RAPPORT N° 11
DU COORDINATEUR CONFIDENTIALITE

Article 17, alinéa 2, de l'arrêté du 21 mars 2002 relatif aux gestionnaires de réseaux et article 7, alinéa 2, de l'arrêté du 16 octobre 2003 relatif aux gestionnaires de réseaux gaziers

TABLE DES MATIERES

Chapitre I

Préambule

L'article 17 de l'arrêté du 21 mars 2002 relatif aux gestionnaires de réseaux stipule que : « *le gestionnaire de réseau veille à recueillir et à consigner les informations personnelles et commerciales dont il a connaissance dans l'exécution de ses tâches sous une forme et dans des conditions propres à en préserver la confidentialité. Il garantit la séparation systématique entre ces données et celles qui sont susceptibles de connaître une publicité.*

Le gestionnaire du réseau désigne une personne, indépendante des producteurs, fournisseurs aux clients éligibles et intermédiaires, spécialement chargée de la coordination des mesures adoptées en application du présent article. La CWAPE peut solliciter à tout moment de la personne ainsi désignée un rapport sur l'application de ces mesures. »

L'article 7 de l'arrêté du 16 octobre 2003 relatif aux gestionnaires de réseaux gaziers contient des dispositions identiques.

Par acte du 5 décembre 2013, la société ORES s.c.r.l. est devenue filiale d'ORES Assets, intercommunale constituée le 31 décembre 2013 suite à la fusion des GRD IDEG, IEH, IGH, INTEREST, INTERLUX, INTERMOSANE, SEDILEC et SIMOGEL (M.B. du 10 janvier 2014). Elle est chargée de la coordination des mesures adoptées en application des articles 17 et 7 précités.

Le présent rapport couvre les activités d'ORES Assets sur l'ensemble du territoire desservi, tant pour l'électricité que pour le gaz naturel. Il a pour objet d'exposer les mesures prises au cours de l'année 2014 pour répondre mieux encore à l'objectif de préserver la confidentialité des informations dont ORES a connaissance dans l'accomplissement des tâches qui lui sont confiées.

Chapitre II

ORES s.c.r.l. – Filiale d'ORES Assets en Wallonie – Comité d'Ethique

Comité d'Ethique

ORES s.c.r.l., filiale d'ORES Assets, s'est dotée de structures propres parmi lesquelles, conformément à l'article 16, § 1er, 4ème alinéa, du décret du 12 avril 2001 relatif à l'organisation du marché régional de l'électricité et à l'article 17, § 1er, 4ème alinéa, du décret du 19 décembre 2002 relatif à l'organisation du marché régional du gaz, outre le Conseil d'Administration, un Comité d'Ethique.

I. Le Comité d'Ethique en ORES

Le Comité d'Ethique est un Comité constitué au sein du Conseil d'Administration en application de l'article 14 des statuts.

La Charte de Gouvernement d'entreprise établit les principes applicables à ce Comité.

II. Mission du Comité d'Ethique

Le Comité d'Ethique est chargé de contrôler le respect, par le personnel, des règles relatives à la confidentialité des informations personnelles et commerciales.

Pour ce faire :

1. Le Comité d'Ethique bénéficie d'un accès illimité à tous les processus et à toutes les procédures mises en place ainsi qu'au personnel de la société.

2. Le Comité d'Ethique aura à sa disposition le contenu actualisé de tous les processus traitant des informations personnelles et commerciales.

3. Le Comité d'Ethique pourra entendre n'importe quel membre du personnel ayant accès à pareilles données.

III. Confidentialité des informations personnelles et commerciales

Sur base d'une lecture combinée des dispositions décrétales et du Règlement du Comité d'Ethique, les administrateurs, le personnel d'ORES et ses sous-traitants doivent respecter les règles relatives à la confidentialité des informations personnelles et commerciales. Tel que le précisent l'article 16 bis, § 1er, du décret électricité et l'article 17 bis, § 1er, du décret gaz, ces données personnelles et commerciales sont considérées comme relevant du secret professionnel et sont celles reprises aux articles 12, § 2, et 16, § 1er, du décret électricité et aux articles 13, § 2, et 17, § 1er, du décret gaz.

Les données personnelles et commerciales sont à ce titre confidentielles et relèvent du secret professionnel. L'article 16, § 1er, du décret électricité et l'article 17, § 1er, du décret gaz ne précisent pas exactement à qui sont dévolues les tâches stratégiques ou confidentielles. Il n'en demeure pas moins que le Comité d'Ethique doit reprendre à son compte les données reprises à l'article 16, § 1er, du décret électricité, et à l'article 17, § 1er, du décret gaz en ce qu'elles revêtent un caractère confidentiel. Le Comité d'Ethique est strictement chargé de contrôler le respect, par les administrateurs, personnel et sous-traitants d'ORES, des règles relatives à la confidentialité des données visées aux articles 12, § 2, et 16, § 1, du décret électricité et aux articles 13, § 2, et 17, § 1, du décret gaz.

Cette notion de « données » est à resituer dans le cadre des missions exercées par le Gestionnaire de Réseaux de Distribution et par sa filiale ORES, conformément aux articles 12 et 16 du décret électricité et aux articles 13 et 17 du décret gaz tels que repris ci-après.

Pour paraphraser l'article 12, § 1er, 4°, et § 1bis, du décret électricité et l'article 13, § 1er, 4°, du décret gaz, les données sont :

- personnelles : en ce qu'elles touchent directement à la personne physique ou morale ici considérées comme utilisateur de réseau ou catégories d'utilisateurs du réseau ;
- commerciales : en ce que l'utilisation des données relatives à cette personne afférentes à son alimentation ou sa consommation de gaz et de l'électricité pourrait donner un avantage concurrentiel à un opérateur censé ne pas les détenir ou autrement dit, il convient d'éviter toute « *discrimination (notamment) en faveur des associés du gestionnaire de réseau ainsi que des entreprises liées à ces associés ou au gestionnaire de réseau* » (article 12, § 1er, 4°, et § 1bis, du décret électricité et article 13, § 1er, 4°, du décret gaz).

Enfin, il convient de préciser que ces notions ne sont pas à confondre avec la notion de « secret des affaires » à laquelle le personnel d'ORES est tenu dans le cadre de l'examen des dossiers de marchés publics, notamment.

Le Comité d'Ethique examine depuis 2009, sur base des dispositions précitées, les processus ou procédures mis en place en ORES ou par les sous-traitants d'ORES établissant le respect des dispositions en matière de confidentialité des données.

Chapitre III

Les services Access&Transit et Relevé et Validation Comptage – Services internes à ORES

1. Description des activités

Les services Access&Transit et Relevé et Validation Comptage font partie du département Gestion du Marché & Clientèle. Ce département gère d'une part, tous les processus du marché libéralisé et d'autre part, les obligations de service public sociales.

Le service Access&Transit gère le registre d'accès. Le registre d'accès est la pièce maîtresse du marché libéralisé. Il s'agit de la base de données à partir de laquelle s'organisent les relations et les échanges entre les différents acteurs du marché et le GRD. C'est en fait l'instrument qui garantit la mise à jour et les flux d'informations. Chaque point d'accès (appelé aussi point de fourniture) y est répertorié via son code EAN. Derrière ce code, on retrouve principalement les données du client, celle de son fournisseur et quelques autres informations utiles. Couplé à IMDMS - la base de données répertoriant les consommations de chaque point de fourniture - le registre d'accès donne une image complète du marché.

Le service Relevé et Validation Comptage regroupe entre autres les releveurs et les valideurs. Leur rôle est de relever les données de consommation chez les clients pour tout le territoire couvert par ORES et de les valider, c'est-à-dire de vérifier si les relevés sont cohérents au regard des statistiques et historiques de consommation ou des critères climatiques. Le service gère à la fois la relève annuelle des compteurs des clients résidentiels et petits professionnels (une visite tous les deux ans et l'envoi d'une carte l'autre année), la relève mensuelle (une visite tous les mois) et la relève à distance à intervalles réguliers pour les gros consommateurs (quart-horaire pour l'électricité et horaire pour le gaz).

