AUTHENTIFICATION EN SANTE

White Paper

Document v.2.0

Mars 2022

Statut du document	Validé
Code	DP04
Version	v.2.0
Date d'enregistrement	13/03/2023
Responsable du document	MK
Service	Document Marketing
Titre	Livre Blanc – Authentification en Santé

Table des matières

Table des figures

1 Les accés au SIH

1.1 Un contexte global de vigilance

La protection des données est une obligation pour toutes les entreprises et organisations. Les menaces informatiques sont variées et redoutables d'efficacité. Toutes les études arrivent à la même conclusion : les établissements de santé sont de plus en plus la cible de piratage. Selon le baromètre établi par le FIC (Forum International de la Cybersécurité), les entreprises publiques et privées ont été largement ciblées par les organisations pirates, engendrant des violations de données en hausse de 20% en 2020[1]. Selon Cyberpeace Institute, plus de 380 attaques par rançongiciel visant le secteur de la santé ont été recensées au cours des deux dernières années...

Conscientes de cette situation, les instances ministérielles, au travers des agences nationales, comme l'Agence du Numérique en Santé (ANS), imposent de nouvelles règlementations de sécurité aux établissements de santé, impliquant outils, procédures et ressources humaines - *PPT : People, Process & Technology*.

Plus précisément, les établissements de santé doivent, non seulement prendre en compte les **préconisations de l'ANSSI** – Agence Nationale de Sécurité des Systèmes d'Informations, mais surtout se mettre en conformité avec le **référentiel d'identification des personnes physiques** et morales, faisant force de loi au travers de l'arrêté de mars 2022.

Figure 1 : La double réglementation des établissements de santé

1.2 La sécurité les accès au SIH

Par définition, le *« système d'information Hospitalier » (SIH) est un ensemble organisé de ressources sociales et techniques, qui permet de collecter, stocker, traiter et distribuer l'information des établissements de santé.*

[1] Infographie sur le Baromètre Data Breach réalisé par le FIC 2021

Les Directions des Systèmes d'Information (plus particulièrement les Responsables Sécurité des Systèmes d'Informations – RSSI) ont pour mission de sécuriser les accès aux SIH. Cette mission est essentielle pour la préservation et le respect de la confidentialité des données, tout en contribuant directement à la productivité des établissements.

La sécurité informatique est souvent associée à la notion de contrainte. Cette situation est liée au fait qu'elle repose généralement sur la limitation des droits des utilisateurs dans le système SIH et le contrôle des accès. **Cependant, la sécurité ne doit pas être un frein à l'efficacité des utilisateurs, particulièrement dans des secteurs critiques comme la santé.**

> Trouver l'équilibre entre protection des données et facilité d'usage.

Pour être efficace, la sécurité doit couvrir l'ensemble de la chaine d'accès aux ressources. A ce stade, il est nécessaire de distinguer deux niveaux d'accès au SIH :

- L'accès à l'environnement de travail, matérialisé par l'ouverture d'une session de travail depuis un périphérique relié au domaine de l'entreprise ou distant ;
- L'accès à des services numériques comme des applications, logiciels ou ressources ;

Dans la suite de ce document, nous traiterons donc de la sécurité des accès en utilisant les désignations suivantes :

- **Authentification Primaire** : l'authentification des utilisateurs lors de l'accès à leur environnement de travail – ouverture de session ;

- **Authentification Secondaire** : l'authentification des utilisateurs pour l'accès aux ressources logicielles ou services numériques ;

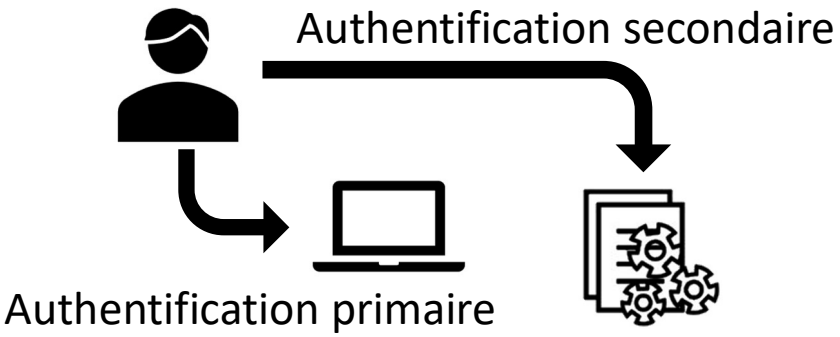


Figure 2 : Différencier l'authentification primaire et secondaire

1.3 Évolution des Systèmes d'Informations Hospitaliers

Depuis les années 90, les acteurs de la santé ont identifié la nécessité de faciliter et fiabiliser le partage d'informations, et d'améliorer la qualité des données nécessaires à l'organisation de l'offre de soins. En conséquence, le système d'information de santé a vu naitre deux évolutions majeures :

- Un référentiel commun de données certifiées et actualisées : RPPS - Répertoire Partagé des Professionnels de Santé ;
- L'identification des Professionnels de Santé par l'attribution d'un numéro unique et attribué à vie.

En 1996, le GIP CPS a lancé la **carte de professionnel de santé**, dite « carte CPS ». Cette carte d'identité professionnelle électronique stocke de manière sécurisée les données d'identification de son porteur, mais aussi ses situations d'exercice. Elle constitue le maillon initial d'une chaine de confiance qui permet à son titulaire d'attester de son identité et de ses qualifications.

En 2007, le '**décret de confidentialité'** modifie le code de la santé publique (CSP), imposant notamment aux professionnels de santé de s'authentifier avec leur carte CPS, avant de pouvoir accéder aux informations médicales stockées dans tout système d'informations de santé.

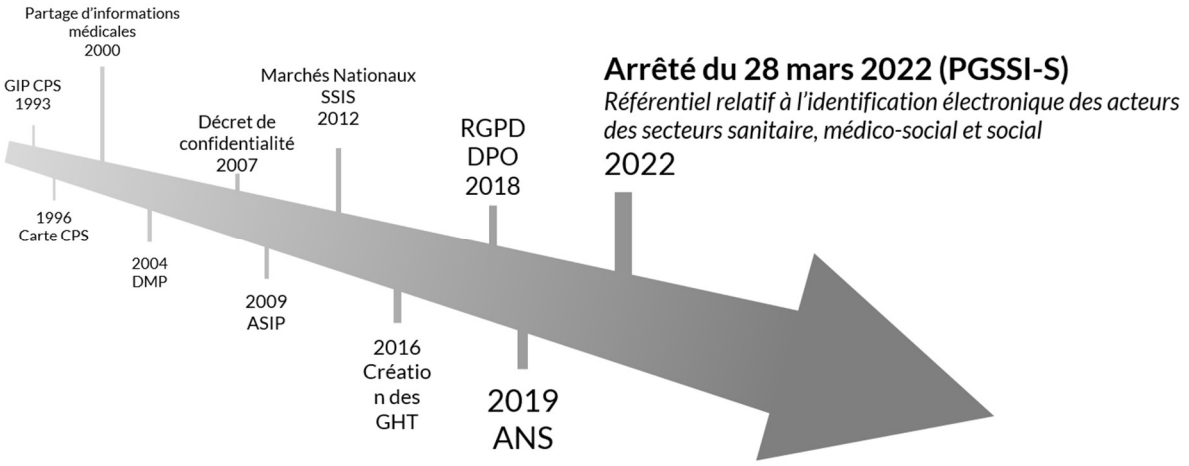


Figure 3 - Evolutions des obligations de sécurité des SI pour les établissements de santé

En 2022, l'ANS a actualisé les exigences de sécurité dans les établissements de santé. Le « référentiel d'identification électronique », rendu opposable par arrêté ministériel, engage la responsabilité légale de l'établissement – « **Arrêté du 28 mars 2022 portant approbation du référentiel relatif à l'identification électronique des acteurs des secteurs sanitaire, médico-social et social, personnes physiques et morales, et à l'identification électronique des usagers des services numériques en santé** ».

