

# L'ASSURANCE RETRAITE SANCTUARISE SES TRANSACTIONS

Pour sécuriser ses flux en environnement http et XML, le régime général de la retraite a implémenté les solutions intégrées de Beware : V-Sentry et I-Sentry. Ce pour accompagner le lancement des services Web destinés à faciliter les échanges entre cet organisme et ses partenaires.



Noël Breton, responsable  
de la production Web et réseau

Si l'actualité institutionnelle de la Cnav est marquée par son changement de raison sociale (elle s'appelle désormais l'Assurance retraite), son métier reste inchangé, la gestion du régime général de la retraite. Pour mener à bien ses missions, le premier régime s'occupant des retraités en France a mis en place un système d'information refondu dans les années 1990 et enrichi au fil des ans. Il permet de faire face à l'arrivée massive à la retraite des générations du baby-boom qui entraîne la gestion de 900 000 demandes de retraite chaque année, au suivi de carrières de plus en plus

complexes et à la nécessité de répondre aux attentes multiples du public.

Organisé autour de cinq processus métier, l'outil informatique de l'Assurance retraite comprend différentes couches applicatives (gestion des données sociales, de la retraite, de l'action sociale, des ressources humaines, logistique, comptabilité, etc.). Ces dernières années, plusieurs portails sont venus compléter cet existant : retraite.cnnav.fr, partenairesactionso-ciale.fr, ventail.fr, fournisseurs.cnnav.fr, etc.

## Un contexte applicatif de haute disponibilité

Pour garantir la haute disponibilité de ces outils, l'entreprise a mis en place une politique sécuritaire avec deux volets : les applicatifs http d'un côté, XML de l'autre. « Nous avons démarré il y a huit ans en mettant en place des pare-feux applicatifs. Au terme d'une consultation publique, nous avons retenu la solution d'Axilliance éditeur entré dans le giron de Bee Ware depuis quelques années. Celle-ci permet de mettre en place une architecture de sécurité active des services en ligne », explique Noël Breton, responsable de la production Web et réseau.

La première application concernée était un Intranet. Il s'agissait de la Base nationale de législation. Véritable outil quotidien du liquidateur, il permet de rechercher des documents via un moteur intégré. La volonté de la publier dans un environnement Internet a nécessité la mise en place de mécanismes de Reverse Proxy permettant de garantir la haute disponibilité des données. I-Sentry, la solution d'Axilliance, a été implémentée « en partenariat avec l'éditeur qui s'était montré très réactif tout au long de notre chantier », indique Noël Breton. Le déploiement de cette première expérience de sécurisation a duré six mois. L'Assurance retraite, connue alors sous le nom de Cnav, avait décidé d'accélérer le mouvement de sanctuarisation de ses outils. « Nous avons pris pour parti de mettre toutes nos applications Web sous le contrôle d'un Reverse Proxy. Ce qui était original à l'époque. L'ensemble des sites Web régionaux de la Cnav étant hébergés sur notre centre informatique de Tours, nous leur avons appliqué immédiatement cette stratégie sécuritaire », rappelle le responsable de la production Web et réseau. Chemin faisant, d'autres outils ont été rajoutés. Il y a six ans, le portail institutionnel cnnav.fr a été verrouillé par les outils d'Axilliance. Tout comme l'ensemble des solutions X-net, déployées au fil de l'eau.

En environnement http, le système retraite.cnnav.fr a été verrouillé. Il contient 2 600 000 inscrits. Entièrement destiné aux assurés, il leur permet de visualiser leur relevé individuel de carrière, d'estimer leur montant de retraite du régime général et de suivre l'état d'avancement de leur demande de retraite. La plate-forme Eventail destinée aux déclarations d'entreprises a connu également le même sort. Très sollicité au mois de janvier par les sociétés qui déclarent les données sociales des cotisants, ce site doit fonctionner sans interruption ni dysfonctionnement. Traitement identique pour l'extranet ouvert aux partenaires que sont la Cnamts et autres Cram. Les 50 000 agents de ces institutions interrogent régulièrement le système d'information de l'Assurance retraite dans un environnement qui doit être sécurisé de bout en bout.

