

# WEBINAR ENOVACOM

MARDI 15 MARS 2016, 10H00-11H00

**IAM : COMMENT GÉRER LES IDENTITÉS  
UTILISATEURS AU SEIN D'UN GHT ?**



 **enovacom**  
WWW.ENOVACOM.FR

# PRÉSENTÉ PAR :



**SÉBASTIEN WETTER**  
EXPERT SÉCURITÉ,  
RESPONSABLE OFFRE  
CHEZ ENOVACOM

[SWETTER@ENOVACOM.FR](mailto:SWETTER@ENOVACOM.FR)



## L'INNOVATION TOURNÉE VERS VOTRE MÉTIER

Créée en 2002, Enovacom est une société française spécialisée dans l'édition de logiciels d'interopérabilité et de sécurité dans la santé.



### Une société en forte croissance et pérenne :

- Activité et métier historique dans la santé (90 % du CA)
- Lancement **international** 2013

### Une équipe de plus de 100 personnes dédiée au secteur santé

- Une équipe de spécialistes basés en France et à l'international
- Ils s'investissent au quotidien dans les problématiques spécifiques des structures de santé qui demandent un effort d'adaptation important

# Interopérabilité

Dématérialisation  
des échanges

**M**essagerie  
**S**écurisée

EAI

EDI  
ESB

**T**raçabilité

# Sécurité

Authentification forte

Référentiel des identités

Sécurisation  
des accès

**IAM**

SSO



PRATICIENS DE L'ÉTABLISSEMENT  
EN ACCÈS NOMADE



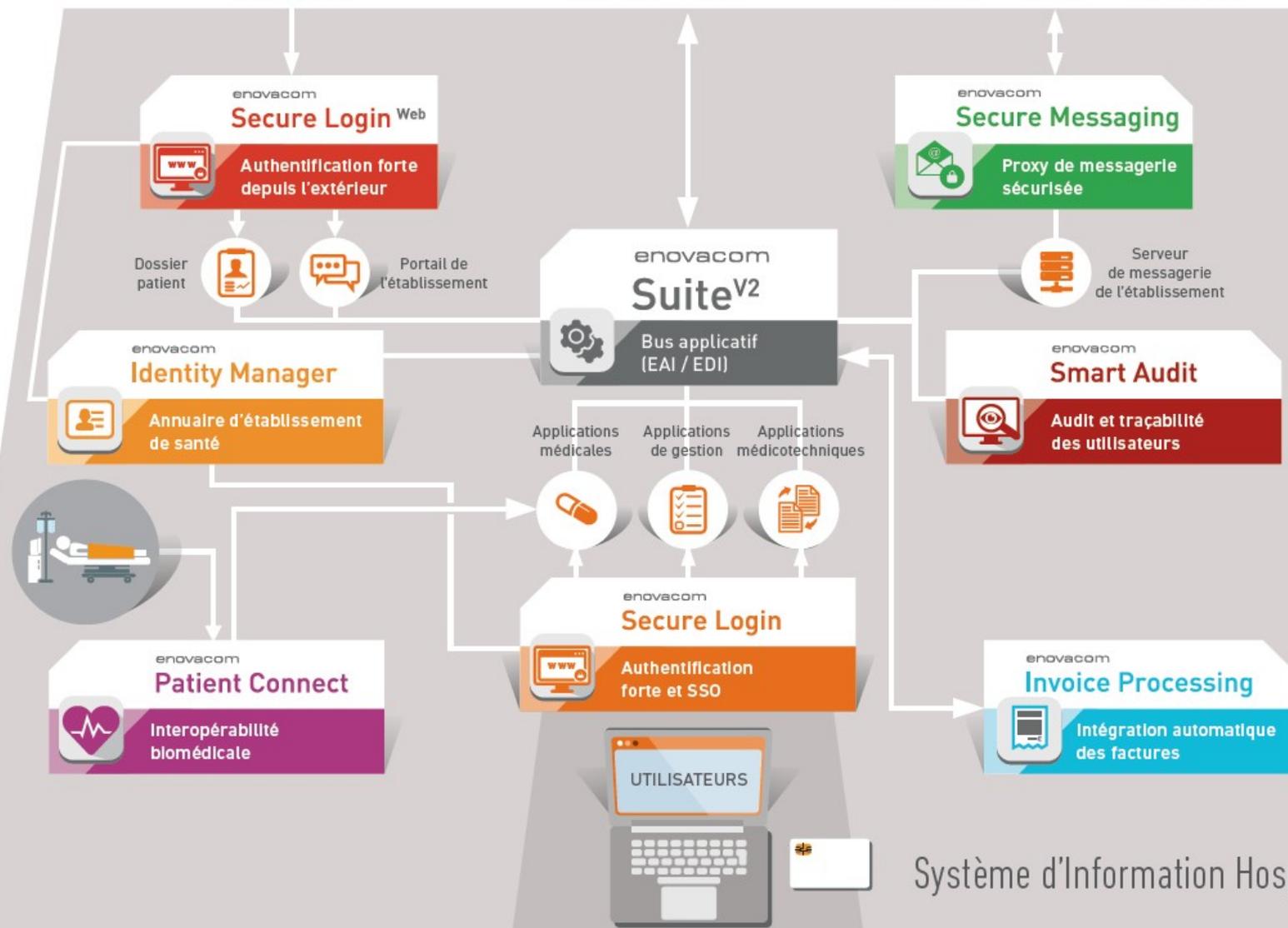
DMP, EFS, LABORATOIRES,  
PRATICIENS, MUTUELLES,...