Le référentiel d'identification électronique (RIE), dans sa dénomination courte, définit les exigences minimales relatives à l'authentification des acteurs du secteur de la santé pour l'accès aux services numériques dits "sensibles", au sens de l'article du L. 1470-1 du code de la santé publique, et qui appartiennent au moins à l'une des catégories suivantes :

- Services partagés, (territoire ou au niveau national) (ex : dossier médical partagé, pharma...) ;
- Services numériques qui intègrent des services partagés ;
- Services proposant un accès web externe aux SI ;
- Services non partagés mais qui intègrent des traitements ou des accès de grande échelle :
    - > 10 000 patients / par an ;
    - > 1 000 professionnels / par an ;

En résumé, le référentiel d'identification des personnes physiques concerne l'ensemble des acteurs du domaine de la santé. **Ces exigences s'imposent à la quasi-totalité des Centres Hospitalier, CHU, CHR, Cliniques, CLCC**.

1.4 L’agenda du référentiel d’identification des personnes physiques

L’arrêté de mars 2022 définit non seulement les exigences de sécurité, mais également le calendrier de mise en œuvre.

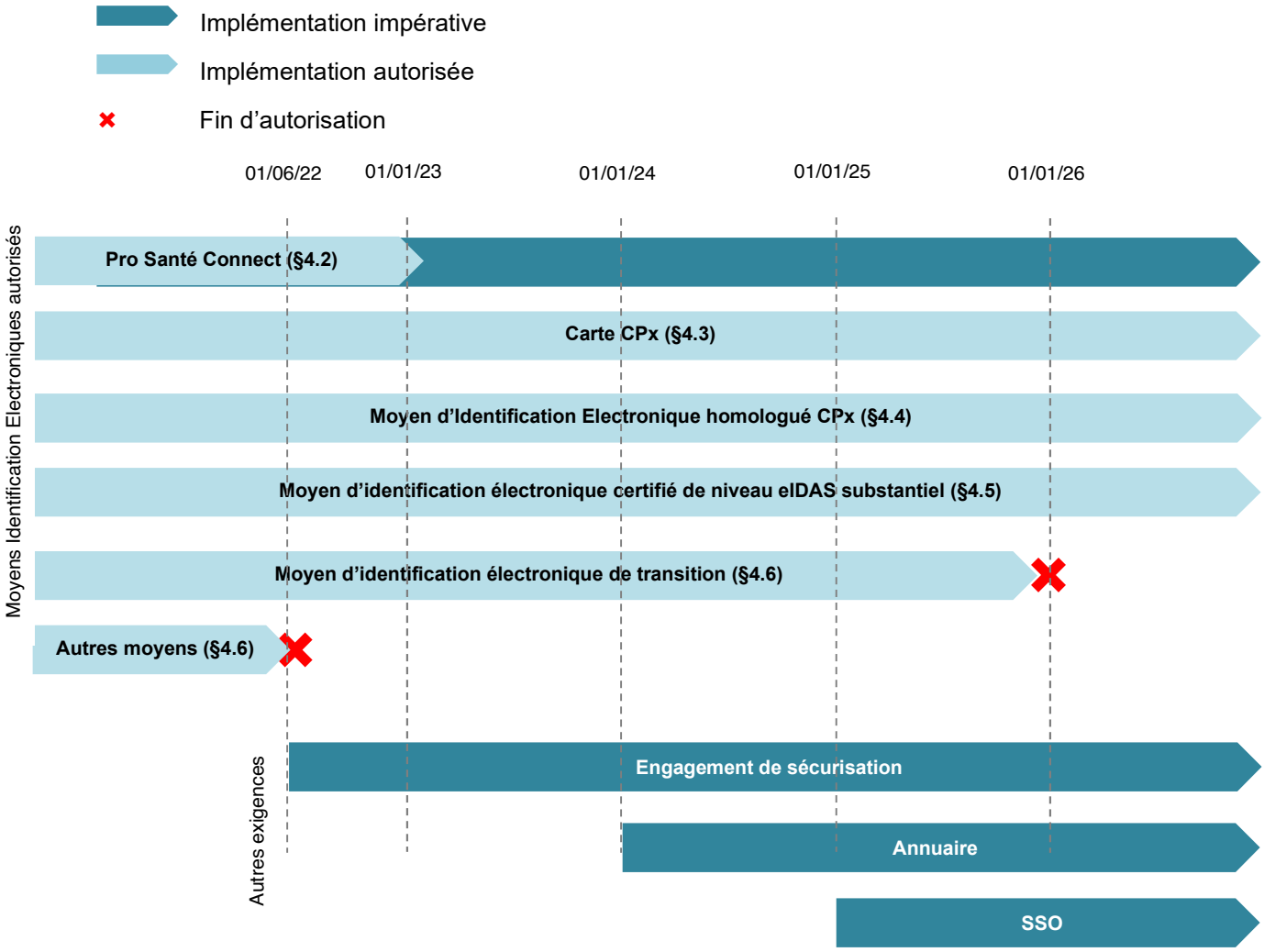


Figure 4 : Calendrier d'implémentation du RIE

2 L'Authentification primaire

L'authentification primaire a pour l'objectif de sécuriser l'accès à la session de travail.

L'authentification primaire est la certification de l'identité d'une personne (éventuellement d'un ordinateur) afin de l'autoriser à accéder à sa session de travail.

La notion d'authentification s'oppose à celle d'identification. Cette distinction est importante. Lorsqu'une personne présente sa pièce d'identité, elle est identifiée, mais n'est pas authentifiée, car le lien entre la pièce d'identité et la personne n'est pas établi de façon indiscutable et irrévocable.

Dans son guide « Recommandations relatives à l'authentification multifacteur et aux mots de passe », l'ANSSI définit l'authentification comme un mécanisme faisant intervenir deux entités distinctes : un « prouveur » et un « vérifieur ». De même, l'ANSSI différencie l'authentification multifacteur, basée sur l'usage de plusieurs facteurs de catégories différentes, et l'authentification forte, basée sur la cryptographie. Ces deux méthodes, présentes dans les recommandations R1 et R2, sont sécurisées.

Dans le cadre des établissements de santé, l'ANS privilégie l'authentification multifacteur, identifiée par l'acronyme MFA pour « Multi-Factor Authentication ».

Le principe d'authentification multifacteur s'appuie sur la *méthode standard des 3 facteurs*. Cette méthode définit trois catégories d'informations différentes (Facteurs) associées à une personne, par exemple :

- **Facteur de connaissance** : « ce que je sais », il s'agit d'une connaissance devant être mémorisée telle qu'une phrase de passe, un mot de passe, un code, etc. ;
- **Facteur de possession** : « ce que je possède », il s'agit d'un élément secret non mémorisable contenu dans un objet physique qui idéalement protège cet élément de toute extraction, tel qu'une carte à puce, un token, un téléphone, etc. ;
- **Facteur inhérent** : « ce que je suis », il s'agit d'une caractéristique physique intrinsèquement liée à une personne et indissociable de la personne elle-même, telle qu'une caractéristique biologique (ADN), morphologique (empreinte digitale, empreinte rétinienne) ou comportementale [(2)].

