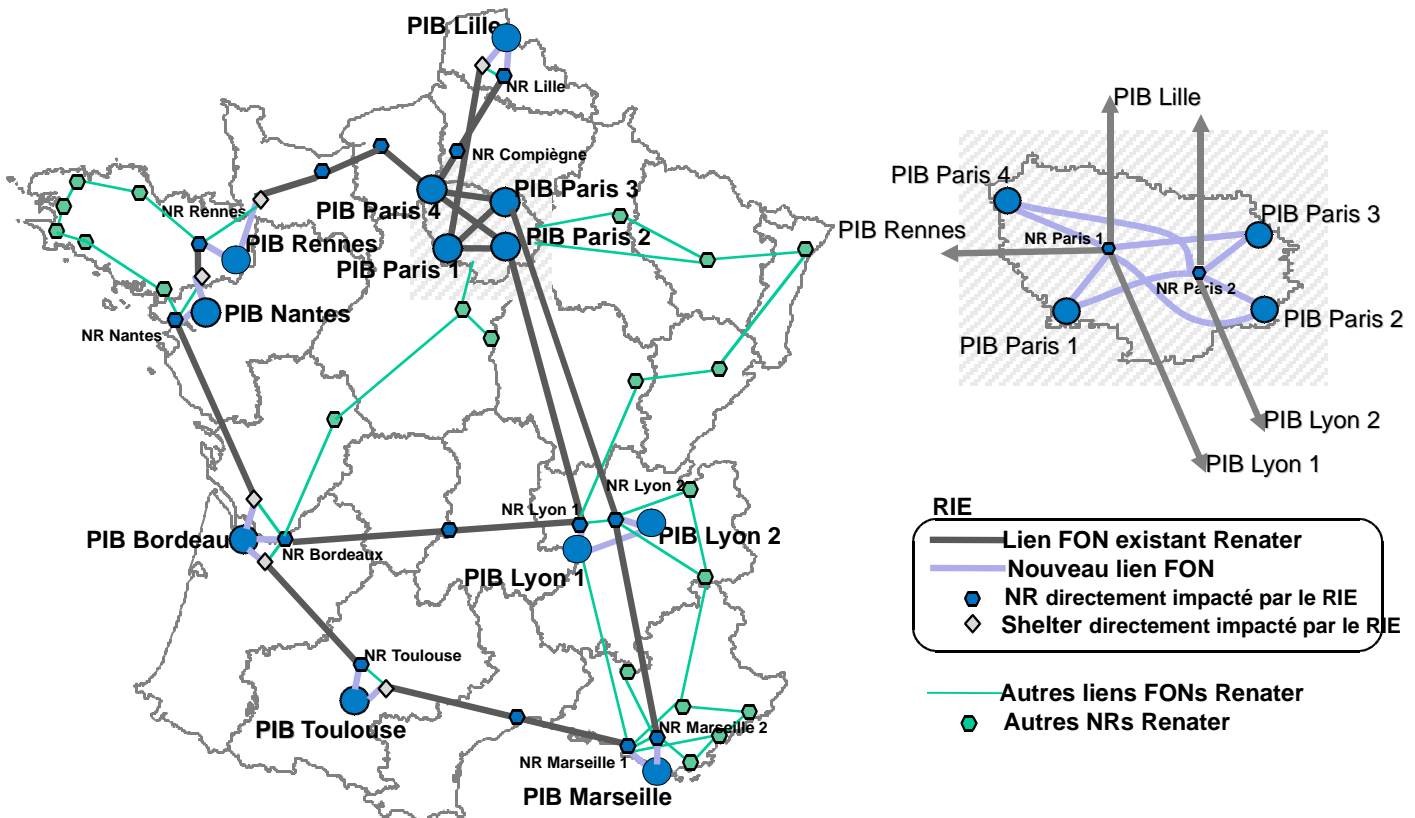


Figure 4 – Carte de cheminement des lambdas RIE

3.1.2 Couches de niveau 2 et 3 au cœur

La vérification d'aptitude du cœur de réseau a été prononcée le 12 septembre, et le cœur optique est opérationnel, et prêt à recevoir les sites ministériels et institutionnels.

Après migration sur le RIE, les flux des systèmes d'information ministériels seront transportés indépendamment sur ce cœur à haut débit, au sein d'une communauté MPLS VPN dédiée, à l'exception des ministères concernés par l'ATE¹ pour lesquels une communauté d'usage sera construite.

3.1.3 Réseaux de collecte

S'agissant des réseaux de collecte, l'accord-cadre permettant le raccordement de la grande majorité des 17 000 sites ministériels à cette infrastructure a été notifié. En fonction du phasage de migration, le raccordement des différents périmètres ministériels fera ensuite l'objet de marchés subséquents portés par les services du Premier ministre sur cet accord-cadre. Le premier marché subséquent a été notifié le 7 août 2013, pour le premier périmètre de déploiement, qui concerne les entités suivantes : ministère de l'Agriculture, de l'Écologie, de la Santé, de l'Intérieur, des Finances (CCRF), du Travail et services du Premier ministre.