INSTITUTIONS :  
DGFIP, CPAM,...

MÉDECINE  
DE VILLE

AUTRES  
ÉTABLISSEMENTS



# DANS CE WEBINAR...

- ❑ En plus de toutes les contraintes et exigences déjà bien connues (Hôpital Numérique, certification des comptes, Auditabilité des SI, PGSSI-S,...), les établissements doivent faire face à une nouvelle réglementation : **les Groupements Hospitaliers de Territoire (GHT)**.
  
- ❑ Durant ce webinar, je vous présenterai les concepts de l'IAM mais aussi la capacité de notre offre à s'adapter aux problématiques du regroupement des hôpitaux et à la convergence des systèmes d'informations. **Venez découvrir l'offre IAM d'Enovacom adaptée aux établissements de santé et aux GHT.**

# SOMMAIRE

- ❑ Le contexte réglementaire général
- ❑ L'évolution vers les GHT
- ❑ Les concepts de la gestion des identités
- ❑ Un premier pas vers la convergence des SI
- ❑ Un exemple de cinématique
- ❑ Les concepts de la gestion des accès (eSSO)
- ❑ Les Questions / Réponses



# LE CONTEXTE RÉGLEMENTAIRE GÉNÉRAL



# LE CONTEXTE RÉGLEMENTAIRE

## Hôpital Numérique

Les indicateurs du programme Hôpital Numérique sont déterminants pour l'obtention de la **certification de l'Établissement de Santé**.

Voici la liste des indicateurs Hôpital Numérique touchant à la gestion des identités et des accès :

Existence d'un référentiel unique de structure de l'établissement (juridique, géographique, fonctionnel) piloté et mis à jour régulièrement dans les applicatifs, en temps utile.

**P 1.4**



Taux d'application gérant des données de santé à caractère personnel intégrant un dispositif d'authentification personnelle.

**P 3.4**

Taux d'applications permettant une traçabilité des connexions au SIH.

**P 3.5**

# LE CONTEXTE RÉGLEMENTAIRE

## Certification & fiabilisation des comptes

- ❑ **INSTRUCTION N° DGOS/MSIOS/2013/62** 21 février 2013  
 méthodologique pour l'auditabilité des systèmes d'information dans le cadre de la certification des comptes des établissements publics de santé
  
- ❑ **Guide méthodologique pour l'auditabilité des systèmes d'information**
  - PARTIE 1 : PRESENTATION DE LA DEMARCHE GLOBALE
  - PARTIE 2 : SE PREPARER A L'AUDIT DU SIH
  - PARTIE 3 : FICHES PRATIQUES



# L'ÉVOLUTION VERS LES GHT



# LES GROUPEMENTS HOSPITALIERS DE TERRITOIRE (GHT)

## Outil de coopération renforcée :

- ❑ **Loi Santé** - avril 2015 - Nouvel outil pour intensifier la collaboration entre établissements de santé.
- ❑ **Obligation d'adhésion à un GHT pour tous les établissements publics** - 1<sup>er</sup> Juillet 2016.
- ❑ **En cas de non-respect de cette obligation – 1<sup>er</sup> Janvier 2018** – L'établissement ne sera plus attributaire des dotations MIGAC.