L'authentification MFA d'un utilisateur est réalisée à partir de deux facteurs.

[2] Note : définition ANSSI : « Recommandations relatives à l'authentification multifacteur et aux mots de passe »

2.1 MFA dans la santé

Depuis mai 2007, l'article R1110-3 du décret 'de confidentialité' n°2007-960 précise que *« l'accès par des professionnels de santé aux informations médicales à caractère personnel conservées sur support informatique ou de leur transmission par voie électronique, l'utilisation de la carte de professionnel de santé* (carte CPS) *mentionnée au dernier alinéa de l'article L. 161-33 du code de la sécurité sociale est obligatoire »*. En cela, la carte CPS est utilisée comme *facteur de possession*.

L'ANS a renforcé les exigences de sécurité dans les établissements de santé. Ces exigences sont détaillées dans le **« référentiel d'identification des personnes physiques et morales » rendu opposable par l'arrêté de Mars 2022**. Le référentiel définit, entre autres, les seuls systèmes d'authentification autorisés (MIE : Moyen d'Identification Electronique) dans le cadre d'une authentification MFA, comme les cartes CPx, mais également les dernières technologies, comme : **l'application e-CPS et le référentiel Pro Santé Connect**.

2.1.1 Les cartes CPx

Une carte de la famille « CPx » est une carte d'identité professionnelle électronique dédiée aux secteurs de la santé et du médico-social. Le « x » de « CPx » renvoie au fait qu'il existe plusieurs types de cartes en fonction de l'appartenance du porteur à un ordre ou une catégorie spécifique de personnels :

- CPS : carte de professionnel de santé ;
- CPF : carte de professionnel en formation ;
- CPE : carte de personnel d'établissement ;
- CDE : carte de directeur d'établissement ;

Une carte CPx permet à son titulaire d'attester de son identité et de ses qualifications professionnelles. Elle contient les données d'identification de son porteur : Identité (numéro d'identification, nom patronymique, nom d'exercice, …), profession, spécialité, identification du mode d'exercice…

La carte CPx est inscrite :

- Dans la loi (article L.1110-4 du code de la santé publique) comme un outil indispensable pour l'accès aux données de santé à caractère personnel ;
- Dans le référentiel d'authentification de la Politique Générale de Sécurité des systèmes d'Information de Santé (PGSSI-S) ;

La carte CPx contient les « certificats » électroniques d'authentification et de signature du porteur. Les usages de la carte CPx sont multiples, notamment :

- Identifier via le processus d'authentification forte ;
- Apposer une signature électronique ;
- Sécuriser les accès physiques (locaux, restaurant, parking...) dans les structures de santé ;
- Renforcer la sécurité des accès aux logiciels utilisés par le professionnel de santé ;

Carte CPx (§4.3)

MIE nativement autorisé, la CPx est sans doute le moyen d'authentification le plus adapté pour les établissements de santé :

- Elle est délivrée gratuitement par les organismes d'état. Précédemment complexe, le processus de commande des CPS a été amélioré. Ce processus peut être automatisé au travers des solution FairTrust IAM ;
- Depuis 06/2020, la carte CPS intègre une nouvelle puce intégrant les fonctions de contrôle d'accès Mifare DESFire EV1. La technologie Mifare permet l'authentification rapide par jeton de session ;
- Elle s'inscrit dans différentes déclinaisons des cartes CPx : CPE, CPA, CPF, CP Service…

Enfin, l'usage des cartes est aujourd'hui accepté par les utilisateurs des établissements de santé. Elle est facile à manipuler, à transporter au quotidien, répond, si nécessaire, aux exigences d'hygiènes. Ses seuls défauts seraient sa fragilité (risque de casse), la perte et le cout des lecteurs associés.

Attention, afin d'être conforme aux exigences de sécurité, la solution d'authentification basée sur la CPx doit utiliser le certificat électronique d'authentification et de signature de la carte.

2.1.2 e-CPS et Pro Santé Connect

A l'instar de la carte CPS, la e-CPS est un système d'identité professionnelle électronique dédiée à l'ensemble des acteurs professionnels de la santé et du secteur médico-social. Elle contient les données d'identification de son porteur. La e-CPS offre la possibilité aux professionnels de santé de s'authentifier avec leur mobile ou leur tablette, sans passer par un poste équipé d'un lecteur de carte. Elle répond ainsi aux enjeux d'authentification en mobilité des professionnels de santé.

Plus de détails sur e-santé.gouv.fr

Dans sa mission d'amélioration de la sécurité des systèmes d'information en santé, l'ANS fait évoluer le Code de la santé publique (CSP) et le Code de l'action sociale et des familles (CASF). Notamment, par l'ordonnance n°2021-581 du 12 mai 2021, l'ANS impose les points suivants :

- *A partir du 1er juin 2022*, l'accès aux services numériques sensibles comme le DPI d'établissement ou du GHT, la gestion du temps, la GAM, le DMP, le dossier Pharma…. nécessite une **authentification forte basée sur une carte CPS, ou e-CPS** ou d'autres moyens sous réserve d'homologation par l'établissement. L'authentification simple par le couple identifiant / mot de passe ne sera plus autorisé ;
- *A partir du 1er janvier 2023*, tous les établissements doivent implémenter une **authentification via le référentiel Pro Santé Connect** de l'Agence Numérique de Santé.

Figure 5 : Usage de l'e-CPS - Source ANS Aout 2022

Pro Santé Connect (§4.2)

Le référentiel **Pro Santé Connect** est un fédérateur de fournisseurs d'identités (FI). Il permet aux professionnels de s'authentifier avec sa e-CPS, ou sa CPS, de transmettre des informations d'identifications issues du RPPS et d'accéder à des applications et fournisseurs de service, comme « Pro Tous Anti Covid », ou « Vaccin Covid » de la CNAM.

Ces nouvelles dispositions sont détaillées dans le document « Référentiel d'identification électronique des acteurs de santé » de l'ANS.

Toutefois, l'authentification par e-CPS nécessite un certain nombre de manipulations et un smartphone. Cette méthode d'authentification, sécurisée et conforme aux exigences de l'ANS, est pratique pour l'accès à aux applications (MSSANTE, Vaccin Covid…), mais son usage reste « lourd » pour une authentification quotidienne en établissement de santé.

L'e-CPS ne sera sans doute pas le système d'authentification primaire, mais une solution très intéressante en système d'authentification alternatif (auto-dépannage) ou pour un usage en mobilité.

Enfin, l'ANS a contribué à la conception et au développement du flux CIBA (Client **Initiated Backchannel Authentication Flow**). L'objectif de CIBA [3] est de permettre l'authentification d'un utilisateur sur une application client lourd via le référentiel Pro Santé Connect.

2.1.3 Les moyens d'identification électroniques homologués et certifiés de niveau eIDAS substantiel

Moyen d'Identification Electronique homologué CPx (§4.4)

Moyens d'identification électronique certifié de niveau eIDAS substantiel (§4.5)

Conformément au « référentiel d'identification électronique », les établissements disposant déjà d'un système d'authentification, par exemple une carte de type MiFare, doivent faire « homologuer leur solution ». Si vous souhaitez réaliser cette homologation vous même, l'ANS met à votre disposition des guides d'accompagnement.