La gestion journalière des applications informatiques utilisées par les deux services susmentionnés - le registre d'accès pour Access&Transit et IMDMS pour le service Relevé et Validation Comptage – est confiée à Indexis, filiale d'ORES et EANDIS.

2. Mesures spécifiques adoptées au sein des services examinés

- **Service Access&Transit**

  L'infrastructure informatique est sécurisée et l'accès à l'application est individualisé et réservé aux membres de l'équipe Access&Transit. Toute nouvelle demande d'accès est soumise à l'approbation du cadre responsable du service.

  Les fournisseurs ont également accès à l'application mais chaque fournisseur ne peut disposer que des données des clients pour lesquels il a reçu une acceptation d'enregistrement sur le point d'accès de la part du registre d'accès. Les règles de sécurité et d'accès de l'application informatique gèrent cette mise à disposition limitée de l'information liée au point d'accès.

Outre cette sécurisation via l'application informatique, le service Access&Transit même ne communique des renseignements par mail ou par téléphone sur le point d'accès qu'au fournisseur reconnu sur ce point d'accès. Il va de même pour l'historique du point d'accès.

Si un fournisseur lance un scénario de marché drop ou pose d'un compteur à budget -ce qui sous-entend que le client a des difficultés de paiement-, un autre fournisseur qui lancerait un switch (changement de fournisseur) sur le point d'accès ne recevra pas comme message de retour qu'un drop ou une pose d'un compteur à budget sont en cours mais qu'un scénario de fin de contrat est en cours. De ce fait, le nouveau fournisseur ne pourra pas prendre connaissance des difficultés de paiement du client.

Access&Transit ne communique des renseignements par téléphone, par courrier ou par mail qu'au client (ou à une personne mandatée par ce dernier) qui se trouve sur le point d'accès et seulement durant la période d'occupation de ce client. Le client final n'a pas accès à l'application informatique même.

Une traçabilité est possible de toutes les transactions du marché ainsi que des envois de données. Une traçabilité est également possible des actions de chaque personne ayant accès à la base de données.

Les documents du service Access&Transit portent tous le logo de confidentialité. Les procédures et instructions du service sont uniquement accessibles par le service même.

- **Service Relevé et Validation Comptage**

L'infrastructure informatique est sécurisée et l'accès à l'application est individualisé et réservé aux membres du département Gestion du Marché et Clientèle. Toute nouvelle demande d'accès est soumise à l'approbation du cadre responsable du service. Le call center a un accès aux applications via une interface Web sécurisée par un mot de passe.

Les fournisseurs ont également accès à l'application via une interface web mais chaque fournisseur ne peut disposer que des consommations des clients pour lesquels il a reçu une acceptation d'enregistrement sur le point d'accès de la part du registre d'accès. Les règles de sécurité et d'accès de l'application informatique gèrent cette mise à disposition limitée de l'information liée aux consommations du point d'accès.

Un client qui souhaite connaître son historique de consommation le recevra sur l'adresse d'expédition du client fournie par le fournisseur. Il peut être envoyé à une autre personne ou à un fournisseur mais ceux-ci doivent avoir un mandat écrit et signé du client du point d'accès concerné.
Une traçabilité est possible de toutes les transactions du marché ainsi que des envois de données. Une traçabilité est également possible des actions de chaque personne ayant accès à la base de données.

Les PDA (*Personal Digital Assistant)* des agents releveurs qui permettent l'introduction de l'index sur place sont sécurisés par un mot de passe.

Chapitre IV

Le service de Sécurité Informatique d'ORES

1. Description des activités

Le service de sécurité Informatique d'ORES fait partie du département Informatique. Il est placé sous la responsabilité du Chef de Service responsable des Architectures et de la Sécurité Informatique.

La mission de la sécurité informatique ORES se résume en cinq types d'actions génériques. Elle consiste à:

- définir le périmètre et les vulnérabilités liés à l'usage des technologies de l'information et de la communication;
- garantir la confidentialité, l'intégrité et la disponibilité des actifs informatiques, ainsi que la protection de la vie privée;
- mettre en œuvre et valider les architectures, les mesures, les outils et les procédures de sécurité;
- optimiser la performance du système d'information en fonction du niveau de sécurité requis;
- assurer les conditions d'évolution du système d'information et de sa sécurité en respectant les contraintes légale, règlementaire et contractuelle.

L'efficacité de la sécurité d'un système d'information ne repose pas uniquement sur les outils de sécurité, mais également sur une stratégie, une organisation et des procédures cohérentes. Cela nécessite une structure de gestion adéquate dont la mission est de gérer, mettre en place, valider, contrôler et faire comprendre à l'ensemble des acteurs de l'entreprise l'importance de la sécurité. Cette structure a été mise en place en 2011 chez ORES.

2. Mesures et plans d'actions

Le Service Informatique d'ORES a établi un rapport complet de l'activité sécurité Informatique ORES 2014 : « Rapport annuel du Comité de Sécurité : Décembre 2014 ».

Le programme de sécurité pour l'année 2014 a comporté les actions suivantes :

- Finalisation du projet d'implémentation de SAP IDM pour les environnements SAP.
- Extension de l'outil SAP IDM pour les environnements Windows et certaines applications basées sur des bases de données ORACLE : Strucom et Netgis.
- Implémentation d'un outil de gestion des risques IT et des risques Scada.
- Analyse de l'existant Smart Grid/Smart Meter du point de vue de la sécurité IT.
- Implémentation du SSO (Single Sign On) pour les environnements SAP.
- Participation à la rédaction des cahiers des charges MDM Release 2 et GIS/GIR.
- Participation à la validation des offres CMS Atrias.
- Réalisation de plusieurs tests de sécurité : Cronos, Scada, Smart Meter et MDM Release 1.

- Réalisation d'une série de tests afin de suivre et mesurer le respect de la politique de Sécurité Informatique d'ORES.
- Définition d'un processus et d'une structure organisationnelle pour la gestion des accès.
- Définition et mise en œuvre d'une politique de sécurité concernant l'utilisation de l'Internet et des réseaux sociaux (collaboration avec RH).

3. Réalisations 2014

- Implémentation SAP IDM

    - solution SAP ECC6 (UNIWALL)
        - environnement de production (WP1) ;
        - environnement d'acceptance (WA2) ;
        - environnement de développement (WD2) ;
        - environnement de test de clôture comptable (WP1S) ;
    - solution SAP PPM (Project & Portfolio Management) :
        - environnement de production (WP8) actuellement utilisé dans le cadre du projet Cronos (*);
        - (*) Projet Cronos : cette application remplace l'application Trace. Elle s'appuie sur les technologies SAP et Microsoft SharePoint dont la gestion des autorisations est basée sur l'Active Directory de Microsoft ;
    - solution pour les applications liées à l'Active Directory
        - solution Cronos
            - environnement de production ;
        - solution Mercure
            - environnement d'acceptance ;

    - mise à disposition d'un site Web permettant aux personnes autorisées d'assignation manuelle d'un métier dans SAP IDM ;

- Revue complète des accès sur les différents types d'équipements (outillage, charroi, télécom,…)

  Toutes les personnes qui avaient accès à la gestion d'un équipement dans SAP obtenaient l'accès à tous les types d'équipements y compris les équipements dits sensibles.
  Une restriction d'accès a été appliquée à différents documents et types d'avis SAP.
  Le système SAP ne permettait pas avec une version standard de gérer des autorisations par catégories d'équipements.
  Un développement spécifique a été réalisé afin de sécuriser la gestion des accès par type d'équipements et par métier.