# LES GROUPEMENTS HOSPITALIERS DE TERRITOIRE (GHT)

## Les chantiers à mener :



Constitution du GHT



Le projet Médical Partagé



Identifier les axes de mutualisation

- Transfert de fonctions et d'activités



La gouvernance



Convention  
GHT

# LES GROUPEMENTS HOSPITALIERS DE TERRITOIRE (GHT)

## L'Établissement support assurera :

- ❑ La gestion et l'optimisation d'un SIH convergent
- ❑ La gestion d'un département d'information médicale de territoire
- ❑ La fonction achats
- ❑ La coordination des formations
- ❑ Mise en place des pôles inter-établissements

# LES CONCEPTS DE LA GESTION DES IDENTITÉS



# LES CONCEPTS DE LA GESTION DES IDENTITÉS

## LA PROBLEMATIQUE

- ❑ Multiplication des applications **hétérogènes**.
- ❑ De plus en plus de **référentiels utilisateurs** souvent avec des technologies différentes et **incompatibles**.
- ❑ Augmentation non contrôlée des **charges d'administration et de support**.
- ❑ Difficulté pour contrôler **l'accès aux applications**



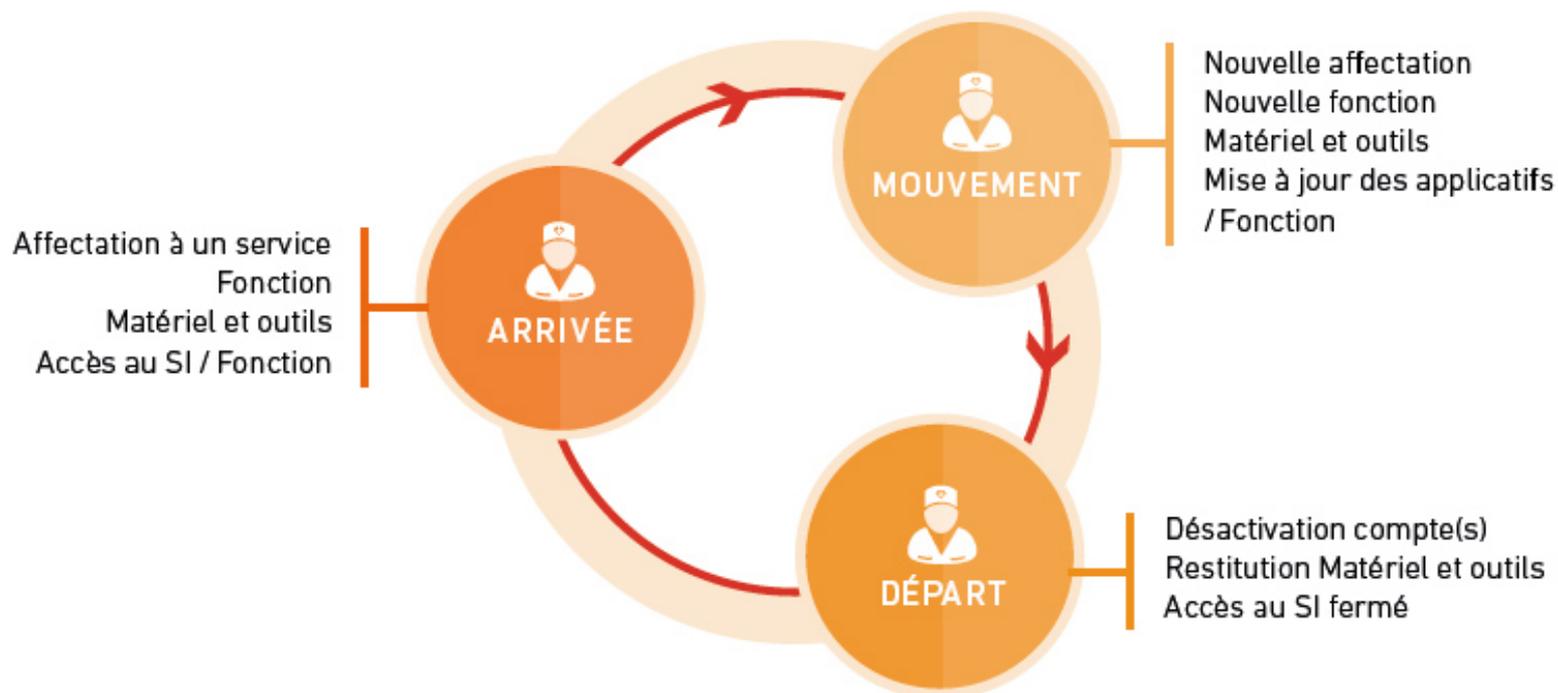
# LES CONCEPTS DE LA GESTION DES IDENTITÉS