Attention, le processus d'homologation est complexe, long et consommateur de ressources (équivalent à une certification RGS**). Au regard des autres approches possible et MIEs autorisés disponibles, il semble que l'homologation d'une solution tierce soit inopportun.

.

[3] La spécification CIBA venant tout juste d'être adoptée, les travaux de développements sont en cours.

En complément, le référentiel autorise les MIEs certifiés eIDAS substantiel. À ce jour, seule la solution Docapost bénéficie de cette certification. Ce MIE n'est pas réellement utilisable dans le contexte hospitalier.

Il est probable que d'autres moyens d'identification certifiés eIDAS de niveau substantiel apparaitront sur le marché. Ces MIE seront directement « autorisés ».

2.1.4 Les moyens d'identification électroniques de transition

Moyens d'identification électroniques de transition (§4.6)

Conscient des délais relativement courts pour la mise en conformité, le référentiel d'identification échelonne la mise en œuvre des exigences de sécurité.

Jusqu'au 31/12/2025, le référentiel autorise l'utilisation de **moyens d'identification de transition.**

Il s'agit d'une méthode d'authentification obligatoirement multi-facteurs, basée sur un mot de passe d'une entropie de 50 bits, renouvelé régulièrement, associé à :

- Un code TOTP ou OTP ;
- Ou une application mobile enrôlée sur le téléphone de l'utilisateur ;
- Ou une empreinte digitale vérifiée par le téléphone de l'utilisateur ;

Un mot de passe d'une entropie de 50 bits est complexe à mémoriser. En conséquence, il est intéressant d'utiliser un gestionnaire de mots de passe : coffre-fort ou Single Sign-On. Le SSO étant fortement préconisé ou obligatoire à partir du 01/01/2025, sa mise en œuvre semble opportune à court terme.

2.1.5 Les autres moyens d'identification

Autres moyens (§4.6)

Publié au mois de mars 2022, l'arrêté ministériel du 28 mars 2022 précise que seul les MIEs autorisés seront acceptables pour l'authentification des utilisateurs à partir du 01 juin 2022.

Ces délais étant relativement courts, durant une période de transition, les établissements ne seront pas sanctionnés au regards de la non-conformité au référentiel d'indentification. Cependant, les établissements ont l'obligation d'établir un plan de sécurisation conforme à l'arrêté et décrit dans le document « Engagement de sécurisation ».

2.1.6 Engagement de sécurisation

Engagement de sécurisation

L' « engagement de sécurisation de l'identification électronique » est un document interne à la structure, **obligatoirement validé en 2022**. Il décrit le plan d'actions et le planning prévisionnel d'implémentation des solutions de sécurisation du SIH, afin d'assurer la conformité au référentiel.

L’engagement se compose principalement de deux parties :

- Une description de l’état d’implémentation de l’identification électronique, les MIE déployés et le plan d’action pour la conformité jusqu’en 2026 ;
- Une partie confidentielle présentant les risques résiduels et le plan d’action de correction des éventuelles non-conformités ;

Les engagements de sécurité doivent obligatoirement impliquer la Direction Générale. En cela, le document doit être signé par le responsable légal du fournisseur des services numériques en santé concernés, ou, à défaut, par un délégataire dument habilité.

Afin de suivre l’évolution du plan d’action, le document doit être mise à jour au minimum chaque année, ou après une évolution significative, et validé.

L’engagement de sécurité est exigible par les autorités à tout moment et réclamé en cas de cyberattaque ou de faille de sécurité du SIH.

3 Authentification Secondaire

L'authentification secondaire a pour l'objectif de sécuriser l'accès aux services numériques du SIH.

L'authentification secondaire [4] est le processus permettant de certifier l'identité d'un utilisateur pour l'accès à une application, une ressource ou un service numérique.

Depuis les années 60, Fernando Corbató a instauré une sécurisation des accès au SI par l'identification des utilisateurs grâce à un couple d'informations secrètes : **identifiant et mot de passe**. Même si cette méthode est entrée dans les usages courants, il existe encore des failles de sécurité principalement liées aux mauvais usages des mots de passe.

Depuis, de nouvelles méthodes d'authentification sont apparues. Cependant, beaucoup d'applications nécessitent encore une authentification par mot de passe.

3.1 L'authentification par mot de passe réglementé

3.1.1 Automatiser l'authentification secondaire

Comme son nom l'indique, le 'Single Sign On', très souvent désigné par son acronyme 'SSO', définit un principe d'automatisation de l'authentification d'un utilisateur auprès de l'ensemble de ses services numériques, applications et sites web. Ce principe s'appuie sur une première authentification unique, idéalement renforcée.

Dans ce principe, l'utilisateur s'authentifie une première fois, idéalement via une authentification forte ou multifacteur (MFA), puis accède à ses ressources sans avoir besoin de se réauthentifier. L'authentification secondaire est réalisée automatiquement.

En conséquence, le Single Sign-On (SSO) offre les avantages suivants :

- **Sécurité** : L'utilisateur se concentre sur une seule authentification définie en fonction des exigences de sécurité (identifiant / mot de passe, authentification forte, MFA …). Le cycle de vie des mots de passe étant géré de manière transparente, il est possible de masquer totalement l'usage de ceux-ci et donc d'en empêcher le partage non-autorisé entre utilisateurs.
- **Efficacité** : Après la première authentification, l'utilisateur ne saisit plus de mots de passe : pas d'erreur de saisie, accès rapide aux ressources. Une conséquence importante de l'usage d'une solution de Single Sign-On est la réduction quasi-totale des cas d'attaques par phishing (usurpation d'URL par exemple) ;
- **Confort** : Les utilisateurs accèdent rapidement aux ressources, sans action d'authentification et sans avoir besoin de mémoriser de multiples mots de passe ;

[4] Cf. Définition page 7

- **Conformité** : Comme les mots de passe sont gérés dans un outil, ils peuvent être longs, complexes et changés régulièrement. La sécurité est améliorée et les bonnes pratiques ANSSI respectées ;

Le Single Sign-On répond aux exigences de l'ANS concernant la sécurisation des accès aux ressources numériques. En plus de faciliter l'authentification des utilisateurs, le SSO permet de respecter les préconisations de l'ANSSI comme :

- Stockage des secrets utilisateurs dans un référentiel sécurisé ;
- Gestion du cycle de vie des mots de passe : Renouvellement régulier ;

Le SSO ne gère pas les droits des utilisateurs dans les ressources du SI. Il simplifie et renforce la sécurité des accès. La gestion des droits et habilitations est réalisée par la gestion des identités et des accès (IAM – Identity & Access Management).

3.1.2 Single Sign-On et Coffre-Fort de mots de passe

Le SIH est composé d'un ensemble hétérogène d'applications. Beaucoup d'applications nécessitent encore une authentification par mot de passe. En outre, la plupart des applications intègrent leur propre base d'utilisateurs et n'utilisent pas l'annuaire technique de l'établissement.

L'authentification par mot de passe est une **méthode sécurisée si les bonnes pratiques sont respectées**.

L'ANSSI décrit les bonnes pratiques [5] pour une authentification simple, par mot de passe. Notamment, les recommandations R32 et R33 précisent la nécessité :

- D'utiliser des mots de passe complexes [6] et longs [7] ;
- D'utiliser des mots de passe différents pour chaque ressource ;
- Éventuellement d'en changer régulièrement ;

Si l'authentification par mot de passe n'est pas pilotée par un outil, la mise en œuvre de ces pratiques conduit systématiquement à des dérives : mots de passe notés dans un carnet, stockés sur le poste de travail ou dans le navigateur. Il est donc indispensable d'utiliser d'un outil de gestion des mots de passe applicatif, nommé « Password Manager » ou « Coffre-Fort de mots de passe », pour l'authentification secondaire.