Les premiers sites pilotes seront ainsi raccordés à partir de septembre 2013. La grande majorité des 17 000 sites ministériels sera ensuite raccordée de 2013 à 2016.

3.1.4 Migration

Sur le premier périmètre, des travaux spécifiques sont engagés depuis septembre 2011 avec l'ensemble des ministères de la communauté ATE pour définir le plan d'adressage cible et préparer la migration des directions départementales interministérielles et des préfetures. Un groupe de travail est par ailleurs constitué avec l'ensemble des ministères pour définir les stratégies et modalités de migration des différents périmètres ministériels.

Dans le cadre du premier périmètre, une étape pilote, menée de septembre à décembre 2013, permettra tout d'abord de tester le bon fonctionnement des liens sur un nombre restreint de sites, puis de valider le processus de déploiement de masse. Le déploiement généralisé sur l'ensemble des 5000 sites pourra alors être lancé début 2014, avec un objectif d'achèvement à fin 2014, ce qui nécessitera une cadence maximale mensuelle de 150 sites par semaine.

3.2 La structure pilotant la construction et l'exploitation a été créée

Parallèlement aux travaux de construction du RIE, il s'est également agi de définir les moyens de gérer et d'exploiter durablement le réseau. Le Premier ministre a demandé en janvier 2012 au Conseil général de l'économie, de l'industrie, de l'énergie et des technologies (CGEIET) d'étudier le périmètre fonctionnel de la future structure interministérielle en charge de la gestion du RIE, en particulier les missions, la forme juridique, les modalités de gouvernance et le dimensionnement de ses moyens.

Le rapport du CGEIET remis au cabinet du Premier ministre en juin 2012, et dont les conclusions ont été présentées aux DSI des ministères a préconisé la création d'un service à compétence nationale (SCN) chargé de construire et de gérer le réseau interministériel de l'État, rattaché au directeur interministériel des systèmes d'information et de communication, mais disposant d'une large autonomie décisionnelle et financière.

Ce portage fait suite au souhait fort exprimé par les ministères que l'opérateur du réseau RIE constitue une structure ad hoc et ne dépende pas d'un seul ministère.

Le périmètre du SCN porte sur le réseau et les services associés. Le périmètre des services pourra être étendu sur validation des instances de gouvernance, en fonction des opportunités d'offres de service interministérielles et de mutualisation existantes. Le maître d'ouvrage de ce réseau pourra être de cette manière une force de proposition pour de nouveaux services ultérieurs (messagerie, téléphonie, etc.).

Le service à compétence nationale « Réseau interministériel de l'État » a ainsi été créé par arrêté du Premier ministre au 17 décembre 2012. Il est chargé de la gestion du réseau interministériel de l'État et des services associés. La construction et la gestion du RIE sont ainsi réalisées à partir des compétences ministérielles existantes. Ses agents viennent aujourd'hui de sept ministères.

1. ATE : Administration Territoriale. Cette communauté regroupe les services déconcentrés dans les préfetures et sous-préfetures des ministères.

Ce service s'appuie sur les instances de gouvernance de la DISIC : conseil des systèmes d'information et de communication avec les secrétaires généraux des ministères et comité technique des systèmes d'information et de communication avec les directeurs des systèmes d'information ministériels.

3.3 Un projet de mutualisation source d'économies de fonctionnement importantes

Les scénarios économiques de modélisation du retour sur investissement, construits sur la base d'entretiens conduits avec les DSI ministérielles, ont confirmé l'obtention de gains de plusieurs millions d'euros par an avec la mise en place du RIE par rapport au maintien des réseaux existants.

Les consultations notifiées à ce jour, correspondant à la construction du cœur de réseau, au raccordement des sites capillaires, et au transit internet sont pleinement conformes aux hypothèses de modélisation de l'étude économique.

Concernant la collecte, pour le premier périmètre, les gains moyens sur le budget de collecte sont supérieurs à 30%, à parc déployé homogène. Un calibrage des évolutions en débit par entité devra par ailleurs être réalisé pour tenir compte de l'évolution nécessaire pour certains sites.

4 La SSI au cœur du projet

4.1 Les options générales de sécurité

La mise en place du RIE, en tant que réseau de transport interministériel, participe de l'amélioration de la sécurité et de la protection des systèmes d'information et des données de l'État, dans un contexte général marqué par un accroissement des menaces informatiques et cybernétiques. Ainsi, le regroupement des réseaux ministériels dans une infrastructure globale de transport indépendante d'internet, permettra, en cas d'indisponibilité ou d'attaque grave sur celui-ci, de préserver la continuité des échanges interministériels, et donc d'assurer la continuité de l'action gouvernementale.