Objectif

**« Donner les bons droits d'accès aux bonnes personnes, au bon moment... et les contrôler »**

# LE CYCLE DE VIE DE L'AGENT

Gérez le cycle de vie de votre agent simplement



# UN PREMIER PAS VERS LA CONVERGENCE DES SI



# LA GESTION DES IDENTITÉS UTILISATEURS ADAPTÉE AUX GHT

- ❑ Un référentiel **multi-structures** adaptable et personnalisable aux différents établissements
- ❑ Une intégration des données à partir de **plusieurs sources** (plusieurs logiciels GRH, gestion du temps,...)
- ❑ Une **gestion centralisée** et unifiée des identités et des ressources
- ❑ La **gestion des activités**
  - ❑ des agents et de leurs rattachements
  - ❑ aux différentes structures
- ❑ La **gestion des habilitations**
  - ❑ adaptée pour chaque établissement

enovacom

**Identity Manager**



# SYNTHÈSE DES BESOINS MÉTIERS

enovacom

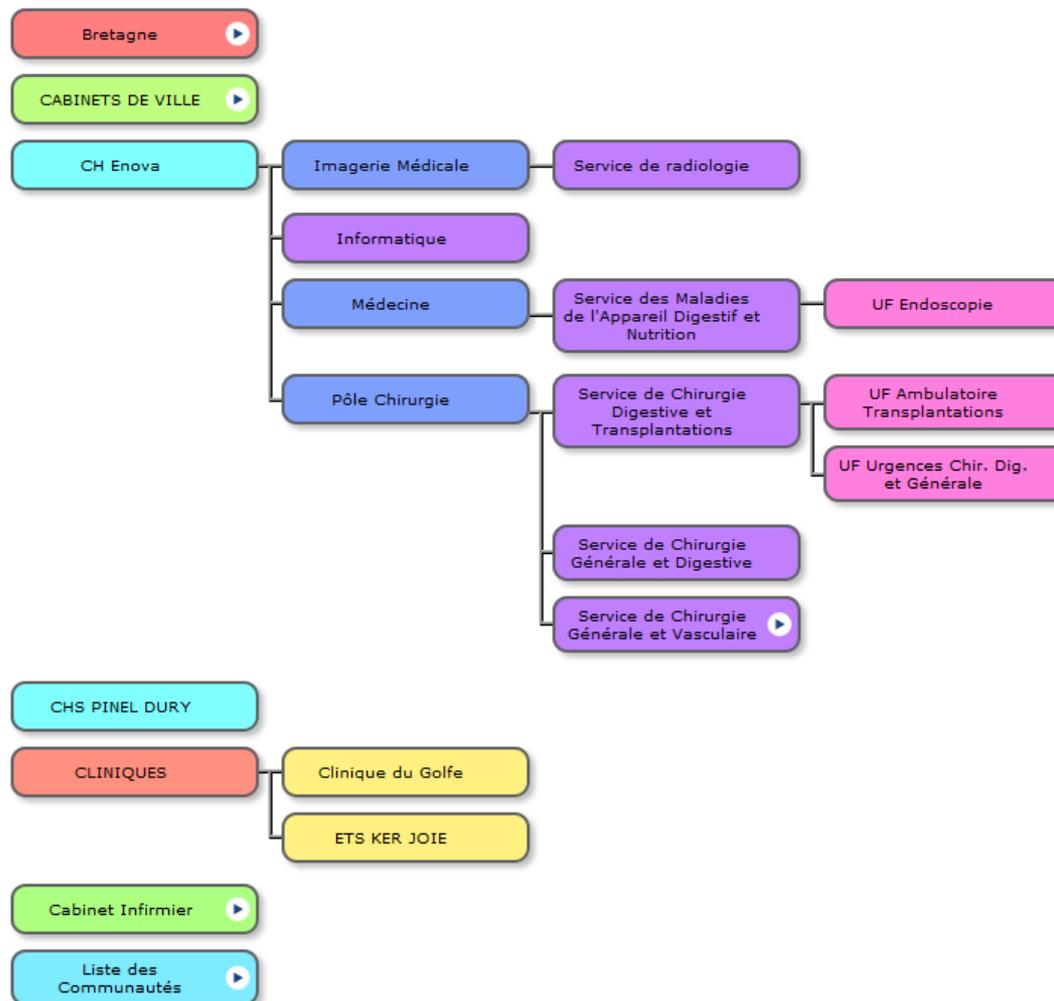
## Identity Manager

- ❑ **Réduire les coûts** en mettant en place une solution automatisant un grand nombre de tâches habituellement effectuées manuellement.
- ❑ **Limiter le risque sécuritaire** en contrôlant les accès utilisateurs ainsi que leurs autorisations sur les différents composants du SI en impliquant le cœur du métier.
- ❑ **Alignement sur les normes réglementaires** : la mise en place de procédures de validation électroniques des demandes.
- ❑ **Améliorer la traçabilité des accès** en fournissant des rapports et une vision temps réel de l'ensemble prérogatives des collaborateurs du groupe à partir d'une plate forme unique.
- ❑ **Conserver l'historique des actions de demande d'habilitations** et de droits afin d'être capable de produire des rapports sur les processus et droits des personnes.

# ORGANISATION MULTI-STRUCTURES

- Structures
- Personnes
- Equipements
- Rôles - Habilitations
- Administration
- Sécurité

## Graphe des structures



# SCHÉMA D'ARCHITECTURE FONCTIONNELLE GHT

## DONNEES SOURCES



Base données RH1



Base données RH2



Annuaire

National, Régional...



Autres

Saisie manuelle , fichiers,...

enovacom

## Identity Manager



Référentiel  
Personnes, structures,...

Moteur de règles  
Rôles, habilitations,...