Lorsque le Coffre-Fort de mots de passe réalise automatiquement l'authentification dans les applications, sans action de l'utilisateur, les outils prennent souvent la dénomination « SSO », créant parfois une confusion entre le produit et le principe de Single Sign-On.

Au-delà de l'automatisation de l'authentification, le SSO renouvèle régulièrement les mots de passe et les remplace par des mots de passe complexes et différents pour chaque application. Idéalement, un outil de SSO intègre les fonctionnalités suivantes :

---

5 Cf. Guide « Recommandations relatives à l'authentification multifacteur et aux mots de passe »

6 Une suite alphanumérique aléatoire utilisant minuscules, majuscules, chiffres et caractères spéciaux, sans lien avec l'utilisateur

7 Un minimum de 10 caractères. Idéalement plus de 12 caractères

- **Prise en compte de tous types d'applications :** Etant donné l'hétérogénéité du parc applicatif des établissements de santé, l'outil doit traiter l'authentification pour des types d'applications très divers comme les applications web, les clients lourds ou applications textes, exemple émulateurs AS/400 ou TN3270 ;
- **Référentiel sécurisé :** Les secrets utilisateurs, comme les identifiants et mots de passe, sont centralisés, par exemple dans une base de données, de manière sécurisée ;
- **Authentification automatisée transparente :** Dans des versions avancées, l'outil automatise la saisie des secrets dans les champs d'authentification afin de simplifier l'accès aux ressources ;
- **Renouvellement des mots de passe :** L'outil facilite la création de mots de passe complexes et idéalement gère leur renouvellement régulier par des mots de passe complexes, en conformité avec votre politique de sécurité. À terme, les mots de passe utilisateur sont tous complexes ;
- **Fonctionnalités avancées :** Afin de couvrir un maximum des cas d'usage des établissements de santé, l'outil de gestion des mots de passe pourra intégrer des fonctionnalités avancées comme :
    - Multicompte : Plusieurs comptes d'authentification pour un même utilisateur et une ressource donnée ;
    - Compte partagé : Un seul compte d'authentification pour plusieurs utilisateurs de la même ressource ;
    - Délégation de compte : Permettre à un utilisateur de s'authentifier à la place d'un autre utilisateur, sans communiquer les secrets d'authentification, sur une période de temps ;

3.1.3 Le Single Sign-On du RIE

SSO

Au plus tard au 01/01/2025, le Référentiel d'Identification Electronique demande l'implémentation d'une solution de Single Sign-On. Cette exigence s'applique :

- Pour les structures responsables de **plus de 5 services sensibles** ;
- Ou comptant plus de **5 000 professionnels** ayant accès à au moins un service sensible ;

Pour être conforme au référentiel, la solution de SSO doit :

- S'appuyer sur les identités de l'annuaire central ;
- Etre compatible avec les MIEs autorisés ;
- Etre compatible avec le protocole CIBA et le référentiel Pro Santé Connect.

La mise en place d'une solution SSO apporte, non seulement, une ergonomie et un confort aux utilisateurs, mais permet également d'augmenter le niveau de sécurité. C'est pourquoi, la mise en œuvre d'un SSO est exigée pour les structures les plus importantes, et fortement recommandée pour l'ensemble des établissements.

FairTrust SSO est la première solution à avoir intégré l'authentification par e-CPS et protocole CIBA.

3.1.4 Authentification par jeton

L'évolution des technologies permet, dans certains cas, d'éliminer les mots de passe de la chaîne d'authentification, grâce à un jeton d'authentification. Cette méthode est réservée aux applications et services web récents. Elle repose sur un échange d'informations structurées (jeton d'authentification) entre deux systèmes :

- Un système offrant un service à l'utilisateur, comme par exemple une application ou un service web. Ce système appelé **« Service Provider » (SP)** a besoin de connaitre l'identité de l'utilisateur. Il va donc la demander à un tiers (système) de confiance ;

- Un système détenant l'identité de l'utilisateur, appelé « **Identity Provider » (IDP)**. Il s'agit souvent d'un référentiel central sécurisé. Il fournit les informations d'authentification nécessaires au « Service Provider ».

Dans un processus d'authentification par jeton, souvent identifié comme « fédération d'identité » ou parfois « Modern Authentication », l'utilisateur doit s'authentifier au moins une fois. Nous sommes bien sur le principe du Single Sign-On. Cette authentification, idéalement forte ou MFA, certifie l'identité de l'utilisateur auprès du référentiel d'identité (IDP). En conséquence, le niveau de sécurité établi par l'authentification primaire est redistribué sur l'authentification secondaire.

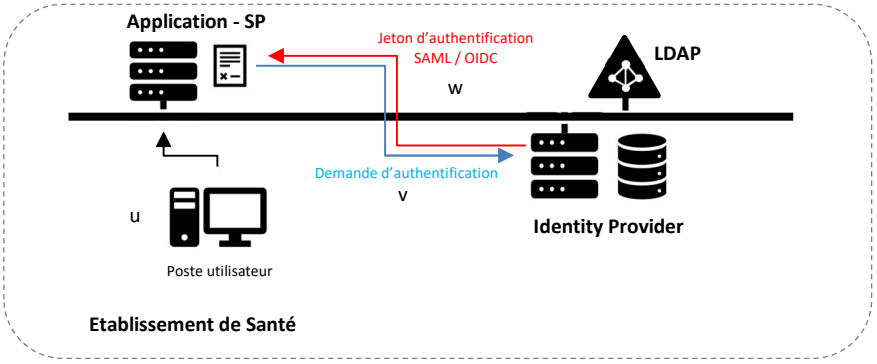


Figure 6 : Processus d'authentification par jeton

Lorsqu'un utilisateur lance une application ❶ disposant des fonctionnalités de SP, le SP adresse une demande à l'IDP ❷. L'IDP, ayant certifié l'identité de l'utilisateur, retourne au SP un jeton d'authentification ❸, intégrant si nécessaire des informations complémentaires sur le profil de l'utilisateur. À des fins d'utilisabilité, la structure des jetons est normalisée. Les principaux protocoles sont SAML, OAuth, OpenID Connect (OIDC).

Cette méthode d'authentification trouve sa place dans beaucoup de schémas, par exemple, dans le cadre de l'authentification des utilisateurs d'un centre hospitalier avec un référentiel de sécurité centralisé dans l'établissement support, du Groupement Hospitalier Territorial.