- Intégration de nouveaux métiers ORES dans SAP

  D'une part, plusieurs métiers d'ORES n'ont pas besoin d'accéder à SAP et, d'autre part, l'intégration de nouveaux logiciels dans SAP a requis de mettre à jour l'inventaire des métiers qui doivent accéder à SAP.

- Sécurisation et gestion des accès via l'Active Directory dans l'environnement Windows

  L'accès aux applications d'ORES était géré dans l'Active Directory de GDF Suez.
  Pour plus d'autonomie et afin de faciliter la gestion des accès, un système dédicacé à ORES a été mis en place.

- SAP Single Sign-On (SSO).

  ORES a acquis le logiciel SAP Secure Logon Client qui permet d'utiliser le UserID et le mot de passe de Windows pour s'identifier sur tous les environnements SAP (standard Kerberos) en dehors de l'environnement SAP ECC6 de production (UNIWALL) planifié pour 2015.
  Cela permet d'une part, de faciliter les connexions puisque seul le mot de passe Windows doit être connu et, d'autre part, d'augmenter la sécurité.

- Gestion globale des risques de sécurité

  L'évolution de la sécurité IT est de passer au management par les risques via la gestion des risques, la définition d'un DRP (Disaster Recovery Plan) et l'établissement d'un BCP (Business Continuity Plan).
  La première étape de la mise en place d'une gestion de la sécurité par les risques est d'avoir une gestion des risques efficace en couvrant aussi bien la partie Informatique de gestion que la partie Smart Grid et Smart Meter.

- Définition d'une architecture sécurisée pour l'AMI

  L'AMI (Advanced Metering Infrastructure) est la passerelle entre le compteur Smart Meter et la solution MDM (Metering Data Management). Il est situé à la frontière entre le domaine des Smart Meters et le domaine Informatique d'ORES. Du point de vue de la sécurité, l'AMI est un point critique car une intrusion via les Smart Meters permettrait d'atteindre l'environnement informatique d'ORES.
  La sécurité IT a défini une architecture sécurisée (DMZ, Firewalls) pour la mise en place de la solution AMI en l'isolant de l'environnement informatique afin d'éviter toutes les intrusions sur les serveurs informatiques d'ORES.

- Les accès à Internet

  La politique d'accès à Internet était basée sur une autorisation par rapport à un site web. Cette politique n'était pas en adéquation avec les besoins du business (rapidité et flexibilité).
  ORES a basé les autorisations d'accès sur des catégories de sites web, plutôt que sur un site web.
  Ceci a permis de :
    - faciliter la gestion des accès au niveau opérationnel IT ;
    - augmenter la flexibilité vis-à-vis du business ;
    - améliorer le contrôle de la sécurité : l'autorisation d'accès pour une catégorie de sites web est discutée en Comité de Sécurité IT.

- Définition de plan d'actions et de stratégie pour la période 2014 – 2018

    - Stratégie 2014 – 2018 de la sécurité IT ;
    - Plan 2015 – 2018 pour la sécurité Smart Meter ;
    - Plan 2015 – 2018 pour la sécurité Smart Grid.

4. Changements majeurs en 2014

- A l'aube du Smart Meter et du Smart Grid, ORES a pris conscience des besoins d'intégrité et de confidentialité dans la manipulation des informations transportées au sein de ces deux domaines ainsi que des risques d'attaques potentielles.
- ORES a confié cette tâche à la sécurité IT afin qu'elle mette en place des dispositifs pour garantir la protection des données échangées au niveau du Smart Meter et du Smart Grid.
- Afin de définir les actions à mettre en place pour la sécurisation de l'environnement Smart Grid, un bilan de l'existant a été fait. Les résultats de l'audit de sécurité ont permis de définir un plan 2014-2018 de sécurisation de l'environnement Smart Grid.
- La sécurité IT a pris en charge la sécurisation du futur environnement Smart Meter. Un test de vulnérabilité de la solution compteur/concentrateur PLC-3G a été effectué afin d'évaluer le niveau de sécurité du protocole PLC-3G et de définir les critères de sécurité à inclure dans le futur cahier des charges Smart Meter.

5. Objectifs 2015

- Déploiement de la gestion des risques IT
- Implémentation de SAP IDM pour les applications qui sont dans la base de données ORACLE : Netgis, Proxxx
- Implémentation de SAP IDM pour les applications SAP : Odicea, PPM
- Implémentation de SAP IDM pour l'environnement Mercure production
- Implémentation du SSO pour l'environnement SAP ECC de production (UNIWALL)
- Implémentation de la solution Citicus pour la gestion des risques
- Inventaire et prioritisation des assets IT
- Déploiement de sondes de sécurité au niveau du projet RFP Réseau
- Inventaires DRP et BCP
- Demande d'autorisation auprès du FEDICT et mise en place d'une fédération d'authentification pour les futures solutions extranet d'ORES (au standard SAML 2.0)
- Exécution du plan d'actions 2015 issu de l'audit des accès IT 2014
- Participation à l'écriture du cahier des Smart Meters pour les aspects sécurité : PKI, SOC, SIEM
- Etude de la solution PKI pour le Smart Meter
- Mise en place de « QuickWin » de sécurité pour le Smart Grid
- Ecriture de la politique de sécurité Smart Grid.

Chapitre V

N-ALLO

En 2010, N-Allo a fait évoluer l'environnement de travail des collaborateurs de façon assez importante avec l'introduction de la Coupole en remplacement de Vantive.
La Coupole doit être vue comme une application assurant un certain niveau de convergence entre les différentes applications sous jacentes au sein desquelles les opérateurs sont appelés à travailler.
En 2011, l'environnement de travail du personnel de N-Allo traitant les interactions pour ORES n'a pas été significativement modifié.
Mais en 2012, la mise à disposition par ORES d'un certain nombre de web services permettant un dialogue plus facile avec les applications de gestion (SAP ISU, SAP PROCLI, CTH, ICCWeb…) a permis de mettre en place les premières fondations d'une architecture SOA (Architecture Orientée Service).
En 2013, deux modifications ont été apportées au paysage applicatif d'ORES :

- *D'une part, l'extension de l'offre en terme de web services a permis d'enrichir le travail au sein de la coupole ;*
- *D'autre part, une application pilote 'Portail ORES' a été mise en œuvre et est actuellement en cours d'évaluation au sein d'un Back Office d'ORES : ce portail offre aux collaborateurs d'ORES le même environnement applicatif que pour les collaborateurs de la première ligne mais avec des fonctionnalités dédicacées ainsi qu'un transfert du contexte de l'appel lorsqu'un client est transféré de la première ligne vers les Back Offices.*

2014 a vu deux évolutions importantes :

- *La première concerne l'ensemble du périmètre N-Allo : tous les sites opérationnels de N-Allo sont maintenant connectés tant pour les données que pour la voie à un IP backbone supporté par Telenet. En d'autres termes, en lieu et place d'une connectivité point à point entre les différents sites, ces sites sont tous connectés sur un réseau virtuel porté par Telenet ;*
- *La seconde est propre à l'environnement d'ORES et elle est particulièrement importante dans le contexte de la sécurisation des accès et du contrôle de ceux-ci vers les applications contenant des données privées de l'organisation. L'accès vers ces applications est désormais géré au sein de l'Active Directory d'ORES et attribué à l'agent dans des conditions de contrôle plus strictes. Pour plus de détails quant à cette solution, voir la partie infra relative à la Coupole.*

Enfin, dans le cadre de la préparation aux éventuels plans de délestage, N-Allo a réalisé avec succès cet automne une campagne exceptionnelle de test des infrastructures, des procédures et des systèmes pour s'assurer de la continuité du service dans des conditions d'urgence.

○ UN MODELE PARTAGE : UN DEFI

En matière de technologie, les principes fondamentaux d'un contact center peuvent être à certains égards considérés comme antagonistes.