Connecteurs  
de consolidation



Connecteurs  
de provisioning aval



## APPLICATIONS CIBLES



Active Directory



Dossier Patient1



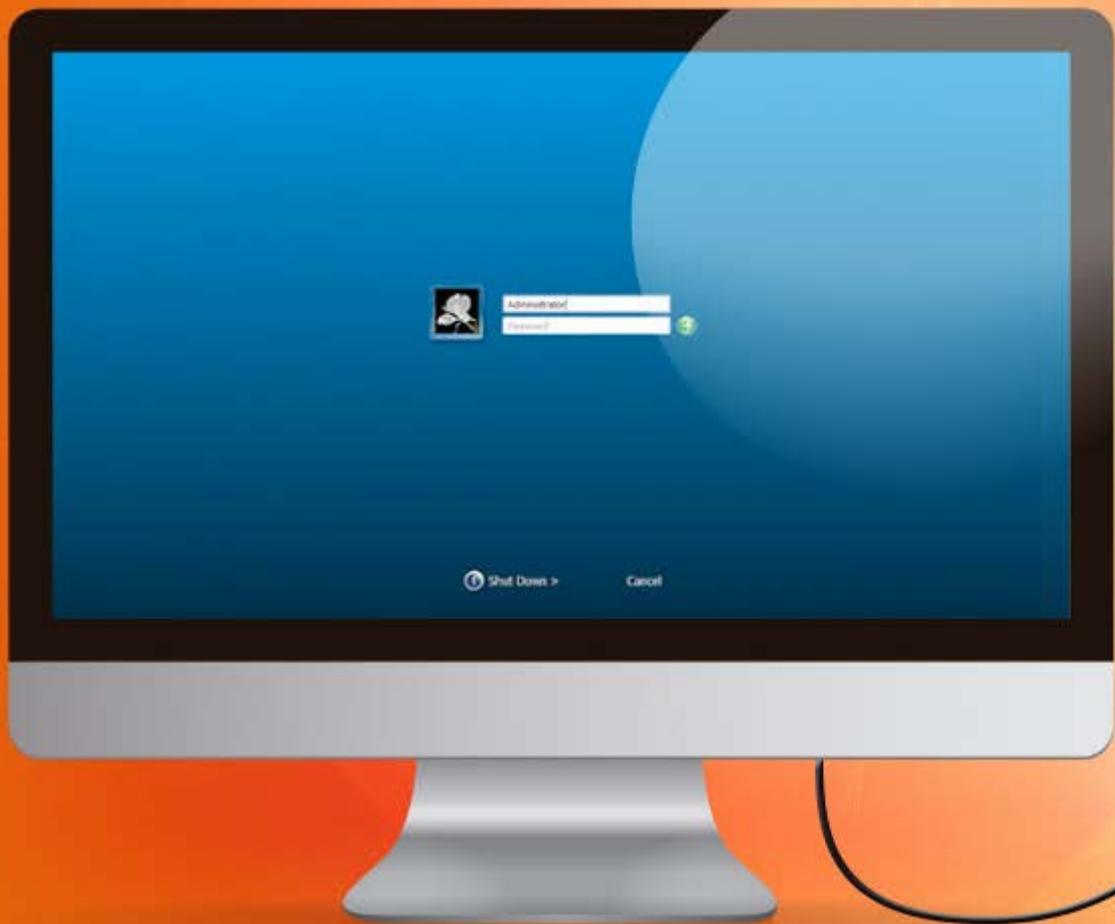
Dossier Patient2



Autres

# LES CONCEPTS DE LA GESTION DES ACCÈS (ESSO)



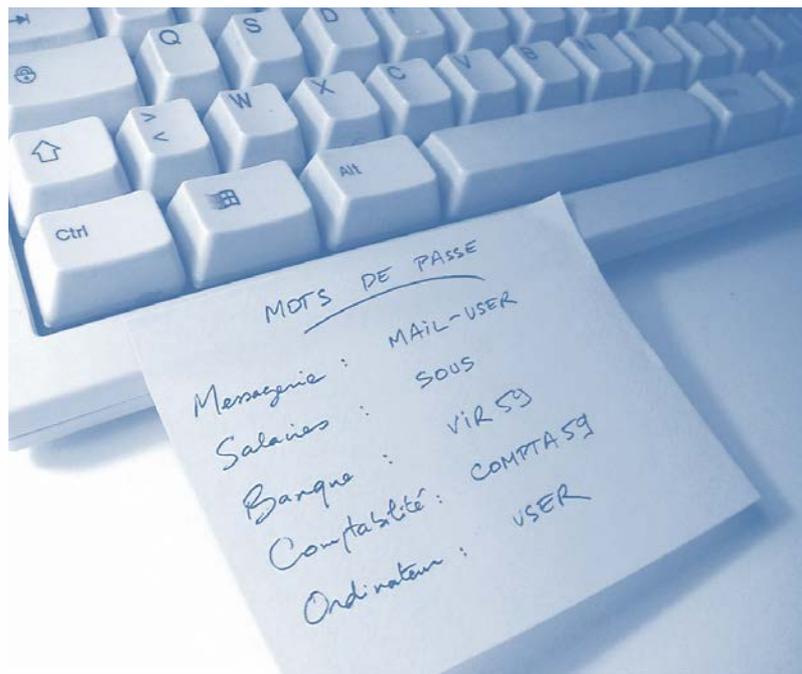


# LES OBJECTIFS D'UNE SOLUTION DE GESTION DES ACCÈS SSO ?

- ❑ **Sécuriser les accès** aux postes de travail et aux SIH
- ❑ **Simplifier et automatiser** l'accès des Professionnels de Santé à leurs applications
- ❑ Répondre aux exigences de **confidentialité**
- ❑ **Faire gagner du temps aux utilisateurs**
- ❑ **Identifier et tracer les utilisateurs**
- ❑ Grâce au module d'audit des connexions



# LE MOT DE PASSE : FAILLE PRINCIPALE DE SÉCURITÉ DU SI



- ❑ Premier point d'entrée sur le Système d'Information
- ❑ 70% des actes malveillants sont d'origine internes
- ❑ La Politique de Formation des mots de passe à l'initiative des administrateurs ou des utilisateurs...
- ❑ Les variétés d'attaques possibles :
- ❑ Attaques directes : force brute, dictionnaire
- ❑ Attaques indirectes : filoutage, keylogger, etc.

