

	DOCUMENT INFORMATIF Annexe technique - référentiel IAM et sécurisation du poste de travail (GAIA)	Diffusion par : PILNH - DSN	0085-DI-223
	Processus : INF-CHU-Gestion des Services Numériques	Page 1 / 6	V. 01

1. INTRODUCTION

Le CHU de Nantes a mis en œuvre un projet de sécurisation d'accès à son Système d'Information par la mise en place d'une solution GAIA (Gestion des Annuaire des Identités et des Accès) pour être conforme au décret N°2007-960 du 15 mai 2007 relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique.

Cette solution est basée sur :

- Une carte d'établissement de type carte IAS bi technologie (contact et sans contact) avec embarquement de certificats.
- La solution Entreprise SSO de l'éditeur Evidian pour le contrôle d'accès au poste de travail et le SSO (Single Sign On) pour la connexion aux applications nécessitant une authentification
- La solution IAM (Identity Access Management) V9 de l'éditeur Evidian pour
 - Le référentiel des identités basé sur un annuaire de type AD LDS
 - Le référentiel de la politique de sécurité des applications et règles d'attribution basé sur le module Policy Manager
 - Le provisionnement automatique et manuel des applications à travers des connecteurs basés sur le module User Provisionning
 - La gestion des Workflow du cycle de vie des identités et des demandes d'habilitations basé sur le module Request Manager
- La gestion de l'audit des accès et des habilitations basées sur un univers Business Object

2. LA CARTE D'ETABLISSEMENT

Le CHU de Nantes met à disposition de l'ensemble du personnel hospitalier une carte d'accès nominative. Ces cartes sont multi services (accès au SI, locaux, parking, porte-monnaie self...)

Il s'agit d'une carte de type IAS qui embarque des certificats d'authentification délivrés par la PKI d'entreprise du CHU de Nantes basé sur la solution de PKI Microsoft.

2.1 Spécifications de la carte IAS

La carte Gemalto IAS-ECC est le support cryptographique retenu par le CHU NANTES pour la mise en œuvre de la carte d'établissement.

Il s'agit d'une carte bi technologique disposant :

- D'un composant carte à puce
- D'un composant RFID

Les spécifications générales de la carte IAS-ECC de Gemalto sont rappelées ci-dessous :

- Niveaux de certification : Certification IAS-ECC et EAL4+ PP SSCD Q1 2009
- Dimension du support cryptographique : ISO 7816-1
- Mode(s) de communication du support cryptographique : Contact, sans contact ISO14443-A 1, 2, 3, 4 et Mifare 1K
- Services de cryptographie intégrés à la puce : 3DES (ECB, CBC), AES (128, 192, 256), RSA jusqu'à 2048bit, SHA-1, SHA-2, ELC P256, Génération « onboard » de bi-clés RSA, conforme aux exigences de la PRIS v2 pour tout type de certificats *, ** ou ***
 - ☐ Capacité de stockage de la puce : 64 Ko d'EEPROM disponibles pour les données licitatives et plus d'une douzaine de certificats
 - ☐ Système d'exploitation de la puce : JavaCard Virtual Machine, RTE et API conformes à JC2.2.1, Card Management & API conformes à GP2.1.1 (protocoles SCP01 and SCP02)

REDACTEUR(S)	VERIFICATEUR(S)	APPROBATEUR(S)	Date d'application
Eric MALEVIALLE (Responsable - PILNH \Services Numériques\Infrastructures)	Pierrick MARTIN (Coordonnateur qualité - PILNH \Services Numériques)	<Ne pas modifier>	30/05/2023

- Nombre supporté d'insertion et de retrait du support cryptographique contact : 10000
- MTTF (Mean Time To Failure) : Plus de 500K cycles de lecture/écriture

3. AUTHENTIFICATION PRIMAIRE ET SSO

Pour l'authentification primaire des utilisateurs du Système d'Information du CHU de Nantes, la solution s'appuie sur le module Entreprise SSO. Ce module permet d'assurer l'authentification primaire à base de certificats « Etablissement » stockés dans la carte d'établissement (composant à microprocesseur).

