

Tour d'horizon des services de RENATER

Laurent Gydé
GIP RENATER

Résumé

L'offre de services de RENATER évolue continuellement. Quelques mois après d'importantes réorganisations opérées au sein du GIP, cet article récapitule la nouvelle offre de services consolidée de RENATER, les modalités de son évolution et l'organisation mise en œuvre.

Mots clefs

RENATER, NREN, CRU, CORAP, UREC, services

1 Introduction

En janvier et avril 2011, le périmètre des services du GIP RENATER a été étendu par l'intégration des missions et des équipes du Centre Opérationnel du Réseau Académique Parisien (CORAP, 5 personnes) et de la cellule technique du Comité Réseau des Universités (CRU, 11 personnes). Des compétences supplémentaires, mises à disposition en février 2011 par le CNRS et issues de l'Unité Réseaux du CNRS (UREC, 4 personnes) ont par ailleurs renforcé les équipes techniques du GIP sur des missions de sécurité ou d'ingénierie du réseau et de ses services.

La première partie de cet article décrit et illustre par des exemples concrets les principaux cas de figure conduisant à l'introduction ou au retrait éventuel d'un service sur RENATER. On y trouvera en particulier l'organisation et le fonctionnement du Groupe de Consultation sur les Services.

Dans un second temps, nous passons en revue l'ensemble des services que RENATER propose à la communauté Enseignement Recherche française, selon un classement en trois catégories : les services réseaux, les services applicatifs et les services de sécurité.

Enfin, les outils et les prestations mis en place pour la fourniture des services par le GIP RENATER sont abordés dans la troisième partie. La nouvelle organisation de l'équipe, en vigueur depuis juin 2011 et conçue pour correspondre au récent élargissement des missions, y est décrite et expliquée.

2 L'évolution des services de RENATER

Avant d'entrer dans le détail du portefeuille des services de RENATER, il convient d'exposer les modalités qui gouvernent son évolution. Une qualité essentielle de cette offre doit en effet être de s'adapter aux nouveaux usages et d'évoluer conformément à l'environnement technologique et scientifique de la communauté des utilisateurs. Les principales raisons conduisant à l'introduction de nouveaux services sont les suivantes :

- la demande des utilisateurs est prise en compte au sein du Groupe de Consultation sur les Services (GCS) dont le fonctionnement et les premiers résultats seront donnés ;
- les évolutions technologiques et l'innovation doivent rester un critère essentiel afin de maintenir le réseau au niveau requis par les usages les plus exigeants ;
- les collaborations européennes et internationales permettent l'accès à des services mutualisés avec d'autres réseaux dans le monde ;
- la reprise au sein de RENATER de certains services, déployés initialement dans un contexte local à un établissement ou à une communauté, permet de les pérenniser et d'en accompagner la demande croissante.

2.1 Les utilisateurs et le Groupe de consultation sur les services

Créé en 2010, le Groupe de Consultation sur les Services, ou GCS, de RENATER a pour vocation d'organiser le dialogue entre RENATER et ses utilisateurs après que des nouveaux services de nomadisme, d'authentification ou de sécurité, soient venus enrichir l'offre initiale de services de connectivité au réseau. En effet, ces applications situées dans les couches plus hautes ont rendu indispensable la possibilité pour les utilisateurs de s'exprimer sur la nature précise de chaque nouveau service et sur les modalités administratives et techniques de sa fourniture. Le GCS est composé de personnes désignées par les organismes membres du GIP RENATER (c'est à dire représentés au conseil d'administration) et il rapporte au conseil d'administration du GIP.

Les réunions du GCS se tiennent deux fois par an ; elles sont pilotées par la Direction des Relations Extérieures de RENATER, en collaboration avec la Direction Technique (et la cellule technique du Comité Réseau des Universités ou CRU, jusqu'en 2011).

Ce groupe de travail favorise donc l'information des membres du GIP RENATER concernant les services mais a aussi pour vocation de permettre au GIP de recueillir des propositions et des expressions de besoins à des fins prospectives.

Le GCS a déjà traité de nombreux sujets dont la fédération d'identité, la fourniture de certificats (Terena Certificate Services), l'adressage et le nommage, l'antispam, IPv6, la visioconférence, la ToIP, etc. Dès sa première année de fonctionnement, le GCS a en particulier produit une étude sur un service mutualisé de messagerie collaborative à partir de laquelle le conseil d'administration du GIP a décidé le lancement d'une phase pilote dès 2011.