**NÉCESSITÉ DE METTRE EN PLACE UN MOT DE PASSE COMPLEXE ET DES PROCÉDURES DE SÉCURITÉ ORGANISATIONNELLES**



# EXEMPLE DE ROBUSTESSE DE MOT DE PASSE

Evaluation de la résistance du mot de passe à différentes attaques brute-force

**ENFANT** : 6 caractères, minuscules.

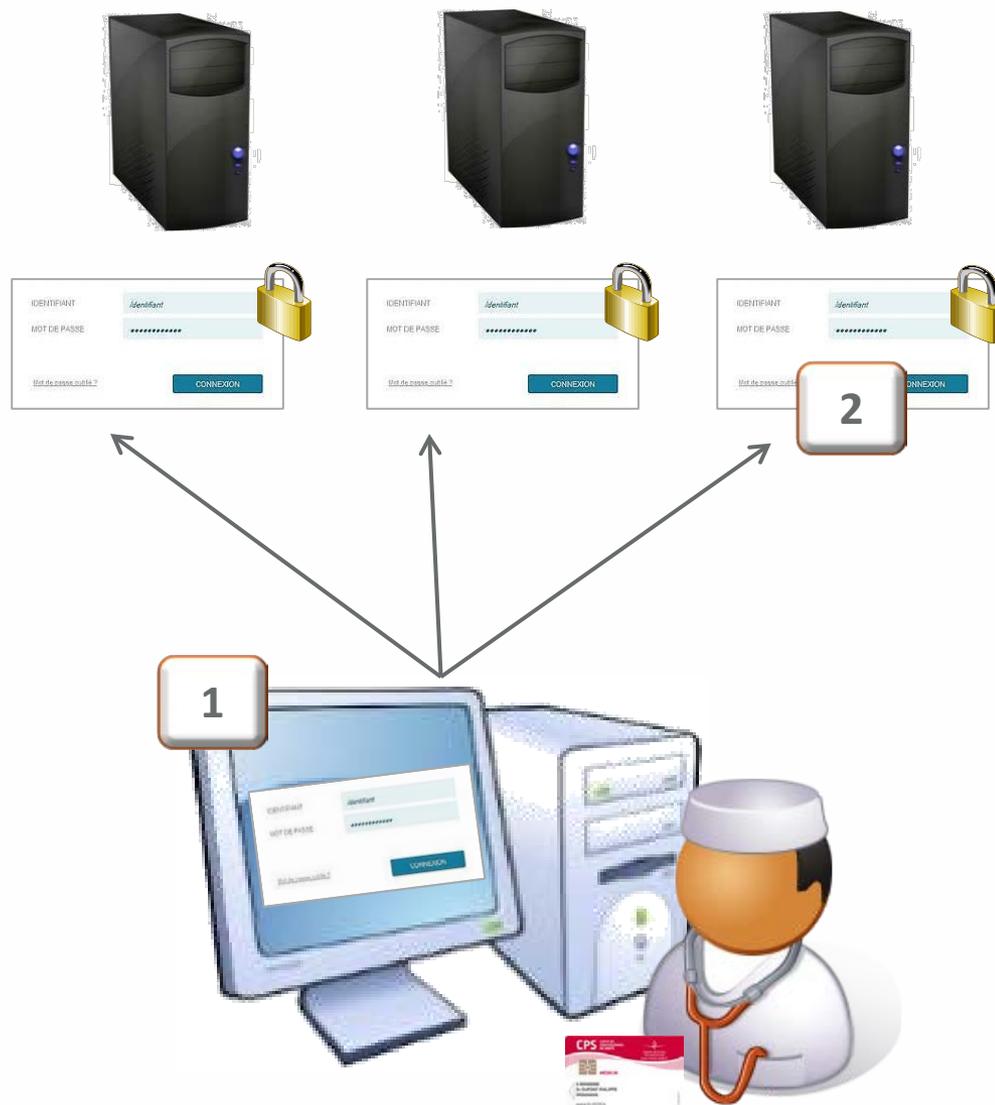
**ght8CD%E7am**

Résistance à une attaque standard		3 JOURS		23 milliards de JOURS 63 millions d'ANNEES 633.187 SIECLES
Résistance à une attaque distribuée		INSTANTANE		9 millions de JOURS 25.327 ANNEES 253 SIECLES
Résistance à une attaque avec l'ordinateur le plus puissant de la planète		INSTANTANE		48 JOURS
Résistance à une attaque utilisant les 500 plus puissants ordinateurs de la planète		INSTANTANE		3 JOURS

# LES APPLICATIONS DU SIH & L'AUTHEMNTIFICATION FORTE

- ❑ 1<sup>ère</sup> « authentification primaire ».
- ❑ Toutes les autres authentifications se font automatiquement.
- ❑ **Possibilité d'authentification forte par carte.**

Les logins et mots de passe sont transmis aux diverses applications et ressources du SI par ENOVACOM Secure Login.