3.1 Mécanisme d'authentification

La solution prend en charge automatiquement l'ouverture de session du poste de travail de l'utilisateur. La mire d'authentification Microsoft (Gina) est remplacée par le module Authentication Manager d'Entreprise SSO. Cette Gina a une apparence similaire à celle de la Gina Microsoft et fournit toutes les fonctions de la Gina standard.

L'authentification à base de certificats contrôle la validité, la signature du certificat et sa publication par l'Autorité de Certification de confiance de l'Etablissement.

En ce qui concerne l'authentification sur l'Active Directory celle-ci s'appuie sur le mot de passe Windows qui est stocké dans la carte d'établissement. La validité du certificat d'authentification présent dans la carte d'établissement est vérifiée lors de l'authentification.

3.2 Les différents modes de travail pris en compte

3.2.1 *Mode sédentaire ou poste dédié*

Le poste de travail est dédié à un utilisateur du CHU de Nantes. Il est équipé d'un lecteur de carte à microprocesseur de type contact. L'accès au poste de travail est sécurisé par la carte d'établissement.

3.2.2 *Mode kiosque : Changement rapide d'utilisateurs*

Certains environnements exigent que de multiples utilisateurs puissent partager le même poste de travail, tout en commutant d'une session à l'autre aussi rapidement que possible.

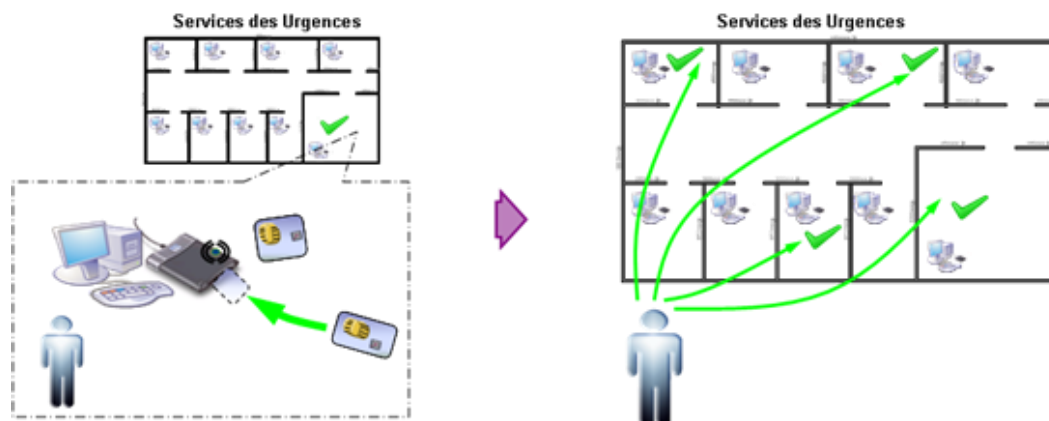
Le changement rapide d'utilisateur « **Mode Kiosque** » fournit une solution où la session Windows demeure la même d'un utilisateur à l'autre mais où le contexte de sécurité du SSO, et l'ouverture/fermeture d'applications sont traités individuellement pour chaque utilisateur.

Le « Mode Kiosque » prend en compte les applications client/serveur, web et déportées dans un client léger. De même les postes dits en « libre-service » sont des postes pris en considération par défaut pour le mode Kiosque/Changement rapide d'utilisateurs.

Le poste de travail est partagé par plusieurs utilisateurs. Il est équipé d'un lecteur de carte à microprocesseur de type contact ou d'un lecteur mixte à la fois contact et sans contact (RFID). L'accès au poste de travail est sécurisé par la carte d'établissement contenant des certificats « établissement ».

3.2.3 Mode itinérance de session

Le mode « **itinérance de session** » ou « **roaming** » permet aux utilisateurs d'être mobiles au niveau d'un service en retrouvant leur session de travail d'un poste à un autre sans authentification systématique. Pendant un délai de grâce et pour un groupe de postes de travail, l'utilisateur n'a obligation de s'authentifier qu'une seule fois sur un seul des postes de travail.



3.3 Single Sign On - SSO

Après l'authentification primaire de l'utilisateur, Entreprise SSO récupère dans le référentiel des données de SSO, les attributs de sécurité de l'utilisateur, tels que les mots de passe pour accéder à ses applications cibles. Ces attributs de sécurité sont stockés de manière sécurisée dans le référentiel des données de SSO puis rapatriés sur le poste de travail dans un cache de sécurité chiffré. La solution de SSO va se substituer à l'utilisateur dans les séquences liées à l'authentification vers les applications protégées par mot de passe. La solution permet ainsi d'assurer la gestion des multiples mots de passe dès lors que l'utilisateur s'est authentifié au démarrage de sa session.

