



GUIDE ABRÉGÉ

Répondre aux exigences françaises d'identité numérique et au niveau de garantie substantiel d'eIDAS avec Imprivata Enterprise Access Management (EAM)





Les établissements de santé de l'Union européenne commencent à mettre en œuvre des cadres nationaux d'identité numérique qui renforcent les exigences d'authentification pour l'accès aux données de santé à caractère personnel. En France, cette évolution conduit progressivement les établissements hospitaliers à déployer des solutions permettant une authentification à deux facteurs (2FA) conforme au RIE, la prise en charge de normes modernes de fédération d'identité et l'intégration aux services nationaux d'identité numérique du secteur de la santé.

Imprivata propose aux établissements de santé des fonctionnalités d'identification, d'authentification et de fédération afin de les aider à répondre à ces nouvelles exigences. Chaque établissement demeure toutefois responsable de sa propre conformité et peut être amené à mettre en œuvre des processus opérationnels, de gouvernance et de vérification initiale de l'identité qui ne relèvent pas du périmètre des produits Imprivata.

Depuis un an et demi, Imprivata améliore sa solution EAM afin de répondre aux objectifs spécifiques du programme HospiConnect :

1. Déployer une authentification forte répondant aux exigences du niveau de garantie substantiel du règlement eIDAS ;
2. Simplifier l'accès aux applications locales grâce à l'authentification unique et, le cas échéant, à la fédération d'identité OIDC (OpenID Connect) ;
3. Connecter les professionnels de santé aux services nationaux par l'intermédiaire de Pro Santé Connect.

Ce document présente les mesures concrètes que les établissements de santé français peuvent mettre en œuvre pour progresser vers la conformité avec Imprivata EAM, tout en offrant à leurs équipes un accès efficace aux postes de travail partagés, aux applications locales et aux services de santé nationaux.

Comprendre les exigences de conformité

Les établissements de santé ne peuvent pas se contenter de déployer une authentification multifacteur. Ils doivent déterminer en toute confiance :

- Qui est la personne qui se connecte ;
- Comment elle s'est enregistrée ;
- Quel dispositif d'authentification lui est associé ;
- Comment le niveau de sécurité de l'authentification est communiqué aux applications ;
- Comment s'effectue l'accès aux services de santé locaux et nationaux.

Pour qu'une stratégie soit conforme, elle doit donc répondre aux exigences suivantes :

- Des processus de vérification d'identité efficaces,
- Une authentification forte,
- Une fédération d'identité sécurisée,
- Capacités d'audit et de traçabilité,
- Un alignement sur les cadres nationaux d'identification du secteur de la santé.

Si Imprivata EAM prend en charge plusieurs de ces exigences techniques, certaines responsabilités incombent toujours aux établissements, parmi lesquelles la politique de vérification d'identité initiale, les processus RH ou encore la conservation des dossiers de vérification d'identité.

1er pilier : enregistrer et authentifier efficacement le personnel

Objectif

S'assurer que le personnel s'enregistre et s'authentifie au moyen de méthodes conformes au RIE, notamment en respectant au minimum les exigences du niveau de garantie substantiel du règlement eIDAS.



Méthode conseillée

Étape 1 : superviser l'enregistrement

Les établissements doivent superviser l'enregistrement de chaque membre du personnel de santé.

Pendant l'enregistrement :

- La vérification d'identité doit respecter la politique de l'établissement.
- L'enregistrement doit s'effectuer en présence d'une personne habilitée.
- Les dossiers de vérification d'identité doivent être conservés par l'établissement.

Imprivata EAM fournit les flux de travail d'enregistrement et les fonctionnalités d'association d'identifiant nécessaires pour mener à bien cette étape.

Étape 2 : associer chaque membre du personnel à un dispositif d'authentification forte

Une fois la personne enregistrée, l'établissement doit l'associer à un dispositif permettant une authentification forte.