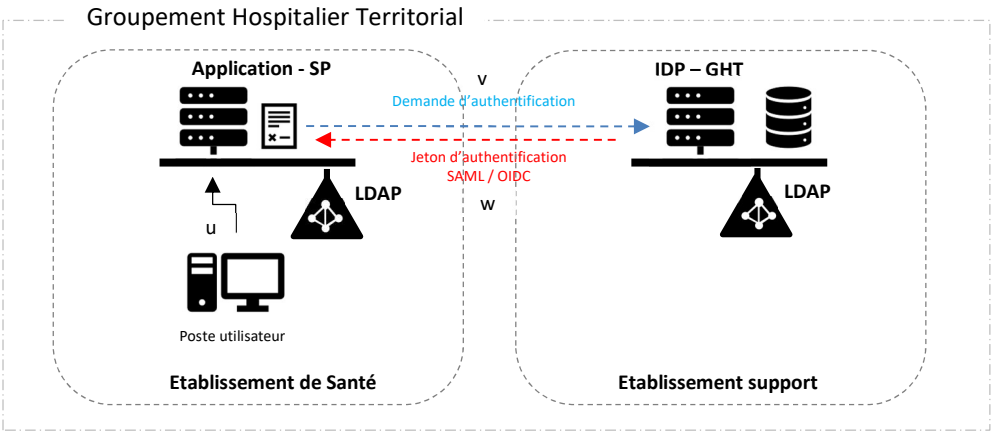


Figure 7 : Authentication par jeton en GHT

En éliminant les mots de passe du schéma d'authentification, vous réduisez les attaques par force brute ('bruteforce attack'), et simplifiez les actions des utilisateurs et administrateurs.

Même si la fédération d'identité présente de véritables avantages, elle est uniquement disponible pour les applications au format web, intégrant le rôle de Service Provider. De plus, il est nécessaire de mettre en place un IDP. En conclusion, cette approche est intéressante mais ne couvre pas la totalité des besoins des établissements de santé.

4 Annuaire de personnes

Les référentiels et les annuaires constituent les fondations d'un système d'information.

4.1.1 Annuaire

On appelle « annuaire » (parfois « répertoire ») un référentiel qui stocke de manière organisée une liste d'attributs valorisés, caractérisant des individus, rattachée à une des structures de l'établissement. L'annuaire comporte classiquement les identifiants, états civils, mots de passe, ainsi que les affectations, statut administratif et fonction. Il est utilisé à des fins opérationnelles de gestion du SI, dans lequel il joue le rôle d'un pivot d'échanges. En raison même de sa fonction de « pivot », l'annuaire a des utilisations diverses : répertoire téléphonique, source statistique, système d'authentification lors de la connexion au système d'information.

Un point délicat de la gestion des annuaires réside dans leur mise à jour. Si les modifications du monde réel (embauche, mutation, changement etc.) ne sont pas enregistrées dans l'annuaire dans un délai « raisonnable » en regard des exigences opérationnelles, le décalage entre l'annuaire et la réalité compromet la qualité du système d'information.

4.1.2 Active Directory

Active Directory (AD) est un service d'annuaire au format LDAP pour les systèmes Windows. L'annuaire technique AD fournit des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows, macOS et encore Linux.

Il permet également l'attribution et l'application de stratégies ainsi que l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc. Un utilisateur peut ainsi facilement trouver des ressources partagées, et les administrateurs contrôlent leur utilisation grâce à des fonctionnalités de distribution, de duplication, de partitionnement et de sécurisation de l'accès aux ressources répertoriées.

4.1.3 L'annuaire central du référentiel d'identification électronique

Annuaire

Au plus tard au 01/01/2024, le Référentiel d'Identification Electronique (RIE) exige la mise en place d'un répertoire d'identités local :

- Contenant l'ensemble des professionnels de santé de la structure ;
- Synchronisé régulièrement avec le SIRH ;
- Contenant le numéro RPPS (si disponible) associé à l'identité des personnes physiques et le vérifier au moins tous les 2 ans ;

L'objectif de l'annuaire d'identité local est d'assurer la cohérence des annuaires techniques (exemple Active Directory) avec les SIRH et de faciliter les contrôles périodiques.

Dans un premier temps, l'Active Directory peut être vu comme votre annuaire d'identités local.

L'utilisation de votre AD comme annuaire d'identité est conforme au Référentiel d'Identification Electronique.

Pour cela, vous devrez mettre en œuvre des processus de synchronisation avec votre SIRH. Dans un SIH constitué d'un Active Directory et d'un logiciel RH, cette synchronistion est facilement envisageable. Cependant, dans une organisation en Groupements Hospitaliers de Territoire, vos devez gérer différents SIRH et un ou plusieurs annuaires Active Directory.

Il semble donc judicieux de construire un annuaire d'identités central indépendant, alimenté depuis les différents SIRH et provisionant vos annuaires techniques (AD).

Le socle de base de la solution FairTrust IAM offre nativement ces fonctionnalités et intègre, en plus, les mécanismes de commandes automatiques des cartes CPx auprès de l'ANS.

4.1.4 Identity & Access Management (IAM)

L'Identity and Access Management (IAM) est une pratique de cybersécurité qui vise à garantir que seules les personnes autorisées ont accès aux ressources et aux données sensibles d'une organisation.

L'IAM implique la gestion de l'identité numérique des utilisateurs, la gestion des droits d'accès aux systèmes et aux données, ainsi que la gestion des autorisations et des privilèges accordés aux utilisateurs en fonction de leurs rôles et responsabilités dans l'organisation.

L'objectif final de l'IAM est de garantir que les utilisateurs ont accès uniquement aux ressources dont ils ont besoin pour effectuer leur travail, au moment où ils en ont besoin, tout en empêchant les accès non autorisés. Ces solutions s'inscrivent dans une démarche zéro trust pour la mise en conformité de votre SI avec les préconisations des agences gouvernementales : NIST, ANSSI, ANS....

4.1.5 FairTrust IAM

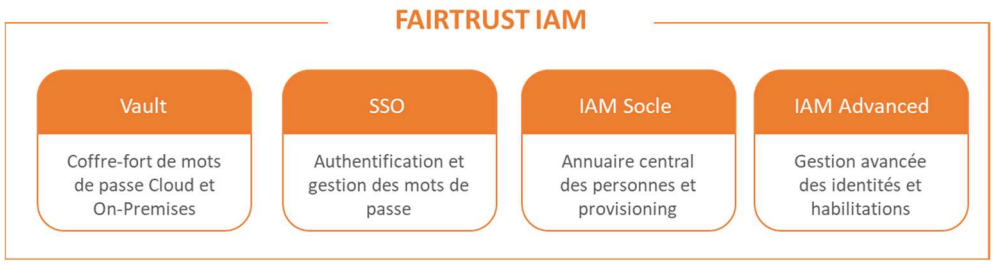
FairTrust IAM gère, structure et automatise le cycle de vie des personnes et de leurs habilitations dans votre système d'information. En résumé, FairTrust IAM contribue à l'amélioration de vos systèmes d'informations en apportant une sécurité opérationnelle liée aux identités et habilitations :

- **Centralisation des droits et des ressources** : FairTrust gère et centralise les d'identités numériques et les droits des utilisateurs (habilitations) pour l'accès aux applications et ressources mises à disposition par l'entreprise ;
- **Optimisation de la gestion des comptes** : FairTrust détermine automatiquement les habitations des personnes, en fonction de règles auditables ;
- **Renforcement de la sécurité** : La révocation automatique des droits supprime les comptes dormant et inopérant et réduit de manière importante les failles de sécurité de votre SI liées au fishing ;
- **Modernisation de la gestion des droits** : FairTrust apporte des fonctionnalités comme le SoD (Segregation of Duty) ou la re-certification des droits des utilisateurs ;
- **Synchronisation des référentiels** : FairTrust intègre les mécanismes de synchronisation entre référentiels :

Alimentation Amont : Les identités sont créées automatiquement en s'appuyant sur les informations disponibles dans votre SI, par exemple les données issues de votre logiciel RH.

Alimentation Aval ou Provisioning : Les habilitations calculées dans FairTrust sont poussées dans les référentiels cibles.

