



Professionnels de Santé

Confidentialité et facilité d'accès
aux informations médicales

La sécurité au cœur de la refonte des S.I. des établissements de santé

La protection des données médicales est un enjeu majeur dans les établissements de santé. Pour autant, les contrôles d'accès ne doivent pas entraver la production de soins. Evidian, éditeur de logiciels de gestion des identités et des accès, facilite le travail quotidien des professionnels de santé tout en protégeant l'accès aux applications médicales.

La première
étape pour
sécuriser votre
S.I. de Santé

Parce qu'elles relèvent de l'intimité et de l'état de santé des patients, leur divulgation peut porter atteinte aux droits et libertés des personnes concernées, les données traitées par les systèmes d'information hospitaliers doivent être particulièrement protégées. Ces données, couvertes par le secret médical, ne peuvent être communiquées qu'à des utilisateurs habilités et autorisés.

Des solutions pour sécuriser votre S.I.

Evidian, filiale de Bull, est un éditeur spécialisé depuis plus de 15 ans dans les solutions de gestion des identités et des accès (IAM). Quatre millions d'utilisateurs actifs accèdent à leurs applications avec les solutions d'Evidian.

Evidian est reconnu par les analystes spécialisés et a été distingué par de nombreux trophées internationaux. La suite Identity and Access Management d'Evidian a notamment remporté le prix de la « Meilleure solution IAM » aux SC Awards Europe 2013 de SC Magazine.

L'offre IAM d'Evidian facilite la gestion des accès, des identités et des rôles. Elle est composée de modules qui s'installent de manière autonome ou s'intègrent avec d'autres modules de la suite ou d'éditeurs concurrents. L'offre IAM d'Evidian est entièrement développée et supportée en France par les équipes d'Evidian.

Compatibilité Carte de Personnel de Santé

Evidian propose la seule offre complète de gestion des identités et des accès adaptée aux cas d'usage dans un centre hospitalier. Elle couvre l'authentification unique (SSO), les processus d'habilitation, le provisioning et la synchronisation d'annuaires.

« Le Collège de Déontologie rend un avis favorable à la demande d'usage du système CPS par les applications de la société Evidian : Enterprise SSO, ID Synchronization, Policy Manager sous réserve d'une utilisation sans mode dégradé. Il insiste sur l'importance du rôle de conseil de l'entreprise concernant la solution CPS »

Collège de Déontologie du GIP-CPS,
Juillet 2009

Une démarche pragmatique

Constitution du référentiel d'identités de l'hôpital

Pour gérer ses accès, l'hôpital doit disposer d'un référentiel d'identités fiable. Ce référentiel peut être Microsoft Active Directory ou tout autre annuaire supporté. Si ce référentiel est actuellement incomplet, *Evidian ID Synchronization* l'alimente et le synchronise avec différentes sources de données (base des Ressources Humaines, paye etc.)

La solution d'Evidian place ensuite dans ce référentiel les informations d'authentification de vos utilisateurs sous forme sécurisée : autorisations, identifiants, mots de passe des applications...

Authentification forte par carte CPS

Comme le demande le décret de confidentialité, *Evidian Authentication Manager* permet de déployer l'authentification forte par carte CPS ou équivalent (carte d'Etablissement) avec certificat X509 (stockés dans la carte à microprocesseur).

Authentification unique (single sign-on - SSO)

Evidian Enterprise SSO se substitue à l'utilisateur lors de l'authentification aux applications protégées par mot de passe. Non intrusif vis à vis des applications, il change les mots de passe automatiquement. Tous les types d'applications protégées par mot de passe (internes ou externes) sont ainsi supportés : Windows, client léger Citrix, web... Un mode d'apprentissage collecte les mots de passe applicatifs auprès des utilisateurs, ce qui accélère le déploiement et inventorie les comptes réellement utilisés.

Changement rapide d'utilisateur – mode kiosque

Dans les unités de soins ou les urgences, infirmiers et médecins accèdent rapidement à des PC en kiosque. Cet accès se fait sous leur propre identité, en fonction de leurs droits, sans fermer la session Windows en cours. Avec *Evidian Authentication Manager*, la session Windows reste la même d'un utilisateur à l'autre. Mais le contexte de sécurité et l'ouverture et fermeture d'applications sont propres à chaque utilisateur, authentifié par carte CPS ou badge radio/RFID.

Lorsqu'un utilisateur retire sa carte du lecteur ou qu'il s'éloigne du poste de travail (RFID ou badge radio non détecté), la session est automatiquement verrouillée.

Si le même utilisateur revient sur le même poste de travail, il retrouve ses applications encore ouvertes. Mais si un autre utilisateur se connecte à ce poste de travail, la solution d'Evidian ferme automatiquement les applications avant d'effectuer un changement d'utilisateur sans « rebooter » le poste de travail.



Délégation des droits des utilisateurs

Un professionnel de santé qui part en formation ou en congés peut déléguer à un collègue, de manière sécurisée, les accès à ses applications métiers afin de garantir la continuité des soins.

Gestion des droits d'accès

En fonction de votre organisation, *Evidian Enterprise SSO* permet de définir des rôles d'administration avec des vues dédiées.

Sa console permet de gérer :

- les droits d'accès aux applications,
- les profils associés aux accès, notamment les méthodes d'authentification,
- les mots de passe des applications dont le changement est pris en compte par le SSO,
- la politique de contrôle des accès en fonction des points d'accès et des horaires,
- le cycle de vie des cartes,
- l'audit et la traçabilité des actions des utilisateurs et des administrateurs etc.

La mobilité au service du professionnel de santé

Quand il quitte l'hôpital à la fin de son service, l'activité du professionnel de santé ne cesse pas pour autant. De son domicile, de son cabinet et d'où qu'il se trouve, il doit pouvoir compléter les dossiers des patients, consulter les résultats d'analyse et lire les courriels internes.

Evidian Web Access Manager permet aux professionnels de santé d'accéder en toute simplicité aux applications web de l'hôpital (mail, gestion de dossiers patients...), tout en préservant un niveau de sécurité élevé et ce en particulier depuis un poste personnel, une tablette et un smartphone.

Auditer les connexions des utilisateurs

Evidian Enterprise SSO collecte tous les événements concernant l'authentification, l'autorisation et la connexion des utilisateurs ainsi que les actions des administrateurs. Ces événements d'audit peuvent être sélectionnés par des filtres et affichés dans des rapports.

La sécurité de bout en bout

Evidian apporte l'authentification unique et la protection des accès par carte CPS. Sur cette base, l'établissement de santé peut ajouter des fonctions complètes de gestion et de contrôle.

Evidian Identity & Access Manager modélise la politique de sécurité de l'établissement en fonction de rôles métiers. Une fonction de provisionnement crée et supprime les comptes sur les applications ou les systèmes eux-mêmes. Un outil de réconciliation vérifie que la politique du modèle est respectée par les applications.

Evidian Identity & Access Manager automatise et surveille les tâches d'administration des utilisateurs et habilitations. Des rapports permettent de contrôler la bonne application de la politique de sécurité.

Editeur présent mondialement, *Evidian* équipe une cinquantaine d'hôpitaux en France, Belgique, Hollande, Royaume-Uni et Moyen-Orient, de solutions de gestion des identités et des accès. Ces établissements respectent ainsi leurs exigences légales de confidentialité tout en rendant leurs professionnels de santé plus efficaces et autonomes, ce qui améliore la qualité des soins.