Dans l'avenir, le GCS sera aussi appelé à jouer un rôle décisif lors de la fin de vie des services. Au delà du rôle consultatif pour lequel il se prononcera sur le retrait de tel ou tel élément de l'offre RENATER, ce groupe permettra à chaque membre du GIP d'organiser pour lui même les modalités pratiques de la migration vers les services de substitution.

2.2 L'innovation et les évolutions technologiques

Au gré des progrès de la technologie, certains standards, protocoles, logiciels ou équipements rendent disponibles de nouvelles fonctionnalités au bénéfice des utilisateurs. Dans la cadre de la veille et de l'innovation, le GIP RENATER identifie les évolutions techniques à mettre en œuvre pour compléter et améliorer son portefeuille de services, soit lors des déploiements de nouvelles infrastructures, soit lors des mises à jour des matériels et logiciels existants.

Depuis la création de RENATER, cette fonction d'innovation a permis d'introduire de nombreux services pour la communauté : multicast, IPv6, transport optique, authentification réseau massivement répartie, fédération d'identité, VPN de niveau 2 et 3, très hauts débits... Le plus souvent, RENATER a pu réaliser ces progrès bien avant que ceux ci ne deviennent des produits standards du marché, permettant à ses utilisateurs d'être eux mêmes innovants dans leur démarche d'enseignement et de recherche.

2.3 L'accès à des services mutualisés avec d'autres partenaires

RENATER s'inscrit dans une communauté de réseaux nationaux de recherche et d'éducation (National Research and Education Network ou NREN) au sein de laquelle divers partenariats et collaborations permettent de proposer des services sur des périmètres européens et internationaux. RENATER est ainsi l'un des 34 partenaires du réseau européen GÉANT et est membre de l'association TERENA (Trans European Research and Education Networks Association). À ce titre, les équipes du GIP participent à des travaux en partenariat avec les homologues étrangers et bénéficient des résultats correspondants, qui peuvent se traduire par de nouveaux services.

C'est dans ce cadre que RENATER fournit par exemple :

- la connectivité internationale vers les réseaux de recherche, avec des services interdomaine de supervision et de métrologie ;
- l'extension de la mobilité eduroam sur tous les continents ;
- la fourniture de certificats de serveurs et de personnes reconnus par les navigateurs.

2.4 La reprise de services existants

La communauté des utilisateurs de RENATER est à la fois dynamique et techniquement très compétente. Il arrive qu'un service développé initialement par un établissement ou un groupe d'utilisateurs pour ses propres besoins doive évoluer pour répondre à son succès auprès d'une population bien plus large. Compte-tenu de son organisation dédiée à l'ensemble de la communauté de l'enseignement et de la recherche, RENATER est dans certains cas bien placé pour poursuivre la fourniture et l'évolution de ces services. C'est ainsi que des services tels que VRVS (maintenant EVO) ou RMS intègrent notre portefeuille.

3 Les services de RENATER

Dans le cadre de cet article, les services de RENATER sont rangés selon trois catégories : les services réseaux, les services applicatifs et les services de sécurité. Bien entendu, certains services appartiennent à plusieurs de ces catégories et cette présentation est donc une classification possible parmi toutes les autres.

3.1 Les services réseaux

3.1.1 *Service d'enregistrement pour les ressources réseau (adresses IP, noms de domaine)*

Le GIP RENATER agit en tant que LIR (Local Internet Registry) pour les établissements connectés à RENATER. Il assure donc l'allocation des ressources IP (adresses IPv4, IPv6) en fonction des besoins exprimés par les établissements. RENATER dépend du RIPE NCC, registre Internet régional (RIR) en charge de la gestion des ressources IP en Europe. De ce fait le GIP RENATER doit respecter les règles d'allocation définies par le RIPE, qui visent à s'assurer de la bonne gestion des ressources de l'Internet. Les noms de domaine de la zone .fr sont délivrés par l'AFNIC, à laquelle on s'adresse par l'intermédiaire d'un opérateur (bureau d'enregistrement). Le GIP RENATER gère les demandes d'enregistrement ou de modification de noms de domaine pour les établissements agréés RENATER.

