SÉCURITÉ

L'IAM opérationnel au CHU de Nantes

L'enjeu majeur d'un projet IAM / SSO n'est pas technique : il est organisationnel. C'est pourquoi un des facteurs majeurs de sa réussite, au CHU de Nantes, a été son pilotage général par la Direction des ressources humaines. La solution choisie, signée Evidian, a permis un déploiement progressif. Elle gère les cas d'usage les plus complexes tout en fournissant un accès simple et sécurisé au SI. Retour d'expérience.

IAM : trois lettres, un acronyme qui désigne l'Identity Access Management, autrement dit la gestion des identités et des accès. Historiquement, les pouvoirs publics (l'Agence des systèmes d'information partagés de santé – Asip Santé – en tête) ont tenté de convaincre les établissements de santé de déployer un système d'authentification forte pour l'accès à leur système d'information (SI), prioritairement la carte CPS. Après de nombreux avatars, le constat est clair sur le territoire : au dernier Congrès de la sécurité du Mans, un représentant de l'Asip reconnaissait que moins de 3 % des établissements étaient conformes à un décret qui, depuis, est devenu obsolète.

Le CHU de Nantes s'est néanmoins engagé dans ce programme majeur il y a plusieurs années, car un projet IAM dépasse de loin les seuls enjeux du déploiement d'un système d'authentification forte au SI

Intégrer tous les besoins dans un même projet

À Nantes, les premiers groupes de travail (2008) ont immédiatement posé des bases claires pour ce projet. Certes l'accès au SI était une cible, mais le CHU a fait le choix d'une carte multiservice unique pour en faciliter l'adoption : accès au SI, au self, aux locaux et aux parkings. Le groupe de travail est en effet parti du principe qu'une carte unique a moins de chance d'être oubliée dans une blouse ou à la maison.
De plus, il était important pour les utilisateurs de ne plus avoir à retenir les huit mots de passe (chiffre moyen constaté) des applications en tout genre dont ils disposent (session, messagerie, dossier patient, etc.). Pour cela, le déploiement d'un système de SSO (Single Sign On) faisait partie des besoins exprimés. Enfin, le dernier objectif était d'accélérer notablement la délivrance des habilitations applicatives et de supprimer au plus tôt celles des personnels ayant quitté l'établissement.

La gouvernance de ce genre de projet est absolument primordiale. Le CHU a voulu éviter à tout prix que les différentes parties prenantes internes vivent le projet comme une solution purement technique, raison pour laquelle la DSI a obtenu que le pilotage général du projet soit assuré par la Direction des ressources humaines, ce qui a été un facteur majeur de réussite.

Choisir une solution répondant aux critères prédéfinis

Le CHU de Nantes s'est engagé dans un dialogue compétitif pour le choix du prestataire, procédure qui, certainement en 2008, avait un sens : il n'y avait à l'époque aucun segment UniHA qui traitait ce besoin. Si c'était à refaire, le CHU utiliserait bien entendu les marchés UniHA, ce qui tombe bien : la solution retenue – BULL intégrant la solution de sa filiale **Evidian** – correspond à une offre du marché UniHA.

Ce choix a été motivé par différentes considérations, et notamment le fait de disposer d'une solution logicielle unique et intégrée : il n'était pas question pour les équipes DSI de passer du temps à faire dialoguer les briques de divers éditeurs.

De plus, la solution **Evidian** gère les cas d'usage complexes dans un CHU : basculement rapide de session d'un PC en mode partagé, itinérance de session d'un même utilisateur qui se connecte sur divers PC dans une même journée, etc. Les briques internes **Evidian** permettent également de gérer le circuit des habilitations, de l'arrivée de l'agent dans le CHU (approvisionnement amont des identités, implémentation de la politique de droits) à son départ (suppression des identités et des droits afférents). Bien entendu, last but not least, **Evidian** fournit une des meilleures solutions SSO du marché, puisque c'est son métier d'origine. La sécurité globale apportée est de plus un atout majeur : cette solution équipe également des banques et des sociétés officiant dans des domaines très sensibles.

En somme, la solution d'**Evidian** fournit un accès simple et sécurisé avec une authentification forte pour professionnels de santé, administratifs, partenaires et patients. Et ce à tout moment, en toute situation et depuis tout terminal permettant d'optimiser le travail du personnel des établissements de santé.

Les chiffres du projet IAM au CHU de Nantes

- 12 000 agents
- plus de 2 000 personnels extérieurs
- 7 000 postes de travail
- une vingtaine d'applications impactées

Le mot de l'éditeur

Avec plus de 60 clients établissements de santé et 500 000 utilisateurs déployés, Evidian s'avère un acteur majeur dans ce secteur en France et à l'international. La réussite du projet IAM du CHU de Nantes nous réjouit particulièrement par sa dimension, par la complétude fonctionnelle de la solution implémentée. Elle conforte nos choix techniques en termes de produit et de services pour répondre aux besoins des métiers de la santé.