Il s'agit en effet et dans le même temps :

- de mutualiser certaines infrastructures qui sont partagées entre un nombre important de clients : en regard des coûts

associés à cette technologie mais aussi à sa complexité, la mutualisation est un objectif en tant que tel ;

- d'assurer dans le même temps l'indépendance nécessaire entre le traitement et les données associées à chacun de ces clients.

La rencontre de ces deux objectifs est donc un souci constant pour le management du Contact Center et se traduit par la mise en œuvre de solutions propres, d'infrastructures spécifiques.

○ LES ELEMENTS CONSTITUTIFS D'UN CONTACT CENTER

La Plateforme de communication

La plateforme de communication englobe l'ensemble des moyens qui sont mis en œuvre pour assurer les traitements en amont de la distribution de tous les types d'interactions ([1]) pour son traitement : mise en attente et diffusion de message (pour les appels), routage et distribution (pour toutes les interactions),…

Les moyens mis en œuvre pour ce faire sont :

- les lignes téléphoniques qui apportent les appels au sein de l'organisation pour les interactions téléphoniques ;
- le lien IP qui apporte au sein de l'organisation les autres types d'interactions ;
- le central téléphonique qui assure tous les traitements sur ces appels ;
- les autres serveurs qui assurent les traitements sur les autres interactions : serveur mail, serveur documentaire,...
- les applications en marge de ces applications assurant le reporting et le monitoring de chacun de ces canaux de communication.

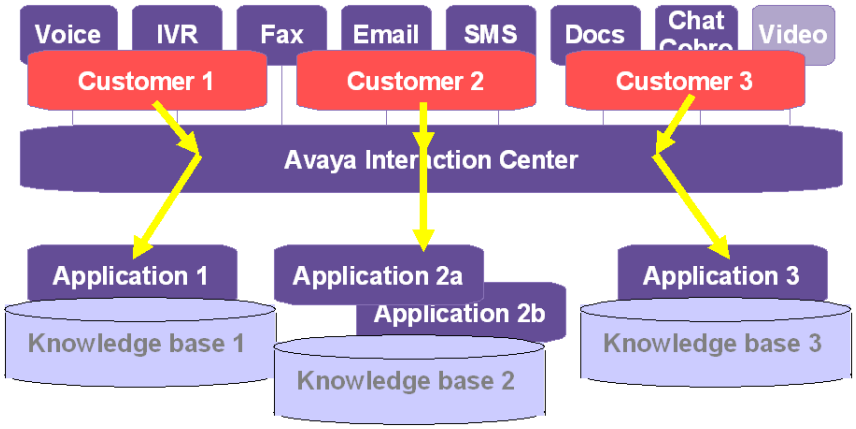
AIC : Avaya Interaction Center

AIC est un ensemble logiciel qui permet d'interfacer les différents canaux de communication avec les applications contenant des données (CRM). Chez N-Allo, AIC est particulièrement utilisé pour les fonctions suivantes :

- reconnaissance de l'émetteur de l'interaction : sur base de son numéro de téléphone pour un appel téléphonique, sur base de son adresse mail pour un mail, sur base de son identification pour une interaction Web,... Depuis le 15 octobre 2012, l'IVR est également utilisé afin de capturer l'identification du client ;
- transfert de l'interaction vers la seconde ligne ou vers les services spécialisés des donneurs d'ordre ;

[1] Il y a lieu en effet de ne plus considérer que les interactions téléphoniques. L'évolution des modes de communication amène effectivement N-Allo à traiter également les mails, les SMS et bientôt les interactions supportées sur le web : chat, co-browsing,...

- ouverture automatique de l'application permettant de traiter l'interaction en fonction du canal utilisé et de l'identification de l'émetteur de l'interaction.



AIC est en fait une extension de ce que l'on appelait le CTI (Computer-Telephony Integration), mais celui-ci ne s'appliquait qu'aux interactions de type téléphonique.

AIC est un logiciel opérationnel qui ne contient aucune donnée sensible : il se limite à référencer chacune des interactions (un appel, un mail,…) et son 'histoire' au sein de l'organisation (ligne d'entrée, routage appliqué, opérateur qui a assuré le traitement, transfert éventuel,…). Pour toute donnée propre à un client, il s'adresse aux systèmes d'information des différents donneurs d'ordre.

Le CRM

Le CRM est l'application centrale du Contact Center. Il est l'espace principal de travail pour les opérateurs. C'est là que l'opérateur reçoit et ensuite traite les interactions.

Pour ce faire, il dispose de trois grands types de données au sein du CRM :

- toutes les données permettant d'identifier le client si cette identification n'a pu se faire en amont dans le traitement auquel cas cette fonctionnalité est automatisée ([2]) ;
- les cases (tickets) associées à ce client, une fois qu'il est identifié ;
- les processus de travail qui permettent de traiter les interactions avec les clients : il s'agit là d'un catalogue de procédures propres à chacun des donneurs d'ordre et qui sont mises à la disposition des opérateurs pour assurer dans les meilleures conditions de qualité et de traçabilité le traitement des interactions. Ces processus sont de plus en plus

[2] Fonction Screen Pop Up qui assure l'ouverture automatique du dossier du client sur base d'informations collectées préalablement.

accompagnés d'informations complémentaires dont les opérateurs peuvent avoir besoin dans le traitement.

Deux types d'application CRM existent au sein de N-Allo :

- les applications des donneurs d'ordre : de plus en plus de donneurs d'ordre disposent de leur propre application CRM ;
- une application CRM construite et maintenue par N-Allo : ce secteur connaît un développement particulièrement important tant la qualité et la vitesse de traitement des interactions par les opérateurs est fonction de la qualité, de la richesse et de la convivialité de cette solution. N-Allo a très largement investi dans ce domaine avec le développement de ce que l'on appelle de façon générale le UDA (Unique Desktop Application), et en particulier pour ORES, la Coupole. Les principes de ce type d'application sont les suivants :
  - une grande convivialité ;
  - une interface unique qui pilote toutes les autres applications de gestion ;
  - la volonté de plonger l'opérateur dans le contexte du client dès que l'interaction est proposée : au lieu d'attendre de l'opérateur qu'il parcoure différents menus dans les différentes applications de gestion afin de pouvoir répondre au client, c'est l'application qui va faire ce travail de façon automatisée et qui va de la sorte proposer à l'opérateur l'information nécessaire à la compréhension de la problématique de l'interlocuteur, voire même la réponse à sa question.

Les applications clients

Pour certaines procédures de travail, l'opérateur peut être appelé à consulter ou à effectuer des mutations dans les applications des donneurs d'ordre. Ces applications sont propres à chacun des donneurs d'ordre de N-Allo. L'accès à ces différentes applications est géré par une 'password policy' et est défini avec chacun des donneurs d'ordre.

Le reporting/monitoring

Le reporting est l'ensemble des moyens qui permettent de mesurer l'activité réalisée au sein du Contact Center. Le monitoring permet de remonter les mêmes informations mais en temps réel afin de pouvoir intervenir directement sur les opérations.

Le reporting et le monitoring sont réalisés principalement sur les informations collectées au sein de l'AIC : on y dispose là de toutes les informations quantitatives relativement :

- à l'activité sur chacun des points d'entrée pour les différents types d'interaction : les points d'entrée sont propres à chacun

des donneurs d'ordre. Il s'agit d'un numéro de téléphone, d'une adresse électronique, d'un numéro de SMS,...

- à l'activité des opérateurs ;
- à la durée de traitement des interactions.

Les réseaux

L'ensemble des systèmes est relié par des réseaux hybrides. N-Allo ayant migré l'ensemble de sa technologie vers l'IP, la totalité des connections sont des liens IP. Ces réseaux sont particulièrement importants dans l'organisation N-Allo eu égard à sa structure sur 6 sites et au nombre de ses clients. N-Allo a également une connectivité importante avec plusieurs donneurs d'ordre extérieur à l'organisation.