3.1.2 *Raccordements et services à l'accès*

Selon les localisations et les besoins spécifiques, les sites utilisateurs peuvent être directement raccordés à un NR (Nœud RENATER) ou, cas le plus fréquent, utiliser les services et l'infrastructure d'un réseau métropolitain ou régional. Dans les deux hypothèses, l'accès au réseau national se traduit par la mise en place d'un agrément décrivant en particulier les conditions techniques et contractuelles d'utilisation du réseau, ainsi que les contreparties financières éventuelles. L'interface SAGA (Système d'Aide à la Gestion des Agréments) permet non seulement de décrire le site et les caractéristiques de base de son raccordement (localisation, correspondants, adressage, interface physique, débit), mais aussi de déclarer la souscription à des services complémentaires parmi ceux décrits dans le présent article.

3.1.3 *Accès et exploitation des points d'échange (SFINX, REUNIX, GUYANIX ...)*

Le GIP RENATER gère plusieurs points d'échange Internet (Internet Exchange Point ou IXP) : le SFINX en métropole, le REUNIX à l'île de la Réunion et (en projets) le GUYANIX en Guyane ainsi que le MAYOTIX à Mayotte.

Ces IXP facilitent les échanges locaux entre Fournisseurs d'Accès à Internet (FAI), et entre RENATER et ces FAIs. Les utilisateurs de RENATER peuvent ainsi bénéficier de meilleures performances au moment d'accéder à des FAIs locaux. RENATER participe également au développement de l'Internet en promouvant les points d'échanges. En métropole comme dans les DOM-TOM, les points d'échange opérés par RENATER permettent d'optimiser la bande passante des accès Internet locaux et des liaisons RENATER vers la métropole.

3.1.4 *Services de VPN*

Les services de VPN de RENATER sont utilisés par les établissements qui ont besoin d'une infrastructure réseau dédiée sur le réseau national. Pour chaque demande, les équipes de RENATER proposent la solution technique la plus à même de construire le circuit. En fonction des services qui doivent être véhiculés dans les circuits (Ethernet, IPv4, IPv6, multicast...), des débits et du coût, le VPN mis en œuvre peut être de type L3VPN, L2VPN ou circuit optique utilisant les technologies de multiplexage de longueurs d'ondes.

3.1.5 *Services de communication voix et image*

Le transport de la voix et de l'image est de plus en plus utilisé entre sites raccordés au réseau. RENATER met donc à disposition des services pour répondre aux usages des utilisateurs : téléphonie sur IP, visioconférence sur poste de travail, pont de visioconférence, etc.

ToIP (Telephony over IP) : ce service permet d'utiliser l'infrastructure RENATER pour établir des appels entre sites raccordés à RENATER. Des évolutions sont prévues en 2012 pour mutualiser les accès RTC des établissements au moyen de *trunks* SIP et ainsi réduire les coûts de téléphonie.

EVO (Enabling Virtual Organisations) est un service de visioconférence sur le poste de travail mais il est aussi possible d'accéder à une réunion EVO depuis un poste téléphonique ou un terminal dédié (de type H323). Le client EVO est une application JAVA ne nécessitant aucune installation et s'exécutant sur toutes les plate-formes. Il propose de nombreuses fonctionnalités telles que le partage d'écran, la messagerie instantanée ou l'enregistrement de sessions.

Visioconférence H323 – GDS (Global Dialing Scheme) : un service de routage d'appel mondial a été développé dans le monde éducation/recherche pour une mise en relation entre terminaux de visioconférence indépendamment de leur adresse IP. Pour sa communauté, RENATER assure la gestion du préfixe français (0033).

RMS – Remote Meeting System : ce service fournit des salles (virtuelles) de visioconférence H323 avec un mécanisme de réservation sur un pont mutualisé. Il est aussi accessible depuis des téléphones. Développé par le Centre de Calcul de l'IN2P3, ce service est en cours de reprise par RENATER et sera disponible pour l'ensemble de ses utilisateurs dès 2012.

3.1.6 Services de mobilité (eduroam/eduspot)

Le service eduroam ("Education Roaming") utilise une infrastructure sécurisée pour permettre un accès WIFI nomade au sein de la communauté Recherche et Enseignement aux niveaux national et international. L'identifiant et le mot de passe de l'utilisateur restent le même quel que soit son lieu de connexion. Des partenariats avec des opérateurs commerciaux afin d'étendre encore la couverture du service sont envisagés.