Voici quelques exemples de dispositifs :

- Les solutions sécurisées par badge FIDO2 ou MIFARE DESFire ;
- Les divers mécanismes agréés tels que les clés d'accès et l'application Imprivata ID.

L'objectif : s'assurer que le dispositif d'authentification est associé de manière unique à la personne vérifiée.

Choisir une méthode d'authentification adaptée

Il existe différentes méthodes d'authentification selon le flux de travail clinique, le type d'appareil, l'application et le niveau de garantie demandé. En effet, le niveau de sécurité n'est qu'un des éléments à prendre en considération, avec la fréquence d'authentification, le partage d'appareils et la rapidité de connexion lors des changements de poste de travail ou d'application.

Imprivata EAM prend en charge plusieurs méthodes d'authentification au sein d'un cadre d'accès commun. Les établissements peuvent ainsi choisir les dispositifs d'authentification adaptés aux flux de travail sur site et à distance, tout en garantissant l'homogénéité de leur politique d'authentification et de l'accès à l'ensemble des services de santé locaux et nationaux.

Méthodes d'authentification prises en charge par Imprivata EAM :

Méthode d'authentification	Flux de travail adapté	Poste de travail partagé / sur site	Accès à distance	Principaux enjeux
Badge MIFARE DESFire	Accès très fréquent à des appareils partagés	Parfait pour un accès rapide et sécurisé	Pas le cas d'usage principal	Lorsque l'établissement gère les badges, leur remplacement est rapide. La configuration doit assurer le niveau de garantie demandé.
Dispositif d'authentification FIDO2	Authentification forte sans mot de passe prenant en charge l'accès très fréquent des membres du personnel soignant aux appareils partagés et leur accès national	Solution la plus efficace pour fluidifier l'accès par badge	Possible selon le dispositif d'authentification et l'appareil	Le dispositif d'authentification, l'enregistrement, l'association d'identité et l'implémentation doivent correspondre au niveau de garantie demandé.
Imprivata ID	Authentification mobile forte vérifiée via deux canaux de communication distincts	Utile lorsque l'authentification mobile est adaptée au flux de travail	Parfaitement adaptée aux flux de travail à distance agréés en mode push	La disponibilité des téléphones mobiles, la politique relative aux appareils et la facilité d'utilisation doivent être prises en considération. Une procédure d'enregistrement, d'association d'identité et d'implémentation est nécessaire.
CPS / eCPS	Liaison d'identité initiale aux services nationaux et flux de travail Pro Santé Connect (PSC)	Les flux de travail avec CPS peuvent nécessiter des interactions supplémentaires avec le personnel.	Dépend du flux de travail PSC	Concerne le processus de liaison d'identité initiale aux services nationaux décrits dans ce guide. À distinguer de l'authentification au quotidien avec Imprivata EAM.

Le dispositif d'authentification n'est qu'une première étape. Une fois que la personne s'est authentifiée de façon sécurisée via Imprivata EAM, elle accède aux applications locales au moyen de l'authentification unique (SSO) ou de la fédération OIDC. Elle accède aussi aux services de santé nationaux via Pro Santé Connect en fonction de la liaison d'identité effectuée. Cela évite de créer une expérience d'authentification distincte pour chaque application.



Enjeux cliniques et opérationnels

- Postes et appareils partagés : privilégier les méthodes qui réduisent le nombre d'étapes d'authentification manuelles à répéter à chaque changement de poste de travail.
- Cycle de vie des moyens d'authentification : prévoir des procédures permettant de révoquer et de remplacer rapidement les dispositifs perdus ou endommagés afin de permettre une reprise rapide du travail.
- Accès à distance : choisir une méthode d'authentification forte approuvée et adaptée aux usages pour lesquels les badges ne peuvent pas être utilisés.
- Niveau de garantie : celui-ci dépend non seulement de la technologie, mais également de l'enregistrement, de l'association de l'identité, de la politique d'authentification et de la mise en œuvre.