LA MISE EN ŒUVRE AU SEIN DE N-ALLO

○ LE MODELE

De par son organisation, son architecture et sa gestion, l'ensemble de la plateforme de N-Allo est mis à la disposition des différents sites opérationnels et des différents donneurs d'ordre selon un modèle que l'on connaît aujourd'hui sous le nom de SaaS (Software as a Service). Les éléments actifs qui sont décrits ci-dessous sont distribués de façon transparente sur le réseau interne de l'organisation et sont intégrés de façon à offrir des services de façon tout à fait distincte aux différents utilisateurs sur les différents sites de N-Allo ou de donneurs d'ordre externes.

L'évolution du marché vers ce type de modèle est une réalité mais est également importante pour N-Allo : en effet, de façon presque systématique maintenant, les solutions logicielles sont construites pour permettre le fonctionnement dans ce type d'architecture ; elles offrent donc les mécanismes de cloisonnement entre les activités supportées.

○ LA PLATEFORME DE COMMUNICATION

La plateforme de communication en tant que telle est une infrastructure totalement partagée, en ce sens qu'elle est unique pour l'ensemble de l'organisation et de ses clients.

Cependant au sein de celle-ci, ont été définis les cloisonnements suivants :

- Pour chaque donneur d'ordre de N-Allo, un cluster étanche est défini ; on retrouve au sein de ces clusters les différents points d'entrée de chacun des donneurs d'ordre (DDI : ce sont les numéros d'entrée propres à chacun des donneurs d'ordre, les 'functional mailboxes',...) ;
- Pour chacun de ces points d'entrée, des règles de routage propres ont été définies : par règle de routage propre, il faut

entendre que chaque interaction reste dans le cluster au sein duquel elle est rentrée.

L'isolement des activités les unes par rapport aux autres fait régulièrement l'objet de tests. De plus en plus de configurations assurent cette exclusion.

De plus, afin d'assurer l'isolement des activités de chacun des donneurs d'ordre, ceux-ci disposent de leurs propres PRAs (bouquet de lignes d'entrée). Il n'y a plus, comme c'était le cas auparavant, d'effet d'échelle entre les différentes activités.

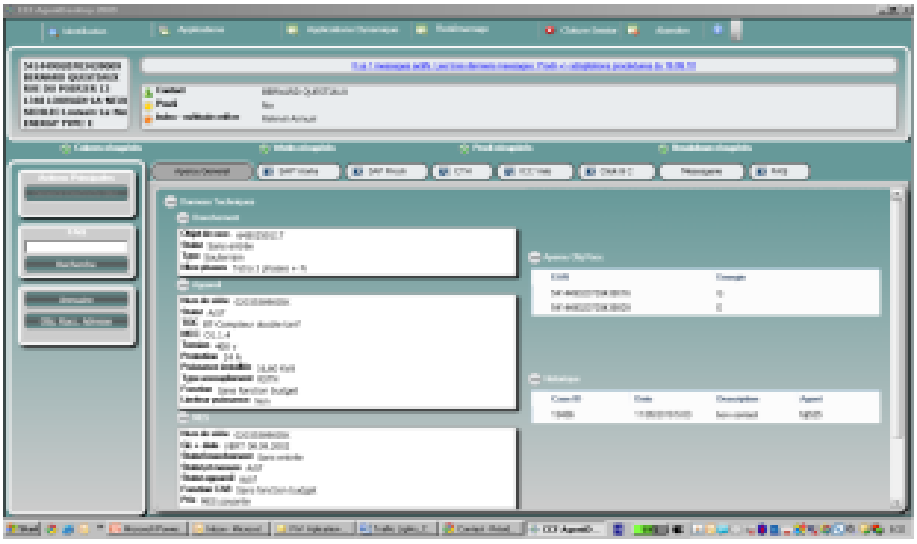
○ AIC

L'AIC hérite du cloisonnement réalisé au niveau de la plateforme de communication : sa fonction se limite à la distribution des interactions reçues sur les différents canaux aux opérateurs disposant des compétences propres pour les traiter.

○ LE CRM – LA COUPOLE

ORES COUPOLE @ N-Allo

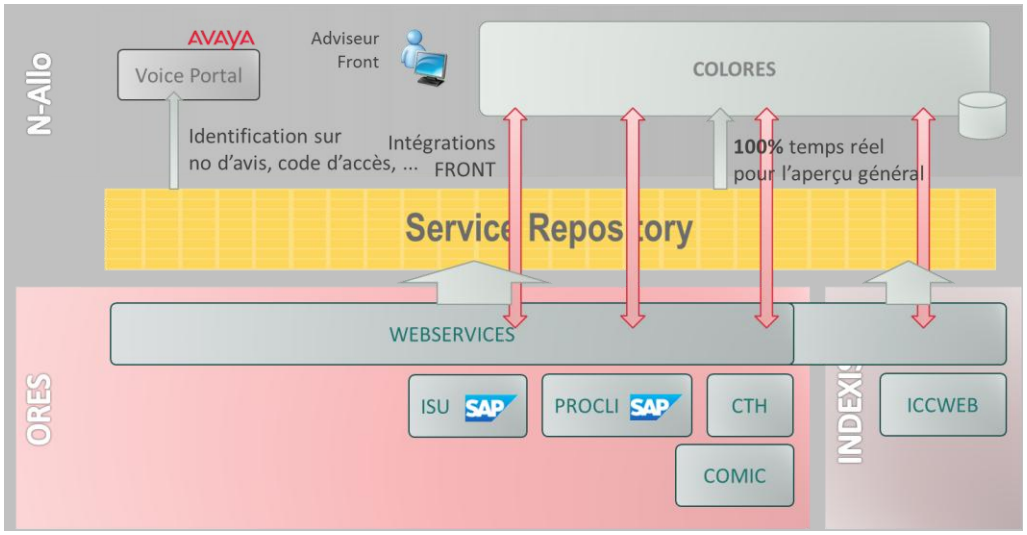
Avec le développement de l'application Colores, les collaborateurs de N-Allo traitant les interactions d'ORES disposent de leur environnement propre totalement séparé de tout autre environnement opérationnel.



En d'autres termes, c'est exclusivement les collaborateurs travaillant pour ORES qui ont accès à cette application.

Techniquement, les données sont dans une base indépendante totalement et physiquement séparée de toute autre donnée dans l'environnement N-Allo.

L'architecture sous-jacente à cette application a en 2012 fondamentalement évolué. En effet, grâce à la publication par ORES de web services (à ce stade, avec un périmètre fonctionnel réduit), N-Allo a mis en place un Service Repository permettant d'assurer des services à valeur ajoutée sur les IVR ainsi qu'au sein de la Coupole. Ces services ont été repris dans le cadre du projet Accessibilité en partenariat avec ORES et portent principalement sur l'identification du client ainsi que la qualification de la raison d'appels.



En matière de droits d'accès à l'application, ceux-ci ne sont attribués qu'à des collaborateurs travaillant pour le client ORES. Ces droits sont exclusifs et gérés au sein de l'Active Directory de N-Allo. Une réplication de ce Directory est faite vers ORES qui se base sur ces données afin de permettre l'accès à l'environnement SAP. Cette mécanique de contrôle d'accès – SSO : Single Sign On - portée par un modèle de SAP permet un contrôle centralisé par ORES des personnes ayant accès aux applications, de leur niveau d'autonomie et de leur utilisation de l'application.

Quant à l'accès aux services web publiés par ORES, ils sont strictement protégés par l'utilisation du protocole https ainsi que l'échange de certificats.