# L'ARCHITECTURE D'ENOVACOM SECURE LOGIN

## ✓ Un composant d'authentification primaire

Il gère l'authentification primaire par carte à puce et permet d'adapter le paramétrage aux différents cas d'usage.

## ✓ Une interface d'enrôlement des cartes à puce

Elle permet de sélectionner le mode d'authentification en sans-contact.

## ✓ Un agent local déployé sur le poste de travail de l'utilisateur

Il permet l'authentification automatique aux applications.

## ✓ Une console d'administration

Elle permet de gérer l'ensemble de la configuration du SSO et la diffusion des modèles d'applications.

## ✓ Un repository

Il contient les caractéristiques des applications intégrées au SSO.



# UTILISATION D'ENOVACOM SECURE LOGIN

## Insertion de la carte CPS



Insérez une carte à puce.  
[Présentation eSSO SmartCard](#)

Changer d'utilisateur



## Saisie du Code PIN de la carte



00B1048756  
 Ouverture de session par carte à puce  
 0.0B1048756@carte-cps.fr

Code confidentiel  

[Présentation eSSO SmartCard](#)

Changer d'utilisateur

# UTILISATION D'ENOVACOM SECURE LOGIN

freemforms - 0.8.2 / WETTER Sebastien

Search by Name (press Alt up/down cursor to cycle)

Mister	MICHU	Robert	01 02 1956	Grande rue Paris 75000 France
--------	-------	--------	------------	-------------------------------

Mister MICHU Robert - 57 year(s) 11 month(s) 1 days  
Grande rue Paris 75000 France

EASYCRYPT.net

Boîte de réception | Nouveau | Dossiers | Recherche | Récupération du courrier | Options

État du quota : 0,11 Mo / 100,00 Mo (0,11%)

Boîte de réception (1)

Sélectionner: [v] Marquer comme: [v] Déplacer | Copier | Messages à

Supprimer | Liste blanche | Imprimer la liste

	N°	Date	De	Sujet [Enfajade]
<input type="checkbox"/>	1	19.07.2013	WebMail Easycrypt	Bienvenue sur Easycrypt.net
<input type="checkbox"/>	2	12.11.2013	À: sebastien.wetter@easy test	

orangeHRM

Admin | HR | Leave | Time | Recruitment | Performance | My info

Configuration | Employees List | Add Employee | Reports

Employee information

Employee Name: M | Employment Status: Includes

Support Case Operations | Agent Performance | Contract Performance | Customer Accounts

Case History - Cases entered/closed by week

Case Mean Time To Resolve (in Days) by week

Open Case Aging by Priority

Case TTR for past 30 days by Priority

Case Priority: Low, Medium, High

Case Reason: Breakdown Installation, Other, Performance

Case Origin: Email, Internet

Top Ten Customers: Wunderwerk, General Doctors Clinica, Japan Barista Importers, Appassion Regional National, Patis Patis S&A, Semp Medical, Gant Tech Conglomerates, Swiss Chocolate Co., Estrop de Mexico, Tulle Tulle Co.



## EN SAVOIR PLUS...

**Besoin d'informations supplémentaires sur notre offre IAM ?**



[info@enovacom.fr](mailto:info@enovacom.fr)

[www.enovacom.fr](http://www.enovacom.fr)

521 avenue du Prado

BP 80 186

13268 Marseille

Tél : + 33 (0) 4 86 670 000

# Retrouvez la rubrique REPLAY

[WWW.ENOVACOM.FR/RESSOURCES/REPLAYS.HTML](http://WWW.ENOVACOM.FR/RESSOURCES/REPLAYS.HTML)

- VISIONNEZ À NOUVEAU CE WEBINAR EN REPLAY,
- N'HÉSITÉZ PAS À PARTAGER L'INFORMATION !



**PROCHAIN WEBINAR LE 22 MARS 2016**  
MSSanté : Partager l'information  
en toute sécurité



[EVENEMENT@ENOVACOM.FR](mailto:EVENEMENT@ENOVACOM.FR)

Merci de votre participation !  
Suivez notre actualité sur :



@enovacom\_fr / #enovacom



Enovacom



[EVENTEMENT@ENOVACOM.FR](mailto:EVENTEMENT@ENOVACOM.FR)