En s'appuyant sur un portail web dit captif et la fédération d'identité Éducation-Recherche, Eduspot est un autre service permettant le nomadisme des utilisateurs avec une sécurité intégrée moins complète mais aussi un déploiement très allégé.

3.2 Les services applicatifs

3.2.1 Antispam

Un service antispam est proposé par RENATER à l'ensemble des établissements connectés au réseau. Le filtrage des mails est réalisé par un relais de messagerie mutualisé intervenant en amont des serveurs de messagerie des sites. L'analyse anti-virus de ces messages peut être réalisée en option.

3.2.2 Fédération d'identité Éducation-Recherche

La fédération Éducation-Recherche est une infrastructure d'authentification nationale permettant à ses participants de sécuriser et de simplifier l'accès à des ressources Web, via les mécanismes de fédération d'identité. Elle permet aux utilisateurs de réduire le nombre de mots de passe à retenir, étend les bénéfices de Single Sign On jusqu'à des applications hébergées en dehors de leur institution et offre à ces dernières une meilleure maîtrise de la diffusion de données à caractère personnel.

3.2.3 Comptes Réseaux Universels (comptes CRU)

Dans le cadre de la Fédération Éducation-Recherche, les comptes CRU proposent un fournisseur d'identités aux utilisateurs n'en disposant pas dans leur organisme de rattachement. Les comptes CRU permettent notamment d'accéder, via un compte unifié, à de nombreux services proposés par RENATER.

3.2.4 Certificats électroniques

Dans le cadre de l'adhésion française au service européen TERENA Certificates Service (TCS), RENATER fournit à ses utilisateurs des certificats serveurs et des certificats de personnes. Les certificats serveurs sont reconnus par défaut dans les principaux navigateurs Internet et ne provoquent pas l'apparition de fenêtres d'avertissement finalement contre-productives en matière de sécurité. Les certificats de personnes permettent de signer des courriels ou de les chiffrer (sous réserve de mise en place par l'établissement d'un séquestre des clefs) et aussi de renforcer les dispositifs d'authentification.

3.2.5 Universalistes et outils collaboratifs

La plate-forme Universalistes propose un ensemble d'outils collaboratifs intégrés (listes de discussion, wiki, sondage, prise de rendez-vous) destiné à des communautés (enseignants, chercheurs, groupes de travail). Universalistes permet facilement à ces groupes de combiner des espaces privés et la publication de documents. Ce service est utilisé par 270 000 utilisateurs et 1000 groupes. Le serveur diffuse 1.3 million de mails par jour.

3.2.6 Logiciel Sympa

RENATER développe et distribue le logiciel libre Sympa qui est également le cœur du service Universalistes. Ce logiciel serveur de listes de diffusion est un outil majeur de l'internet, utilisé par plus de 10 000 sites à travers le monde, dont 95 % des établissements d'enseignement supérieur français. La communauté autour du logiciel Sympa est très active (NASA, Internet2, etc) et les évolutions du logiciel continuent.

3.2.7 Plate-forme SourceSup

SourceSup est une plate-forme web de gestion de projet (forge destinée aux établissements d'enseignement supérieur et aux organismes de recherche français). Le projet peut être diffusé publiquement ou bien être privé, il peut donc s'agir d'un projet inter-établissements ou bien un projet interne d'établissement. SourceSup héberge à ce jour 500 projets actifs et 1800 utilisateurs.

3.3 Les services de sécurité

3.3.1 Animation du réseau des RSSI

L'animation du réseau des RSSI consiste principalement à maintenir et animer 3 éléments :

- la liste RSSI ;
- l'intranet des RSSI ;
- l'intranet SSI juridique.

La liste RSSI est un canal de dialogue entre RSSI et de communication entre les services du HFDS et les RSSI de l'enseignement supérieur et de la recherche. Elle permet aussi de réagir sur des problèmes mêlant la SSI et ses aspects juridiques.

L'intranet est une zone réservée contenant les documents non publics à l'usage des RSSI exclusivement.

L'intranet juridique est un espace constitué des documents de veille juridique hebdomadaire composés par un cabinet spécialisé à l'usage de l'Éducation Nationale et de l'Enseignement Supérieur. Cet espace contient aussi une FAQ dédiée à la SSI composée de la partie publique des réponses de ce même cabinet au problèmes juridiques que connaissent les RSSI.