Mettre en œuvre et déployer un projet IAM réussi

Un projet IAM/SSO impacte de nombreuses briques du SI : l'annuaire Active Directory, les habilitations applicatives, le poste de travail, etc. (une description plus précise est développée dans le premier ouvrage cité après la signature). La solution d'**Evidian** permet un déploiement progressif : il est possible de déployer dans un premier temps le Back Office (les flux de données internes), puis de s'attaquer au poste de travail (SSO, authentification utilisateur) ou inversement.

Mais l'enjeu majeur de ce projet n'est pas technique : il est organisationnel. En effet, la définition des politiques d'habilitation, le contrôle des identités avant délivrance d'une carte, la connaissance de l'exhaustivité des personnels travaillant au sein de l'établissement – et pas seulement ceux rémunérés – sont autant de questions qui ne relèvent pas de la DSI mais d'autres fonctions supports (RH, services techniques, etc.) qui doivent prendre en charge certaines fonctions ou flux de demandes. La solution doit implémenter des politiques d'habilitation qui doivent être définies par les services en charge de ces domaines fonctionnels : le logiciel sait tout faire, encore faut-il lui exprimer sa demande sans ambiguïté.

En ce sens, la conduite du changement est un aspect important du projet et doit associer le service Communication. À ce jour, le projet est quasiment déployé en totalité sur le CHU.

Analyser les bénéfices d'un tel projet

Un projet IAM, c'est d'abord et avant tout un projet de maîtrise des identités numériques de la structure. Combien d'établissements stockent toujours dans leurs annuaires l'identité de personnels ou de fournisseurs n'exerçant plus en leur sein depuis des années ? Les pouvoirs publics commencent clairement à cibler ce défaut de maîtrise : le critère P3.5 d'Hôpital numérique aborde la question des identités des utilisateurs, et la non-maîtrise de ces identités est pointée par les audits de certification des comptes. Cette anomalie va donc devenir, à terme, un point de non-conformité des SI et gageons que des crédits seront attribués – ou non – en fonction des résultats obtenus dans ce domaine.

Bien sûr, au-delà de ces aspects réglementaires et de sécurité, il y a la facilité d'usage du SI : une fois le SSO mis en place, il est quasi impossible de le retirer aux utilisateurs. Sans parler bien entendu de l'accélération des attributions des identifiants et habilitations, qui passent de plusieurs semaines à quelques jours.

S'adapter aux nouveaux enjeux

La solution **Evidian** évolue vite et dans le bon sens. Ainsi, la brique Wam (Web Access Manager) résout l'équation difficile de l'accès au SI depuis l'extérieur à partir de terminaux divers (tablettes, PC personnel d'un médecin) ne disposant pas de lecteur de cartes. **Evidian** est d'ailleurs pionnier dans ce domaine, avec des solutions basées sur des Flashcode ou des associations de téléphones portables hétérogènes.

Sécuriser le SI, c'est instaurer la confiance

Le déploiement des SI dans le domaine du soin s'accompagne de son corollaire : sans confiance dans le SI, impossible de demander aux utilisateurs et usagers d'y stocker des informations, ce qui est pourtant l'enjeu majeur de l'informatisation du soin. Et dans la sécurité, il y a certes la disponibilité ou résilience – qui reste cruciale –, mais l'on ne peut pas faire fi de la confidentialité : la récente affaire autour du dossier médical d'un coureur automobile célèbre est là pour nous le rappeler.
Evidian est-il le meilleur éditeur de solution IAM/SSO ? Impossible de répondre à une telle question : au dernier Salon de la sécurité à Londres – le plus grand d'Europe –, les éditeurs foisonnaient dans ce domaine, la plupart totalement inconnus sur le marché français.

Mais si l'on rajoute dans les critères de choix la pérennité de l'entreprise – sa diffusion à l'international, son appartenance à un groupe majeur et la forte base installée dans nombre de secteurs de l'industrie ou du tertiaire –, il n'en reste plus beaucoup à y répondre, même dans UniHA.

▸ Cédric Cartau

L'impact réglementaire

Qu'il s'agisse de la certification HAS 2014 ou de l'audit de certification des comptes, les exigences des pouvoirs publics concernant la fiabilité du SI croissent tous les ans. Bientôt, ceux qui ne pourront pas démontrer leur bonne gestion des identités seront, au mieux, en deuxième division des établissements de santé.

Responsable Sécurité des systèmes d'information au CHU de Nantes, **Cédric Cartau** est également chargé de cours à l'École des hautes études en santé publique (EHESP).

Il réalise également des audits de systèmes d'information pour le compte d'établissements publics ou privés dans différents secteurs d'activité.

Il est aussi auteur des ouvrages suivants aux Presses de l'EHESP :
- *La Sécurité du système d'information des établissements de santé, 2012*
- *Guide pratique du système d'information, 2013*
- *Stratégies du système d'information, vers l'hôpital numérique, 2014*