Entreprise SSO est une solution basée sur un **principe non intrusif** vis à vis des applications. Grâce à ce concept non-intrusif, toutes les applications protégées par mot de passe peuvent être supportées.



Le système de SSO est basé sur la détection des fenêtres (gestion des classes) qui apparaissent sur le bureau de l'utilisateur. Il vient donc se substituer aux utilisateurs dans la saisie des informations de connexion lorsque celles-ci sont détectées.

Il est important que toutes les fenêtres d'authentification (connexion, message d'erreur de connexion, changement de mot de passe, changement rapide de contexte de sécurité...) puissent être identifiées de façon unique par le système lors de la détection de celles-ci.

3.4 Changement des mots de passe

Entreprise SSO prend en charge le changement du mot de passe secondaire sur l'initiative du client installé sur le poste et conformément à une politique d'âge du mot de passe qui peut être définie application par application.

La configuration de cette fonction est réalisée par le studio « SSO Studio » permettant de définir les SSO en désignant les actions ou les interfaces programmatiques accessibles depuis le poste client. Si Entreprise SSO détecte que le mot de passe est utilisé depuis une durée dépassée, il procède à la génération et l'envoi d'un nouveau mot de passe. Cette fonction requiert que des fonctions de changements de mot de passe soient accessibles soit par interface utilisateur soit par interface programmatique depuis le poste de l'utilisateur. Si tel

n'est pas le cas, le seul recours sera l'expiration du mot de passe au niveau du serveur d'application qui provoquera le renouvellement du mot de passe.

Entreprise SSO permet de définir des politiques de génération et contrôle du mot de passe application par application afin de définir le nombre de caractères, les longueurs minimale et maximale ainsi que les types de caractère requis pour la formation d'un mot de passe valide au cours de la phase d'authentification d'une application.

3.5 Interfaces contextuelles inter-applications

Dans le cas où une interface contextuelle doit être mise en place entre 2 applications, il faut que l'authentification permettant l'ouverture du canal de communication puisse **être traitée par le système de SSO** et non pas par le passage du compte et mot de passe d'une des applications pour ouvrir une session sur l'autre application.

L'interface contextuelle proposera donc une méthode d'authentification de type fenêtre de connexion ou passage de paramètres (login et mot de passe) au moment de l'initialisation du canal de communication.

Ce mode de fonctionnement permet à chaque application de gérer la complexité et le cycle de vie du mot de passe de façon indépendante tout en garantissant à l'utilisateur un accès « transparent » entre application.

4. GESTION DES IDENTITES ET DES ACCES

4.1 Gestion de la politique de sécurité

Pour rappel, la politique de sécurité a pour objectifs :

- L'assurance que seules les personnes susceptibles d'accéder à l'information y soient autorisées de façon pérenne
- La garantie que ces mêmes personnes n'aient que les droits nécessaires et suffisants correspondant à leur positionnement dans l'organisation.
- La mise en conformité avec la Loi sur l'audit d'accès aux ressources. (LEN2/HSPT).
- La garantie de la sécurité des accès aux informations selon le niveau d'habilitation requis (applications médicales, dossiers patient ...).

L'outil de gestion de la politique de sécurité, **Policy Manager**, s'articule autour de 3 fonctions principales.

- Tout d'abord la création des différents éléments de la politique de sécurité : les rôles, les organisations, les applications, les permissions, les exclusions, les assignations des utilisateurs à des rôles ou à des couples (rôles, organisations)
- Ensuite, l'application de la politique afin de définir un état désiré des droits d'accès et des autorisations des utilisateurs.
- Et pour finir, la comparaison de cet état désiré avec l'état réel des systèmes et applications cibles - et la mise à jour automatique ou manuelle de ces cibles (réconciliation).