○ LES APPLICATIONS CLIENTS

Les opérateurs qui doivent accéder pour consulter ou effectuer des mutations aux applications des donneurs d'ordre voient également ces applications comme des ensemble disjoints. Ceci au travers des mécanismes suivants :

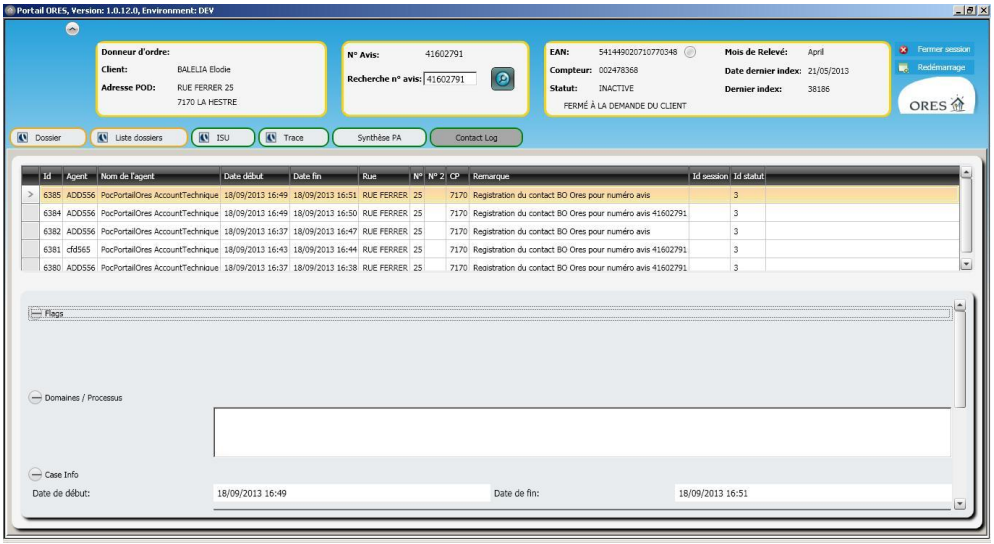
- L'ouverture des applications se fait de façon totalement automatisée en fonction du profil de l'opérateur, et donc en fonction du client pour lequel il travaille ;
- L'accès à ces applications requiert une identification personnelle (profil) qui est propre pour chacun des donneurs d'ordre ;

- Depuis janvier 2009, une application de Single Log On assure également que seules les applications réservées à un certain profil puissent être ouvertes.

Depuis la libéralisation du marché de l'énergie en Wallonie et plus encore depuis la migration vers l'environnement Full ISU Lopex, les opérateurs disposent maintenant pour chacun des donneurs d'ordre d'un seul environnement client dont les accès sont contrôlés par les logins et passwords.

○ LE CRM – PORTAIL BO

Cette nouvelle application a pour but d'offrir aux collaborateurs des Back Offices d'ORES un environnement de travail portant la même philosophie que la Coupole, mais avec des fonctionnalités propres à l'activité dans les Back Offices ainsi que le transfert du contexte lors du transfert de l'appel – ceci permet de ne pas devoir refaire une identification du client lorsque celui-ci est transféré vers le Back Office en raison de l'autonomie de N-Allo.



Les droits d'accès à cette application sont strictement limités aux personnes enregistrées au sein de l'application et dans un groupe spécial de l'Active Directory – l'Active Directory est l'environnement de gestion des utilisateurs et de leurs droits propres sur les applications.

Ce projet est à ce stade en mode 'pilote' en cours d'évaluation auprès d'une population limitée de collaborateurs dans les Back Offices.

○ LE REPORTING ET LE MONITORING

Ces deux activités essentielles pour un contact center se font sur des bases qui garantissent la totale indépendance entre les différents donneurs d'ordre. Il s'agit en effet :

1. des points d'entrée (lignes d'appels, mailboxes,...) : elles sont propres à chacun des donneurs d'ordre ;

2. des skills (compétences) des opérateurs : elles sont, pour ce qui est des activités Fournisseur et Gestionnaire de Réseaux, incompatibles.

○ LES RESEAUX

Prenant en compte que l'ensemble des applications sont extrêmement critiques en matière de sécurité, de disponibilité et de continuité, les différents réseaux sont extrêmement sécurisés. En particulier, les mesures suivantes sont mises en œuvre :

- pas d'entrée du monde extérieur en dehors d'un protocole de sécurisation extrêmement sévère supporté par des firewalls ;
- pas d'accès au réseau sans une identification préalable et personnelle de l'opérateur ;
- monitoring permanent de l'activité sur le réseau ;
- tracing de l'ensemble des actions réalisées au sein des différents systèmes.

En matière de sécurisation et d'isolement, N-Allo a mis en oeuvre une structure en subnetworks, chacun des donneurs d'ordre se trouvant ainsi isolé sur son subnetwork propre. Cette nouvelle structure du réseau est en cours de mise en œuvre et est opérationnelle depuis juillet 2007.

Il faut noter par ailleurs que ces mesures de sécurisation font régulièrement l'objet d'audit de la part de certains des donneurs d'ordre qui se doivent de préserver d'une part l'accès à leurs systèmes d'information et d'autre part la confidentialité des informations disponibles chez N-Allo.

○ SYNTHESE

En mettant ces différents moyens en œuvre, N-Allo peut ainsi garantir une totale étanchéité entre les activités liées aux différents donneurs d'ordre. Cette étanchéité est assurée tout au long du traitement comme suit :

- Au sein de la plateforme de communication : ce sont des numéros propres, des mailboxes,... pour chacun des donneurs d'ordre ;
- A chacun de ces points d'entrée sont associées des règles de routage qui amènent les appels vers des opérateurs propres à chacun des donneurs d'ordre ;
- Ceux-ci identifient le client :
  - soit au sein d'application qui sont spécifiques pour chacun des donneurs d'ordre et qui plongent dans des bases de données distinctes hébergées sur des machines distinctes ;
  - soit directement dans l'application propre au donneur d'ordre ;

- Les processus de traitement des interactions sont propres à chacun des donneurs d'ordre et ils sont accessibles dans les écrans qui sont eux-mêmes spécifiques ;
- Le stockage des interactions se fait dans les environnements propres ;
- Tout le suivi de l'activité se fait sur base de critères qui sont également propres à chaque donneurs d'ordre (ligne, compétences,…) ;
- Le réseau en œuvre au sein de l'organisation est particulièrement sécurisé afin d'empêcher toute intrusion externe ou toute indiscrétion par rapport aux données.

Remarque : la notion d'incompatibilité entre les skills des opérateurs est discutée avec chacun des donneurs d'ordre et tient donc compte de toute exigence particulière.

Ainsi dans le monde libéralisé, il y a stricte incompatibilité entre les opérateurs travaillant pour les activités du Gestionnaire de Réseau et les activités du Fournisseur tandis que des effets d'échelle entre les activités Fournisseur et celles d'autres donneurs d'ordre n'ayant rien à voir avec les marchés de l'énergie sont mis en oeuvre afin d'optimiser la capacité de production de l'organisation.

ORGANISATION OPERATIONNELLE

○ ORGANISATION GENERALE

Les activités gérées par N-Allo au nom du GRD et d'ORES sont organisées sous la direction du Responsable Opérationnel en charge des clients traités sur les sites de Gosselies/Eupen.

N-Allo est appelé pour nombre de ses donneurs d'ordre à mettre en œuvre une gestion étanche dans le traitement de leur clientèle respective. Ces « Chinese walls » font par ailleurs l'objet d'audit (par exemple pour Affineon, dans le secteur de l'assurance, NIBC dans le secteur de la finance,…).

Cette organisation opérationnelle est le prolongement de l'infrastructure technique et permet d'assurer à ce niveau également la totale indépendance entre les différentes activités.