- **Automatisation des processus** : En complément des règles d'habilitation, FairTrust automatise les taches courantes au travers de Workflows ;
- **Traçabilité** : L'ensemble des actions et modifications est tracé dans la solution IAM. Les informations sont disponibles en temps réel sous forme de rapport ;



5 FairTrust SSO en résumé

FairTrust Enterprise SSO est la nouvelle génération de Single Sign-On conçue pour la répondre aux besoins d'authentification et de sécurisation des accès, des entreprises modernes.

Conformément aux principes du Single Sign-On, FairTrust Entreprise SSO renforce l'authentification primaire, centralise les mots de passe dans un coffre-fort sécurisé et automatise l'authentification des utilisateurs dans toutes leurs applications.

FairTrust SSO répond aux bonnes pratiques préconisées par l'ANSSI, ainsi qu'aux exigences des organismes de sécurité Français (ANSSI, BSI, ANS…) et normes internationales (ISO, ENISA, DORA…).

5.1 Solution moderne de eSSO

Issue de 20 ans d'expérience dans la cybersécurité et la gestion de l'authentification des utilisateurs, FairTrust SSO s'appuie sur des technologies récentes et des méthodes de développement modernes. Nativement conçu pour les architecteurs Cloud et OnPremises, cette nouvelle génération de SSO répond aux attentes des entreprises :

- Architecture cohérente avec les entreprises multi organisation ;
- Niveau de sécurité élevé pour répondre aux exigences réglementaires ;
- Console d'Administration centralisée accessible depuis tous périphériques ;
- Facilités d'Administration et Exploitation, pas d'action sur les postes de travail ;
- Prise en compte simplifiée de toutes les applications, Web, Client/Serveur, AS400… ;

Une solution innovante et pragmatique pour répondre aux objectifs de sécurisation des organisations modernes de toutes tailles et dans tous les secteurs d'activité.

5.2 Authentification Forte - MFA

FairTrust SSO intègre l'authentification multifacteur (MFA). Basé sur le principe des 3 facteurs, FairTrust supporte nativement les éléments physiques comme les clés FIDO, carte MiFare / Mifare DESFire ou CPx…, l'authentification par empreinte digitale [8] ou l'usage de code à usage unique : OTP ou TOTP.

Sur présentation d'un premier facteur d'authentification, l'utilisateur est invité à saisir une information secrète, comme second facteur. Cette information peut être un mot de passe ou plus généralement un 'Code PIN' plus rapide à saisir.

En plus des systèmes traditionnels, FairTrust Enterprise SSO est la première solution à avoir intégrer l'authentification par e-CPS développé par l'ANS pour les établissements de santé. FairTrust SSO intègre :

- Le support de l'application e-CPS ;
- L'authentification via le référentiel Pro Santé Connect ;
- La compatibilité avec les flux CIBA ;

Pour simplifier l'authentification par un facteur physique ou inhérent, FairTrust SSO s'intègre de manière transparente dans les interfaces Windows[9] (Credential Provider). Cette authentification s'inscrit dans un processus traditionnel facilitant l'adhésion des utilisateurs au principe de SSO.

FairTrust SSO renforce la sécurité des systèmes d'informations en intégrant l'authentification multifacteur (MFA) tout en conservant un haut niveau de satisfaction utilisateur.

5.2.1 L'authentification rapide – Poste Kiosque ou « Mixte »

Certains usages nécessitent un accès rapide aux environnements de travail, tout en conservant un haut niveau de sécurité. Le mode Kiosque de FairTrust répond à ces besoins. Le poste de travail démarre avec un compte de service « Kiosque » et FairTrust verrouille automatique la session.

Après s'être authentifié, FairTrust déverrouille la session « Kiosque » (quelques secondes) et authentifie automatiquement l'utilisateur dans les applications. En complément, FairTrust crée un jeton de session (respectant les bonnes pratiques de sécurité) et le stocke sur l'élément physique d'authentification[10].

Mieux encore, FairTrust crée le poste « Mixte ». FairTrust fait cohabiter les sessions nominatives et kiosque sur un même poste de travail avec une gestion centralisée de la configuration.

FairTrust SSO apporte l'authentification rapide et sécurisée, respectant les bonnes pratiques, avec un gestion centralisée des « Postes Mixtes ». Vous bénéficiez à la fois de la sécurité des accès et de la souplesse d'utilisation et d'exploitation d'un SSO professionel.

8 Facteur inhérent centralisé, non autorisé en France

9 Voir guide fonctionnel FairTrust SSO

10 Voir guide fonctionnel FairTrust SSO

5.3 L’authentification secondaire automatisée

Fonctionnalité essentielle d’une solution de Single Sign-On, FairTrust SSO automatise l’authentification de l’utilisateur dans l’ensemble de ses applications.

FairTrust SSO s’appuie sur un agent installé sur le poste utilisateur (eSSO) gérant :

- Les opérations de traitements de l’authentification ;
- La configuration de l’agent : interface, mise à jour, actions de la souris ;
- Le coffre-fort local : compte, applications, Mot de passe… ;

FairTrust supporte tous types d’applications, de manière non-intrusive. FairTrust gère le cycle de vie des mots de passe et renforce la sécurité d’accès aux services numériques. Le coffre-fort central hautement disponible, l’algorithme de chiffrement AES256 CGM et les flux https sécurisent les mots de passe et les interaction entre le coffre-fort et les applications. Notamment, l’architecture client/serveur de FairTrust SSO est la seule garantissant véritablement la protection de vos données.

En complément, FairTrust comprend toutes les fonctionnalités standards d’un SSO professionnel : délégation de compte, le multi comptes et les comptes partagés sans divulgation de mots de passe, traçabilité, auto-dépannage...

L’outil de configuration d’application SSO Config simplifie l’enrôlement des applications. Les applications simples sont configurées en quelques clics. Mieux, les applications Web et TSE sont automatiquement enrolées sans actions de configuration.

5.4 Principales caractéristiques de FairTrust Enterprise SSO

Ces fonctionnalités sont détaillées dans le « Guide fonctionnel FairTrust SSO ».

Référentiel d'authentification centralisé

Les données sensibles sont centralisées dans un coffre-fort sécurisé. Chiffrement AES 256 GCM, RSA 2048/4096

Coffre-Fort multiple

Plusieurs coffres-forts pour séparer les usages d'entreprises et personnels pour un même utilisateur.

Auto découverte

Enrôlement automatique et authentification automatisée des applications web.

Auto Apprentissage

Apprentissage automatique des mots de passe applicatif lors du 1er lancement de l'application.

Mot de passe robuste

Apprentissage automatique des mots de passe applicatif lors du 1er lancement de l'application.

Multicompte

Support de plusieurs comptes d'authentification pour une même application.

Comptes partagés

Utilisation d'un même compte authentification synchronisé entre plusieurs utilisateurs.

Délégation de comptes

Délégation des accès utilisateurs en cas d'absence sur une période définit avec autorisation des administrateurs.

Architecture Cloud et On-Premises

Solution conçue et développée nativement pour le Cloud et disponible dans les environnements On-Premises

Traitement « Cash First »

Traitement des actions d'authentification en priorité par l'agent FairTrust. Optimisation des performances et disponibilité hors connexion.

6 FairTrust en quelques mots

Parce ce que nous croyons que la sécurité des systèmes d'informations doit être accessible à toutes les entreprises quelle que soit leur taille, leur métier ou leur compétence en informatique, FairTrust a conçu et développé des solutions pratiques, efficaces et faciles d'accès.