Étape 3 : mettre en œuvre l'authentification multifacteur

L'accès aux données de santé protégées nécessite une authentification multifacteur forte répondant aux exigences du niveau de garantie substantiel du règlement eIDAS.

Avec Imprivata EAM, les établissements de santé peuvent :

- Mettre en œuvre une politique d'authentification multifacteur ;
- Prendre en charge des flux de travail avec authentification forte ;
- Garantir une expérience d'utilisation adaptée au personnel soignant ;
- Prendre en charge les exigences de réauthentification, le cas échéant ;
- Disposer d'un dossier d'audit complet des accès de chaque membre du personnel.

Résultat

Avant tout accès à des informations sensibles, la vérification des membres du personnel de santé est garantie par le niveau de sécurité élevé de leur enregistrement, l'association avec un dispositif d'authentification de confiance et l'authentification multifacteur.

2e pilier : fédérer l'accès aux applications locales

Objectif

Offrir un accès sécurisé, simplifié et sans mot de passe aux applications de santé locales grâce à une méthode d'accès adaptée à chaque application et flux de travail.

En règle générale, les établissements de santé disposent d'un ensemble d'applications hétérogène : services fédérés modernes, applications Web, environnements virtuels et anciennes applications cliniques nécessitant toujours des identifiants et des mots de passe.

L'approche HospiConnect incite à adopter des modèles centralisés d'identification et de fédération lorsque cela se justifie, sans imposer la migration de chaque application ou cas d'usage vers OIDC.

Méthode conseillée

Imprivata EAM doit localement faire office d'autorité d'authentification et de couche d'accès. La fédération OIDC est quant à elle réservée aux applications modernes qui l'acceptent, tandis que les méthodes d'authentification unique prises en charge peuvent étendre l'expérience utilisateur authentifiée aux applications locales et anciennes ne relevant pas de la migration vers OIDC.

Ses avantages :

- Politique d'authentification centralisée,
- Mise en œuvre homogène de l'authentification multifacteur,
- Moindre dépendance aux mots de passe,
- Auditabilité optimisée,
- Meilleure expérience utilisateur

Procédure à mettre en place

1. Identifier les applications contenant des informations de santé personnelles et cartographier les flux de travail cliniques qui y accèdent.
2. Segmenter les applications par méthode d'accès : prioriser la fédération OIDC lorsqu'elle est prise en charge et choisir des méthodes d'authentification unique adaptées avec Imprivata EAM pour les applications locales ou anciennes, en utilisant soit l'intégration via des API, soit le profilage des applications.
3. Configurer Imprivata EAM en tant qu'autorité d'authentification locale et appliquer une politique d'authentification homogène sur l'ensemble des applications prises en charge.

4. S'assurer que le niveau de sécurité est communiqué via les demandes de fédération. Cette exigence est déjà couverte par les fonctionnalités Imprivata Web SSO, la transmission s'effectuant au moyen de valeurs ACR/AMR dans les demandes.
5. Réduire tant que possible l'authentification par mot de passe dans les applications, tout en conservant la méthode d'accès demandée par celles encore exclues de la fédération.

Résultat

En s'authentifiant via Imprivata EAM, le personnel bénéficie d'une expérience d'accès homogène sur toutes les applications locales, soit grâce à la fédération basée sur des normes, lorsqu'elle est disponible, soit au moyen des méthodes d'authentification unique prises en charge.

3e pilier : se connecter à Pro Santé Connect

Objectif

Permettre au personnel de santé d'accéder en toute sécurité aux services de santé nationaux via Pro Santé Connect (PSC).

Méthode conseillée

Imprivata EAM agit localement comme fournisseur d'identité fédérée et comme fournisseur délégué d'accès aux applications et données nationales, tandis que Pro Santé Connect joue toujours le rôle d'autorité de confiance au niveau national.

Liaison d'identité initiale

Dans un premier temps, avant que l'accès fédéré soit possible, la liaison doit être établie entre les membres du personnel soignant et leur identité sur le système national de santé.