○ ORGANISATION PHYSIQUE

En fonction des besoins propres, une isolation physique peut également être assurée entre certaines activités. Les mesures en œuvre chez N-Allo sont par exemple les suivantes :

- Certains donneurs d'ordre disposent d'un local propre (avec ou sans contrôle d'accès) ;

- Certains donneurs d'ordre sont isolés sur des étages distincts ;
- Enfin, pour certains donneurs d'ordre seule une séparation physique simple est mise en œuvre (ilots propres).

Chapitre VI

INDEXIS

Les Gestionnaires de Réseau de Distribution mixtes Flandre / Wallonie ont confié à Indexis la gestion journalière de l'application informatique et de la datawarehouse liées à leurs Registres d'Accès ainsi que la datawarehouse des données de l'application IMDMS de gestion des comptages d'énergie.

La gouvernance, l'organisation et les accès aux systèmes en Indexis ont pu être amenés à un niveau de maturité supérieure suite à un audit délivré fin 2011.
Des nouveaux objectifs ont été fixés dans chacun de ces domaines conformément aux recommandations émises dans l'audit. Par exemple, l'utilisation d'un password management tool pour chaque collaborateur, l'implémentation de « password policies » dans les applications, ou encore la rationalisation des demandes d'accès aux systèmes.

En 2012, tous les domaines (il y en a 11) de la norme ISO 27002 touchant la sécurité de l'information furent abordés. Des politiques ont été définies pour chacun de ces domaines et des initiatives furent prises pour répondre aux vulnérabilités les plus urgentes.
Une banque de données centrale permet à Indexis de gérer d'une façon concluante les droits d'accès aux systèmes et applications. Des procédures pour l'obtention et le suivi des droits d'accès ont été mises en place. D'autres initiatives telles que l'encryptage des données et la classification des documents sont en cours.
En 2012, un audit a permis de mettre en évidence une amélioration significative de la maturité d'Indexis en matière de sécurité de l'information. Les recommandations ont confirmé les projets qui avaient été proposés au Conseil d'Administration.

En 2013, Indexis s'est concentré sur les dangers d'intrusion externe.
En installant une protection « Web Application Firewall », il est possible de détecter des flux de données anormaux vers les applications WEB-internet, comme p.e. des instructions de type SQL qui visent à bloquer les banques des données. En outre, l'implémentation des « password policies » a été imposée.

Indexis a convenu avec ses fournisseurs de service IT d'installer rigoureusement et immédiatement chaque patch de sécurité disponible.

En 2014, IPS (Intrusion Protection System) a été mis en service. Ce système permet à Indexis de détecter et arrêter tout trafic de données anormal ou inconnu avec le monde extérieur et entre les systèmes. Avec la mise en œuvre du projet de réorganisation du VLAN (Virtual Local Area Network), les systèmes et le réseau des données ont été réorganisés en plusieurs couches, chaque couche avec son contenu et sa sécurité spécifique.

Des mesures ont également été prises pour la protection interne. En 2014, le NAC (Network Access Control) a été mis en service. Celui-ci veille à ce qu'uniquement des dispositifs répondant aux dernières mises à jour des logiciels installés et détecteurs de virus puissent être connectés au réseau d'Indexis. La politique relative aux mots de passe a été implémentée pour toutes les applications et avec l'introduction de l'impression sécurisée, les documents sont maintenant imprimés de

façon sécurisée en utilisant un code personnel. Grâce à la politique de rangement du bureau, Indexis souhaite éviter que des documents trainent sans surveillance. Avec l'application de l'encryptage et des certificats, le trafic des données entre les systèmes d'ORES et Indexis a été mieux sécurisé.

L'exécution fin 2014 de tests d'intrusion a confirmé l'utilité et l'implémentation correcte des mesures prises. Un audit de suivi effectué par un consultant externe a également confirmé un niveau de maturité de la sécurité des systèmes d'information plus que conforme aux normes du marché.

ORES travaille actuellement au développement d'un outil informatique propre afin de reprendre en interne les fonctionnalités gérées en Indexis.

Chapitre VII

Relation avec les producteurs

La procédure respecte strictement les dispositions du règlement technique relatives à la procédure de raccordement à la haute tension (articles 69 et suivants du règlement technique).

Cette procédure repose sur les principes et étapes suivants :

- un système de file d'attente est mis en place sur base du principe « Premier arrivé – premier servi » ;

- le producteur prend contact avec le GRD afin d'obtenir un avis préalable sur les possibilités d'accueillir une production décentralisée sur le réseau. Cet avis gratuit est indicatif et n'engage nullement ni le GRD, ni le candidat producteur ;

- réalisation d'une étude facultative d'orientation afin d'établir un ordre de grandeur du coût de raccordement et afin que le producteur puisse évaluer la rentabilité de son projet. A cette fin, le producteur prend contact avec le GRD. Le paiement des frais d'étude conditionne l'initiation de cette étude ;

- Dans les 15 jours ouvrables de l'enregistrement du paiement, le GRD communique au demandeur un rapport qui précise :
  - l'ordre de grandeur du coût de raccordement ;
  - diverses informations technico-administratives utiles pour la réalisation du projet ;

- Réalisation d'une étude détaillée. Le paiement des frais de cette étude et sa recevabilité conditionnent l'initiation de l'étude et la réservation de capacité d'accueil. Dès la réception en comptabilité du paiement des frais d'études, le GRD examine si le réseau est capable d'accepter la production demandée. Pour ce faire, il se coordonne avec le GRT/GRTL.

    1. Dans l'affirmative, le GRD fait, endéans 30 jours ouvrables (40 si P> 1 MW), une Proposition Technique et Financière (dénommée « PTF » dans la suite du texte), rédige un projet de contrat de raccordement en 2 exemplaires et demande au producteur de payer, à titre d'acompte, les frais liés à l'accès au réseau (terme A de la PTF). Lorsqu'une demande ne peut être traitée dans le délai de 30 jours ouvrables en raison d'études de capacité qui doivent être effectuées, sur le réseau de transport ou de transport local, dans le cadre de cette demande, ce délai est porté à 70 jours ouvrables. Une réservation de capacité correspondant à la demande du candidat producteur lui est attribuée. Elle prend cours soit à la date d'envoi de l'accusé de réception de la recevabilité de sa demande soit à la date de paiement de la demande d'étude détaillée (seule la date la plus tardive est prise en compte). Dès l'envoi des documents, le producteur dispose d'un délai de 30 jours ouvrables (40 si P> 1 MW) pour marquer son accord sur la proposition en renvoyant un exemplaire dûment signé du contrat de raccordement et en payant les frais liés à l'accès au réseau. Si

une demande de raccordement ne conduit pas à la conclusion d'un contrat de raccordement endéans ce délai, la procédure de demande de raccordement est considérée comme caduque. Le GRD avertit le demandeur 10 jours ouvrables avant l'expiration de ce délai et informe la CWaPE en cas de caducité. Sur demandes motivées, le demandeur peut obtenir des prolongations de ce délai, de maximum 20 jours ouvrables chacune, avec maintien de la réservation de puissance tant qu'aucune autre demande n'a été introduite. A contrario, dès réception du contrat de raccordement signé et du paiement, la capacité d'accueil réservée est définitivement acquise au producteur sauf désistement écrit de sa part ou si les travaux de raccordement n'ont pas été commandés dans un délai de 1 an (paiement de la totalité des termes B, C et D de la PTF). Dans ce dernier cas, il est possible pour le producteur de demander un délai supplémentaire de maximum 1 an pour la réalisation du raccordement pour autant qu'il apporte la preuve par une attestation d'une autorité communale ou régionale compétente que la demande de permis est bien introduite et suit son cours normal. Dans ce cas, si le délai est prolongé au-delà de 1 an, l'offre est réactualisée. A défaut de produire cette attestation ou si le producteur a confirmé l'abandon de son projet, le dossier introduit et la capacité d'accueil qui s'y rattache deviennent caducs. En cas de désistement du producteur ou d'annulation du contrat pour dépassement du délai, le paiement effectué, lié à la signature du contrat de raccordement, est remboursé après déduction d'un forfait approuvé par la CREG.