## Les applications XML concernées à leur tour

Disposant d'un patrimoine applicatif imposant et hébergé dans un environnement MVS/DB2 en site central et Oracle Application Server en front-office, l'Assurance retraite doit échanger de plus en plus avec ses partenaires. Or, cette architecture est loin d'être ouverte. Pour communiquer avec l'extérieur, l'AR a fait le choix des services Web développés en environnement XML. Ici se posait également la problématique de la sécurisation des transactions. Fallait-il recourir à une boîte noire du marché ou à une solution interne ? La première option a été retenue. Bee Ware a été sélectionné car il propose une nouvelle solution : V-Sentry. Disponible sous forme d'une gamme d'Appliances sécurisées, elle est constituée d'une plate-forme d'optimisation et d'accélération du trafic. Elle se compose de deux modules, Web et XML, permettant de contrôler et de filtrer toute application Web. « Nous avons confirmé l'utilisation de l'offre de ce fournisseur pour nos échanges XML car il connaissait déjà notre

problématique métier et était très disposé à nous accompagner dans notre nouveau chantier », souligne Noël Breton. L'éditeur a participé à la sécurisation de l'ensemble de Web Services développés en interne. Cinq au total.

Hébergeant le portail de GIP Services, l'Assurance retraite entend ouvrir ce dernier via l'un de ces services Web, à ses partenaires qui pourront l'interroger dans un environnement sécurisé. L'accès au serveur d'identification sera également effectué via l'un de ces services Web.

Avant de se lancer dans la sécurisation de ces composants, le régime général de retraite français avait organisé la réalisation d'une maquette l'année dernière. Aujourd'hui, elle est finalisée à 90 %. L'intégration sera effective après validation des transactions.

Tout comme en environnement http, les outils de Bee Ware fonctionnent ici dans une logique de boîte noire. Il n'est donc pas nécessaire de configurer régulièrement les pare-feu. L'administrateur dispose d'une interface homme/machine lui permettant de les administrer. À partir de cette IHM, peuvent être déclarés de nouveaux applicatifs. Par ailleurs, les concepteurs de nouvelles applications XML doivent réaliser des développements supplémentaires autour de ces solutions, développements qui permettent d'assurer leur sécurité.

Si intégrer des outils de sécurisation des flux constitue une étape importante en matière de verrouillage des flux, confirmer régulièrement leur bon fonctionnement est nécessaire. « Nous sommes en permanence sujet à des attaques variées, y compris applicatives. Il fallait mettre en place des solutions de sécurité sans faille basée sur les outils de Reverse Proxy. En complément de ces solutions, nous devons régulièrement vérifier leur aptitude à faire face aux assauts répétés des malveillants », estime Noël Breton.

V-Sentry sera exploité dans le cadre de la démarche de création d'un standard interopérabilité (Interops), orchestrée par différents organismes sociaux : outre l'Assurance retraite, la MSA, le RSI, etc. Dans ce chantier, la Cnav joue

le rôle de producteur de services. Y participent également la direction de la Sécurité sociale (DSS) et la direction générale de la modernisation de l'État (DGME). À travers un tel projet, les organismes impliqués entendent sécuriser les échanges entre eux sur la base d'un standard de propagation des droits d'accès et des habilitations. Les normes techniques retenues sont Https avec TLS, Soap et WS-Security, SAML 2.0 qui permet de définir un protocole pour échanger des informations liées à la sécurité. Une expérimentation avait d'ores et déjà été conduite en 2006. Le champ applicatif concerné était le Web Services Identification. L'année 2008 sera celle de la finalisation de ces tests conduits tout au long de l'année 2007.

Organisme gérant des applications critiques en environnement X-net et XML, l'Assurance retraite a su mettre en place une solution intégrée de gestion des transactions. Mieux, elle est motrice dans le projet de mise en place du standard Interops qui, à terme, permettra à différents organismes de la sphère sociale d'échanger en toute sécurité et à des coûts de gestion optimisés.

**Emmanuel Mayega**