Cette étape initiale s'effectue sur Pro Santé Connect avec un moyen d'identification adapté, à savoir :

- Une carte CPS
- Ou l'identifiant d'une carte e-CPS.

La liaison d'identité nationale étant gérée par Pro Santé Connect, Imprivata EAM intervient une fois la procédure effectuée.

La liaison d'identité initiale n'est pas synonyme d'expérience d'authentification au quotidien

Liaison initiale : chaque membre du personnel de santé suit la procédure sur Pro Santé Connect pour établir le lien avec son identité nationale, en utilisant sa carte CPS physique ou dématérialisée, selon le cas.

Accès au quotidien : une fois la liaison établie, l'authentification s'effectue par le biais d'Imprivata EAM et d'un dispositif d'authentification forte adapté. Ensuite, Imprivata EAM fournit les informations d'authentification à Pro Santé Connect, limitant ainsi la nécessité de présenter sans arrêt sa carte à puce.

Accès national fédéré

Une fois la liaison d'identité effectuée, les membres du personnel bénéficient au quotidien d'un accès fédéré, sans devoir présenter sans arrêt leur carte à puce :

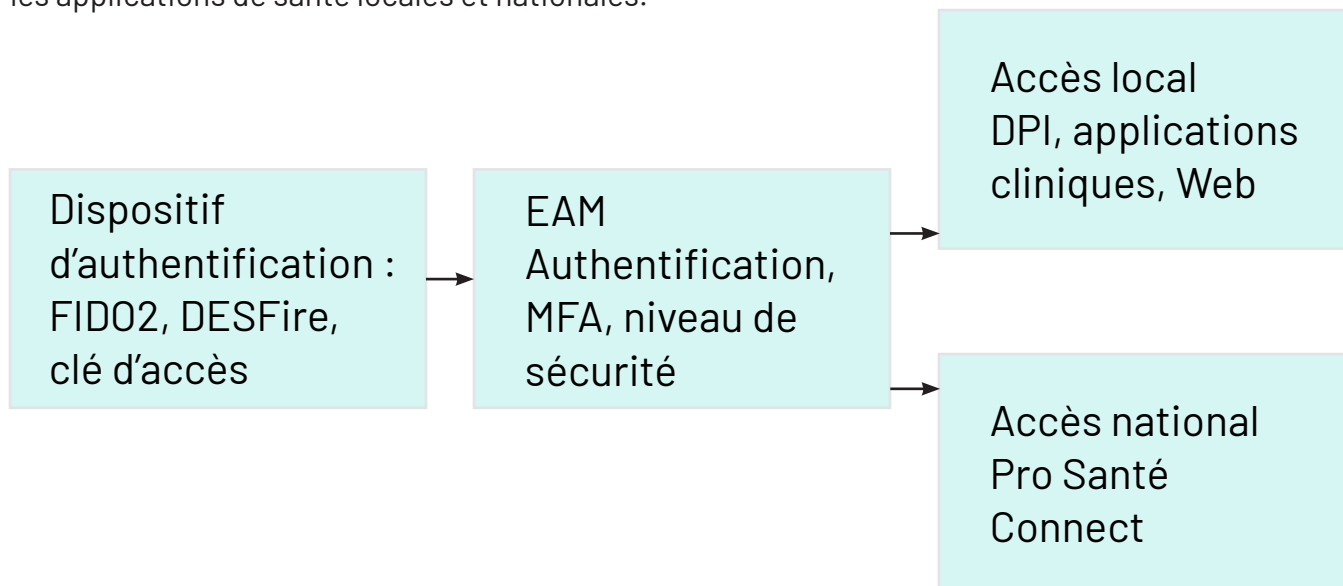
1. L'authentification s'effectue par le biais d'Imprivata EAM, avec des dispositifs d'authentification adaptés.
2. Imprivata fournit à Pro Santé Connect la preuve de l'authentification et son niveau de sécurité.
3. Les demandes d'accès fédéré sont transmises à Pro Santé Connect.
4. Les membres du personnel bénéficient d'un accès aux services de santé nationaux sans devoir présenter sans arrêt leur carte à puce.