2. Si le réseau ne peut accepter qu'une partie de la production, le GRD contacte, dans un délai n'excédant pas 30 jours ouvrables, le producteur pour voir s'il est intéressé par cette capacité d'accueil limitée. Si OUI, le GRD poursuit comme au point 1. pour la capacité d'accueil disponible et comme au point 3. pour la partie non disponible pour autant que le producteur ait confirmé par écrit la poursuite de son intérêt pour cette partie non disponible immédiatement. Si NON, le GRD poursuit comme au point 3. si la demande du producteur ne peut être scindée.

3. Dans la négative, le GRD signale au producteur que sa demande ne peut être acceptée dans l'immédiat et l'informe du motif et si possible du délai approximatif où sa demande pourrait être acceptée soit par désistement de projets en cours et/ou investissements réalisés par le gestionnaire dans ses réseaux. Sa demande est actée - dans un ordre de priorité selon la date de l'accusé de réception de la recevabilité de la demande - dans un fichier en attendant qu'une capacité d'accueil se libère. Cette liste reprend, sur base du critère chronologique défini, les demandes partiellement satisfaites, les nouveaux projets et les extensions de projets existants. Dès que la possibilité de capacité apparaît, le GRD reprend contact, par ordre de priorité, avec les producteurs en attente pour voir s'ils restent intéressés par leurs demandes initiales. Si OUI, la procédure reprend conformément au point 1. ou 2. En cas d'application du 2., le candidat garde son ordre de priorité pour la partie non encore complètement satisfaite. Si NON, la demande du producteur devient caduque et est retirée de la liste d'attente.

- Le projet est radié de la file d'attente si un producteur modifie notablement, en cours de procédure, les données de son installation.

Il convient de noter que la procédure ainsi mise en place n'a donné lieu à aucun litige.

Chapitre VIII

Processus « Travaux clients » - Procédure d'application dans les services internes à ORES

La gestion du processus « travaux clients » est sous la responsabilité du département Infrastructures.
Ce processus traite l'ensemble des demandes de travaux tant externes qu'internes portant sur les branchements et compteurs électricité et/ou gaz naturel.
Les demandes externes peuvent être émises par un client (personne physique ou morale) ou par un tiers mandaté, par un organisme étatique ou par un fournisseur.
Les demandes internes sont émises par les services internes à ORES (Relevé et Validation Comptage, Access&Transit, Metering,…).

Le processus couvre les modules suivants :

- La **CAPTATION** : Collecte et enregistrement des informations nécessaires au traitement d'une demande ;
- L'**ETUDE** : Etude des travaux de réseau nécessaires pour permettre la réalisation du raccordement ;
- L'**OFFRE** : Etablissement et envoi de l'offre pour les travaux et frais d'étude éventuelle ainsi que l'enregistrement de l'accord du client ;
- La **PREPARATION** : Préparation administrative et technique d'une demande de travail et planification ;
- L'**EXECUTION** : Exécution technique du travail ;
- La **POST ADMINISTRATION** : Tâches administratives à remplir pour toute demande après l'exécution d'un travail (encodage, facturation).

Toutes les demandes sont enregistrées et traitées en SAP CS (Customer Service) par l'intermédiaire de l'outil informatique LOPEX.
Les données captées auprès du demandeur permettent de définir la prestation à réaliser par le GRD et de dimensionner le nouveau raccordement ou de modifier celui-ci (puissance mise à disposition, type d'alimentation, type de compteur,…).

Les données personnelles recueillies auprès du demandeur se limitent aux informations nécessaires à l'établissement de l'offre et à la facturation des prestations (coordonnées du demandeur, adresse de facturation, taux de TVA,…).

Dès l'exécution des travaux, les données techniques (assets) relatives au nouveau raccordement ou à sa modification sont enregistrées lors de la post administration en SAP ISU.

En matière de données personnelles, cette database ne contient que le nom de l'utilisateur du réseau de distribution (URD selon le règlement technique) et la date d'effet de son contrat de fourniture, établi avec le fournisseur. Ces informations sont transférées automatiquement à partir du registre d'accès d'A&T. Il est à noter que l'identifiant repris en SAP ISU sous l'URD n'est pas nécessairement le même que celui qui a fait la demande de travaux.
Seuls les intervenants d'ORES spécifiquement dédicacés ont accès aux outils SAP CS ET SAP ISU.

L’accès est en outre sécurisé. Ces outils ne sont donc pas accessibles aux tiers.

Les clients sont informés du respect de la confidentialité des données lors du traitement de celles-ci. Les documents suivants reprennent ces engagements :

- les conditions générales de raccordement,
- le contrat de raccordement (si d’application).

L’infrastructure informatique est sécurisée et l’accès à l’application est individualisé et réservé aux agents ORES en charge de ces prestations.

Chapitre IX

Les projets « smart »

ORES est concernée par le respect de la confidentialité des informations dont elle a connaissance, également dans les projets « smart » qu'elle développe.

Pour rappel, différentes procédures ont été mises en place pour respecter ces principes de confidentialité dans les projets pilotes « smart ».

Pour le projet « GAD » (gestion active de la demande), ORES a basé les études de consommation uniquement sur les données agrégées au poste de distribution qui sont de la sorte rendues totalement anonymes.

Dans le cadre des études et des projets pilotes relatifs à la mise en place d'un système de comptage intelligent et de son déploiement, ORES a contacté la Commission de protection de la vie privée en vue de se mettre en conformité avec la recommandation qu'elle avait émise sur les principes à respecter pour les smart grids et les compteurs intelligents (CO-AR-2011-004).

Une déclaration de traitement a été introduite par ORES et publiée par la Commission vie privée dès septembre 2013.

Cette déclaration précise les précautions prises par ORES dans la gestion des données confidentielles.

Le principe de proportionnalité, établi à l'article 4 de la loi sur la protection de la vie privée, impose au responsable du traitement de collecter exclusivement des données adéquates, pertinentes et non excessives, pour réaliser les finalités envisagées.
La transparence est absolument nécessaire. C'est dans cette perspective que des informations sur le traitement envisagé des données ont été transmises aux utilisateurs de réseau qui pourraient participer à l'étude projetée.

Les clients concernés qui acceptent de participer aux projets ont reçu également tous les renseignements leur permettant d'exercer leur droit d'accès aux informations et de rectification le cas échant : un point de contact leur a été désigné.

Dans la suite des études et des projets pilotes, le Programme Smart Metering d'ORES a mis en place des ateliers de travail sur le thème « Sécurité et Data Privacy ».

ORES a présenté à la CWaPE les actions réalisées pour la protection des données et les orientations prises pour un déploiement à grande échelle.

En concertation avec la CWaPE, et dans la suite de la recommandation européenne (Recommandation de la Commission du 10 octobre 2014 concernant le modèle d'analyse d'impact sur la protection des données des réseaux intelligents et des systèmes intelligents de mesure (2014/724/UE)), ORES procède actuellement à une analyse des risques relatifs à la protection des données des compteurs intelligents selon le modèle du DPIA (*Data Protection Impact Assessment*).

Selon les prescrits de ladite recommandation, *« le modèle doit non seulement faciliter la résolution des nouveaux problèmes concernant la protection des données, le respect de la vie privée et la sécurité rencontrés dans l'environnement de réseau intelligent, mais également contribuer à relever les défis en matière de traitement des données liés au développement du marché de détail de l'énergie »*.
L'avis 07/2013 du groupe de travail de la Commission recommande l'organisation d'une phase d'essai pour la mise en œuvre du modèle. Le modèle du DPIA est disponible sur le site internet de la task-force « Réseaux intelligents » (http://ec.europa.eu/ energy/gas_electricity/smartgrids/smartgrids_fr.htm).