RENATER organise de plus tous les deux ans avec les services du HFDS les journées RSSI de l'enseignement supérieur et de la recherche qui permettent d'échanger sur l'actualité de la SSI.

3.3.2 Recommandations et bonnes pratiques en matière de SSI

À la fois à travers l'intranet des RSSI et des pages sécurité de RENATER, le GIP promeut les bonnes pratiques de la SSI. Ces pages ont pour vocation d'agrèger et de centraliser les documents permettant aux RSSI, administrateurs ou développeurs d'intégrer la sécurité dans leurs projets. Il s'agit par exemple de pointeurs sur des documents de l'ANSSI, des chartes ou des documents préconisant des principes de sécurisation de services (réseaux sans-fil ou annuaires par exemple). La réalisation d'un ensemble documentaire aidant à la rédaction d'une PSSI en est un autre exemple. Ce référentiel ayant pour vocation d'aider les établissements à intégrer la sécurité comme étant un processus permanent et nécessaire.

3.3.3 CERT RENATER (surveillance des flux/réactions en cas d'incident/traitement des requêtes)

En activité depuis 1995, le CERT RENATER a pour rôle d'assister les utilisateurs du réseau en matière de sécurité informatique, et notamment dans le domaine de la prévention, de la détection et de la résolution d'incidents de sécurité. Sa fonction première est d'être le point de contact, c'est-à-dire la structure que l'on appelle à l'aide et qui organise la réaction en cas d'incident. Cette structure permet de centraliser et de diffuser de l'information par des canaux sûrs. La diffusion de cette information se fait sous la forme de notes envoyées au correspondants sécurité des sites.

Le CERT RENATER fait office de point de contact pour l'ensemble de la communauté éducation-recherche française. Il permet l'acheminement rapide d'une communication vers les personnes appropriées sur les sites connectés au réseau RENATER.

Il peut également apporter aux correspondants des sites une aide à la résolution d'incident sous la forme de recommandations techniques ou non.

3.3.4 Administration de l'autorité de certification GRID2-FR

Les mécanismes de sécurité sur les grilles de calcul utilisent massivement l'authentification et le chiffrement à l'aide de certificats électroniques X509, que ce soit pour l'authentification des utilisateurs et des machines ou le chiffrement des communications à l'intérieur de la grille.

L'autorité de certification GRID2-FR a été créée pour répondre à ce besoin. Elle est administrée par le GIP RENATER, en collaboration avec le GIS France Grilles, dans le cadre d'une politique de certification, document qui définit les règles et procédures devant être appliquées pour la gestion des certificats.

4 Organisation pour la fourniture des services

Sous la direction de Patrick Donath, le GIP RENATER est organisé en trois directions :

- la Direction des affaires Administratives et Financières (DAF, responsable Sandra Cabaret) ;
- la Direction des Relations Extérieures (DRE, responsable Sabine Jaume) ;
- la Direction Technique (DT, responsable Laurent Gydé).

Dans le cadre de la fourniture des services aux utilisateurs, le volet contractuel mis en œuvre par la DRE et le volet technique est mis en œuvre par la DT.

4.1 Organisation contractuelle

Les utilisateurs de RENATER (ou les utilisateurs potentiels) contactent la DRE pour connaître les modalités d'accès au réseau et à ses services. Dans le cas des établissements sous tutelle d'un membre du GIP, la DRE assurera l'interface avec cette tutelle pour obtenir son agrément. Pour les établissements ne relevant pas d'un tutelle membre de RENATER, la DRE vérifiera l'adéquation de la demande avec la charte d'utilisation du réseau et proposera une convention financière.

Les services RENATER sont disponibles contractuellement grâce à l'agrément. Depuis janvier 2011, DRE et DT ont travaillé de concert à l'optimisation des procédures de raccordement au réseau RENATER et d'activation des services.