Policy Manager utilise les concepts suivants :

- La prise en compte du couple rôle/organisation au sein d'un modèle RBAC étendu.
- La mise en œuvre des fonctions d'héritage par l'organisation, la hiérarchie ou les rôles.
- La réconciliation pour comparer une politique avec la réalité sans modifier les systèmes et applications cible.
- L'exclusion entre les rôles, les couples (rôles, organisation) et les permissions elles-mêmes.

4.2 Gestion de l'alimentation aval des applications

Le module **User Provisioning** permet de mettre en œuvre les actions de provisionnement, dé-provisionnement et réconciliation entre un état central et les systèmes et applications cibles.

User Provisioning propose des connecteurs et des agents, pour attribuer à des utilisateurs ou des groupes d'utilisateurs ayant le même rôle une série de comptes ou attributs dans des applications systèmes et bases de données.

Les connecteurs de provisionnement fonctionnent sur un serveur central et accèdent à distance aux systèmes ciblés pour réaliser des opérations de provisionnement.

4.3 Connecteurs de provisionnement

La solution permet de gérer différents types de connecteurs :

- LDAP
- Fichiers plats
- Lien ODBC
- API
- WebServices

4.3.1 *Connecteur LDAP (priviligée)*

Dans le cas où l'application utilise une authentification AD, il est préférable d'utiliser l'appartenance à des groupes AD pour fournir les profils applicatifs (habituellement par mapping dans l'application) afin de ne pas avoir à gérer de base locale des comptes.

L'intérêt pour le CHU de NANTES est qu'il n'y a aucune interface à mettre en place car elle existe déjà. Il est juste nécessaire de décrire une politique de droits pour peupler les groupes AD correspondants.

4.3.2 *Connecteur fichiers plats*

Dans ce cas, le référentiel des comptes utilisateurs est stocké dans un fichier de type CSV sur le serveur de politique. Ce fichier est transféré régulièrement vers le serveur applicatif afin de permettre à l'application, via un module d'import, de prendre en compte les nouveaux comptes et modifications liées au cycle de vie des identités.

A minima, il est nécessaire de développer une demie interface du côté de la solution GAIA pour fournir les données attendues par l'autre demie interface fournie par l'éditeur de l'application.

4.3.3 *Connecteur ODBC*

Un lien ODBC est mis en place vers la table des utilisateurs de l'application afin d'inscrire les données des comptes utilisateurs dans celle-ci.

A minima, il est nécessaire de développer une demie interface du côté de la solution GAIA pour fournir les données attendues dans la table utilisateurs de l'application.

4.3.4 *Connecteur API ou Webservice*

Dans le cas d'une interface de type Web Services ou APIs. Elle devra répondre aux standards ci-dessous :

Dans la mesure où elles sont adhérentes aux langages supportés, les standards de la solution GAIA sont le JAVA (1.6) et le C.

L'éditeur fournira donc une interface programmatique permettant de gérer tous les objets de sécurité de son application.

Aucune intervention humaine ne devra être nécessaire pour fournir des droits applicatifs notamment dans l'outil d'administration de l'application à provisionner. Il sera donc possible de :

- Gérer des événements de type :
 - Consultation
 - Création
 - Modification
 - Suppression
 - Désactivation
- Gestion des codes retour sur événements pour faciliter l'exploitation informatique du CHU de Nantes

Les actions de l'interface programmatique devront d'une part pouvoir être journalisées. D'autre part les procédures standard de sécurité interne à l'application devront être

applicables en matière d'authentification du composant (compte de service) comme d'application de permission au(x) compte(s) de service du ou des connecteurs de provisionnement.

En d'autres termes, la connexion par un moyen externe (API ou WS ou autres) devra se faire au travers d'une identité applicative et respecter les permissions de cette identité dans l'application vis-à-vis des objets gérés.

4.4 Vérification et réconciliation des politiques

La solution mise en place à travers son module Policy Manager permet de faire des vérifications d'application de la politique.

En cas d'écarts constatés, il est possible de réconcilier les données à partir de la politique décrite dans le module Policy Manager et donc d'avoir avec certitude une politique appliquée dans les applications telle qu'elle a été décrite.

Pour ce faire, il est indispensable que le module de réconciliation utilise le même connecteur de provisionning pour interroger les données. Cela impose que ce connecteur soit directement connecté aux données contenues dans l'application.

Cette fonctionnalité exclue de fait le provisionning par import de fichiers plats.