De plus, la mutualisation des passerelles vers l'internet, dans le cadre de la mise en œuvre du RIE, permettra un filtrage global et homogène des flux échangés, et une meilleure coordination dans la détection et la réaction face aux attaques. Un cloisonnement interne des flux entre les différentes communautés ministérielles permettra d'éviter les risques de propagation en cas de contamination.

Enfin, la mise en place d'une surveillance globale des flux échangés entre les différentes communautés d'une part, et avec les réseaux extérieurs dont internet d'autre part, permettra de passer à une véritable stratégie de défense active en profondeur, combinant la protection intrinsèque des systèmes, la surveillance permanente et la réaction rapide.

L'ANSSI, autorité nationale dans le domaine de la SSI, est pleinement associée à toutes les étapes de conception et de construction du réseau, et pilote un groupe de travail dédié à la SSI, qui contribue à définir les choix structurants d'architecture et de sécurité afin que le niveau de sécurité du RIE soit conforme aux attentes du conseil des ministres du 25 mai 2011. L'agence apportera également son soutien dans la phase d'exploitation opérationnelle, tout particulièrement dans l'analyse et le traitement des incidents de sécurité. Les sondes de sécurité, aujourd'hui déployées par l'ANSSI sur la plupart des systèmes d'information ministériels seront intégrées nativement au RIE.

La gestion de la sécurité du RIE fait l'objet d'une organisation adaptée au SCN RIE, avec la mise en place en son sein d'un centre opérationnel de la sécurité (SOC), en charge de piloter et de coordonner l'ensemble des actions permettant d'assurer la sécurité du RIE, en interface avec les chaînes ministérielles, et l'ANSSI.

4.2 Exigences particulière de sécurité vis-à-vis de l'utilisation de l'infrastructure RENATER

L'utilisation d'une longueur d'onde spécifique empêche le couplage des flux, et garantit ainsi une étanchéité des flux du RIE vis-à-vis des autres flux pouvant transiter sur le réseau RENATER.

Si le maillage du réseau permet d'assurer l'acheminement des flux par des routes différentes en cas de défaillance de l'un de ses composants, il a été jugé nécessaire de mener une campagne d'évaluation du niveau de sécurité physique et de fonctionnement des locaux hébergeant les nœuds de raccordement RENATER. Les audits menés conjointement par le GIP RENATER et la DISIC dans le cadre de cette campagne, ont permis de formuler des préconisations adaptées pour chaque site, afin de garantir le niveau de sécurité visé. Ces mesures portent notamment sur la protection de l'accès aux équipements, et sur le renforcement de la sécurité des servitudes (climatisation, alimentations électriques). Ce travail conjoint DISIC/GIP RENATER sur les nœuds RENATER concernés par le passage du RIE a d'ailleurs vocation à être reproduit par le GIP sur les autres NR.

Si le maillage permet la transmission des données par différentes routes et répond au moins partiellement aux contraintes de disponibilité du réseau, il est néanmoins nécessaire de s'assurer de la faible probabilité de panne ou d'acte de dégradation volontaire de matériels. C'est pour cela qu'une campagne d'audits sur les différents sites par lesquels transite le RIE a eu lieu. Le périmètre étudié couvre les préoccupations suivantes :

- l'alimentation électrique et le refroidissement des locaux sont-ils assurés, secourus et protégés ?
- l'accès aux locaux par une personne malintentionnée est-il possible ? si oui, peut-il être détecté et la personne identifiée ?
- enfin, la sécurité des locaux contre les sinistres est-elle assurée ?

À l'issue de ces audits, les sites pour lesquels les mesures existantes ont été considérées comme insuffisantes ont reçu une liste de préconisations adaptées à leur situation. Si ces préconisations sont parfois organisationnelles, d'autres nécessitent l'ajout ou la mise à jour de matériels. La mise en œuvre de ces mesures permet une homogénéisation du niveau de sécurité physique de l'hébergement du RIE. Ce travail conjoint DISIC/GIP sur les Nœuds RENATER concernés par le passage du RIE a vocation à être reproduit par le GIP en direction des autres NRs.

5 Conclusion

Le RIE constitue le socle pour la mise en place de services fédérateurs. Par sa conception, il permet le portage des services ministériels ou interministériels existants dès migration des différents systèmes d'information.

De plus, dès sa mise en service, le RIE offrira nativement un accès sécurisé et haut débit à Internet, des interconnexions vers les réseaux des partenaires et les services complémentaires nécessaires au bon fonctionnement du réseau tels qu'un service de résolution de noms de domaine (DNS).

Des travaux sont par ailleurs engagés pour mettre en place progressivement des services interministériels comme la téléphonie (ToIP) et la visioconférence.

Enfin, des travaux spécifiques sont engagés sur le périmètre de l'ATE pour mettre en place des services fédérateurs, tels que l'annuaire, les services de gestion du parc, les serveurs bureautiques, au profit des préfetures et directions départementales interministérielles, qui ne disposent pas de services unifiés à ce jour.