Principaux enjeux

- Pro Santé Connect reste l'autorité qui fournit les identités au niveau national.
- Les établissements hospitaliers demeurent responsables de la gouvernance des identités au niveau local.
- Imprivata fournit le cadre de fédération et d'authentification servant de passerelle entre accès locaux et nationaux.

Résultat

Le personnel bénéficie d'une expérience d'authentification homogène et sécurisée, à la fois sur les applications de santé locales et nationales.



Matrice des responsabilités

Responsabilité	Établissement de santé	Imprivata EAM
Vérification de l'identité	✓	
Conservation des dossiers de preuve d'identité	✓	
Gouvernance de l'enregistrement	✓	
Enregistrement avec authentification forte	✓	✓
Mise en œuvre de l'authentification multifacteur		✓
Flux de travail d'authentification		✓
Fédération OIDC		✓
Composant IdP local		✓
Intégration avec Pro Santé Connect		✓
Gestion d'identité au niveau national		Effectuée par PSC
Conformité réglementaire	✓	

Prochaines étapes recommandées

Les établissements souhaitant respecter les exigences d'identification numérique au niveau national doivent :

1. Mettre en place des procédures d'enregistrement supervisé.
2. Vérifier et documenter l'identité du personnel.
3. Associer les membres du personnel à des dispositifs d'authentification forte adaptés aux appareils partagés et dédiés, ainsi qu'aux flux de travail à distance.
4. Déployer une politique d'authentification multifacteur répondant aux exigences du niveau de garantie substantiel du règlement eIDAS.
5. Fédérer l'accès avec OIDC aux applications locales qui l'acceptent et étendre l'authentification unique avec EAM aux applications prises en charge nécessitant d'autres méthodes d'accès.
6. Mener à bien la procédure de liaison d'identité demandée par Pro Santé Connect pour permettre ensuite l'accès fédéré au niveau national par le biais d'Imprivata EAM.
7. Examiner la politique de l'établissement en matière d'auditabilité, de gestion d'identité et de conservation des dossiers.

Adopter cette méthode permet aux établissements d'utiliser Imprivata EAM comme socle d'une architecture d'identité moderne prenant en charge à la fois les accès locaux et nationaux, tout en progressant vers l'atteinte de leurs objectifs de conformité.



Imprivata est un éditeur de logiciels spécialisé dans l'identité numérique, l'authentification et la gestion des accès pour les organisations des secteurs critiques. L'entreprise redéfinit la manière dont ces organisations résolvent les défis complexes liés aux workflows, à la sécurité et à la conformité, grâce à des solutions qui protègent les données et applications critiques sans perturber les flux de travail. Sa plateforme de solutions interopérables de gestion de l'identité, d'authentification et d'accès permet à des organisations, dans plus de 45 pays, de gérer et de sécuriser entièrement toutes les identités numériques – internes comme tierces – en établissant la confiance entre les personnes, la technologie et l'information.

Pour plus d'informations, veuillez nous contacter au :

Siège social mondial aux États-Unis

Waltham, MA
Tél. : +1 877 663 7446
www.imprivata.com

Siège social européen

Uxbridge, Royaume-Uni
Tél. : +44 (0) 208 744 6500
www.imprivata.com/uk

France

Tél. : +33 (0) 1 84 88 00 15
E-mail : contactfrance@imprivata.com
www.imprivata.com/fr

Allemagne

Langenfeld
Tél. : +49 (0) 2173 99 385 0
www.imprivata.com/de

Copyright © 2026 Imprivata, Inc. Tous droits réservés. Imprivata est une marque déposée d'Imprivata, Inc. aux États-Unis et dans d'autres pays. Toutes les autres marques appartiennent à leurs propriétaires respectifs.