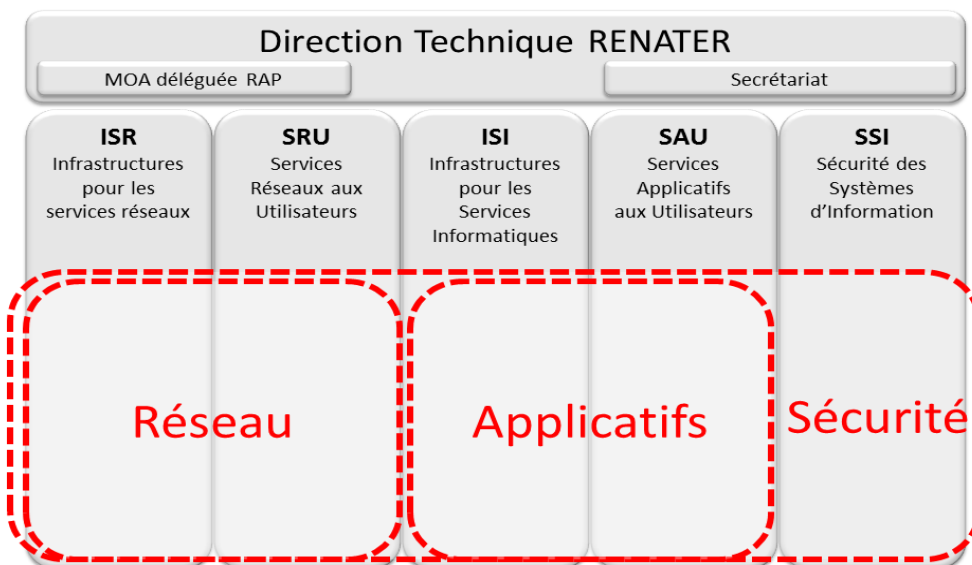
L'agrément est composé de 3 documents :

- la Convention d'Agrément qui décrit les conditions générales et particulières d'accès au réseau et services RENATER ;
- la Charte déontologique : charte de bon usage du réseau et déclaration du contact sécurité ;
- le feuillet « débit RENATER/Sites secondaires » : indique le débit RENATER et la liste des sites secondaires en cas d'agrément multi-sites.

Ainsi, la majorité des services est activable en renseignant l'interface de gestion des agréments¹. Pour d'autres (Universalistes, antispam, Certificats, fédération d'identité...), des documents complémentaires peuvent être demandés. Toute demande relative à l'agrément peut être adressée à l'adresse agrement@renater.fr. Il existe aussi des contacts pour chaque type de service, la liste est disponible sur la page <http://www.renater.fr/support>.

¹<https://saga.renater.fr>

4.2 Organisation technique



Pour prendre en compte les spécificités des différents segments de l'offre de services, et compte tenu de l'augmentation des missions et des effectifs (nouveaux entrants issus du CRU, du CORAP et de l'UREC), la Direction Technique du GIP RENATER a été réorganisée en juin 2011 en cinq pôles, dédiés aux services réseaux (un pôle infrastructures et un pôle services), aux services applicatifs (un pôle infrastructures et un pôle services) et à la sécurité qui est intégrée de façon transversale à l'ensemble de nos activités.

La direction technique de RENATER est aujourd'hui répartie sur quatre sites : Paris, Rennes, Grenoble et Montpellier. La plupart des équipes sont elles-mêmes sur deux sites ou plus. Pour pallier les inconvénients liés à l'éloignement géographique des équipes et des personnes, un VPN dédié au GIP a été déployé et différents outils de communication et de travail collaboratif sont déployés en interne :

- systèmes de visio-conférence de salle et de poste de travail ;
- téléphonie et audioconférence sur IP entre les sites ;
- messagerie collaborative et agendas partagés ;
- messagerie instantanée.

Le GIP RENATER est ainsi et pour lui-même un des premiers demandeurs sur l'ensemble de son portefeuille de services.

5 Conclusion

Après l'émergence en 2009 et 2010 de nouveaux services placés au dessus de la couche réseau (eduroam, Fédération d'identité, antispam), le GIP RENATER a mis en place un groupe de consultation sur les services (GCS) et a poursuivi l'orientation de son organisation interne vers les services aux utilisateurs. Ceux-ci sont ainsi placés au centre des processus de définition, d'élaboration et de production de l'offre RENATER.

L'équipe RENATER s'est vue renforcée avec des compétences issues de structures œuvrant déjà depuis de nombreuses années pour tout ou partie de la communauté Enseignement Recherche. La cohérence globale du portefeuille de services a été une priorité lors de cette intégration et la nouvelle organisation favorise la prise en compte de la sécurité à la fois pour les services et les infrastructures.

En plus des évolutions de l'offre RENATER évoquées dans cet article, la mise en place en 2012 d'un portail unifié pour l'ensemble du portefeuille de services a pour objectif de donner aux utilisateurs une vision consolidée et claire de l'ensemble des services auxquels ils ont accès.