FairTrust est éditeur de solutions de cybersécurité dans le domaine de l'IAM – Identity & Access Management. Nos solutions couvrent l'authentification forte, la gestion des mots de passe, la gestion des identités et des habilitations.

> Il ne peut pas y avoir de Zero Trust sans gestion d'identité
>
> Martin Kuppinger, Founder and Principal Analyst, KuppingerCole Analysts

Les entreprises doivent faire face aux risques de cyberattaques, fraudes, chantages et extorsions. Nous concevons des solutions de sécurisation des accès et de gestion des identités modernes, simples et efficaces, accessibles à toutes les entreprises, depuis les TPEs aux Grandes Entreprises. Nous aidons les entreprises à limiter leur exposition aux risques par une meilleure gestion des droits d'accès et des accès et en renforçant l'authentification des utilisateurs.

> Notre mission est de concevoir des produits modernes, performants et accessibles à tous, pour répondre à la nécessité de sécurité des systèmes informatiques.
>
> David Wonner - Fondateur et Président FairTrust.

6.1 Notre Vision

Aujourd'hui, La sécurité informatique doit être accessible à toutes les entreprises. La sécurisation du SI est une évidence. Elle s'inscrit dans une logique globale comme s'équiper d'une messagerie ou d'outils bureautiques. C'est pourquoi, nous avons conçu des solutions modernes, performantes et accessibles à toutes les entreprises quels que soit leurs tailles ou leurs domaines.

Conçus nativement pour le Cloud, nos produits sont disponibles rapidement sans avoir besoin d'infrastructures complexes ou de ressources importantes. Nous apportons une réponse pragmatique, efficace, basée sur des technologies à la pointe de l'état de l'art.

6.2 Notre Savoir-Faire

Durant plus de 20 ans, nous avons travaillé sur des projets de cybersécurité. Cette expérience nous a permis d'appréhender les besoins fonctionnels des utilisateurs, la complexité des environnements techniques, la pluralité applicative et la diversité des processus internes.

Aujourd'hui, nous mettons à profit cette expérience pour concevoir et développer des solutions pragmatiques d'IAM, basées sur des outils et technologies récents.

6.3 Nos Valeurs

En consolidant notre expérience individuelle, nous avons la conviction que la qualité et la pérennité de notre entreprise reposent en grande partie sur les valeurs que nous défendons : éthique, durable, de qualité, proche de nos clients.

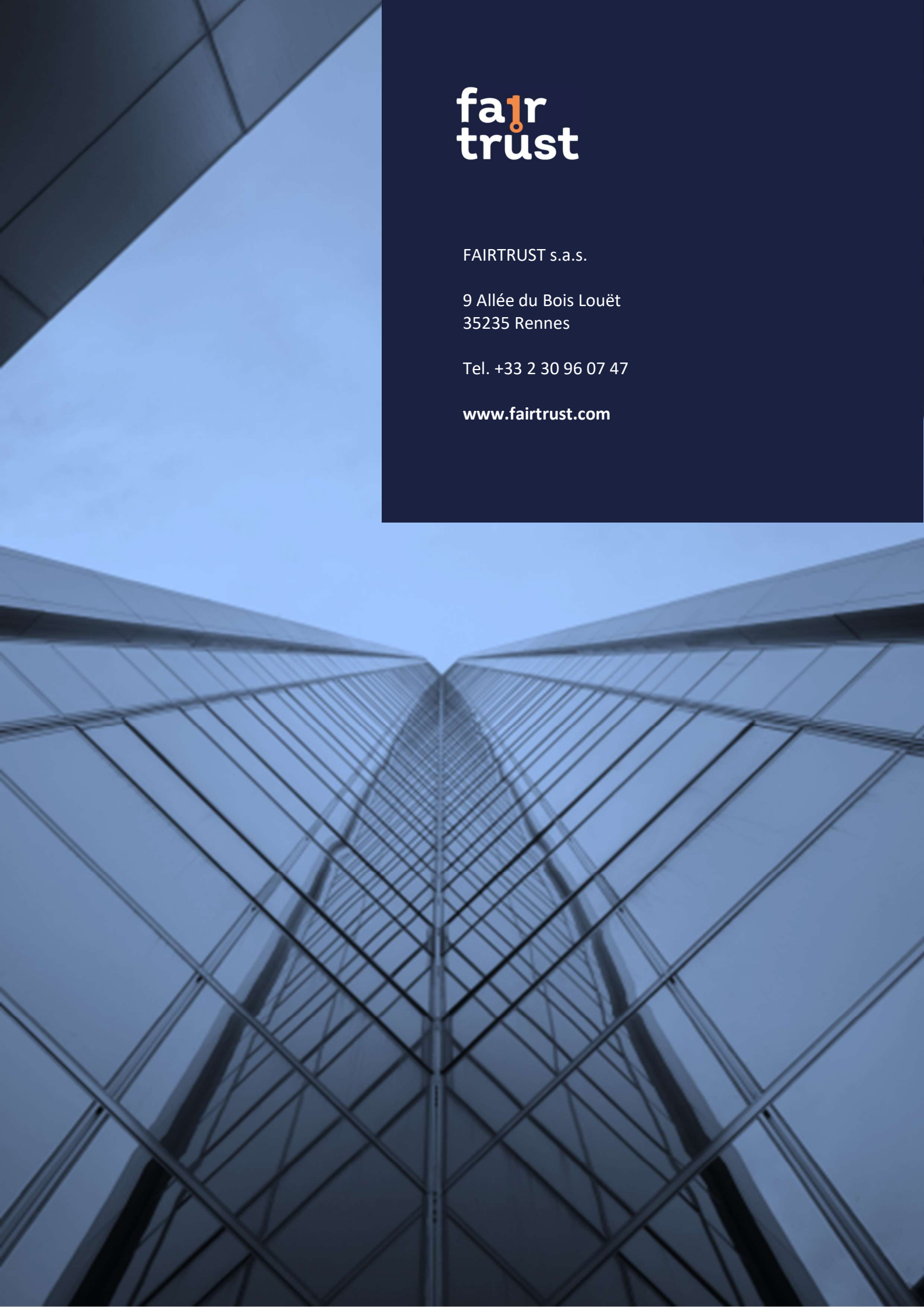
Gagner votre confiance – en apportant des réponses sincères, en respectant nos engagements. C'est pour nous la seule manière d'établir une relation professionnelle sur le long terme avec nos clients, partenaires et collaborateurs.

Partager notre expérience – Ce partage va au-delà de nos produits. Il s'inscrit dans notre volonté de contribuer à la protection et la valorisation de votre système d'information et dans la montée en compétence de nos équipes.

Être à l'écoute – de vos enjeux, contexte et besoins. Parce que vous vous connaissez mieux que quiconque et que nous avons besoin de vous découvrir pour vous apporter les réponses les plus adaptées.

Être Focalisé – parce que nous souhaitons consacrer notre énergie d'abord sur les actions essentielles, nous sommes concentrés sur notre seul secteur d'activité. La compétence ne peut s'obtenir que par la spécialisation.

Humaniser – parce que les hommes et les femmes de FairTrust sont notre première force, la qualité de leurs conditions de travail et de leur environnement est essentielle et fonde notre culture d'entreprise.



FAIRTRUST s.a.s.

9 Allée du Bois Louët
35235 Rennes

Tel. +33 2 30 96 07 47

www.fairtrust.com