FICHET

LIVRE BLANC

NIS 2, CRA : pourquoi votre contrôle d'accès doit être certifié ANSSI

La réponse souveraine de Fichet Group avec SMI Server 4.6, solution certifiée pour la troisième fois par l'ANSSI

www.fichetgroup.com



Introduction



Arnaud Surpas
Président
Fichet Group

Avec la directive européenne NIS 2 et le règlement Cyber Resilience Act (CRA), l'Europe impose un niveau de cybersécurité inédit à des milliers d'organisations. La conformité passe par une démarche globale - gouvernance, gestion des incidents, continuité d'activité - dont la sécurité physique, et en particulier le contrôle d'accès, est un maillon à part entière.

Ce livre blanc explique, sans jargon d'expert, ce que ces textes changent pour vous, et pourquoi le choix d'une solution certifiée ANSSI, conçue et fabriquée en France, est la réponse la plus sûre.

FICHET

Sommaire

NIS 2 : de quoi parle-t-on, et qui est concerné ? 04

La conformité NIS 2 : une démarche globale, dont le contrôle d'accès est un maillon clé 06

La certification ANSSI : la preuve objective de robustesse 08

La réponse Fichet Group : souveraine, certifiée de bout en bout 10

Rester conforme dans la durée : SML, veille R&D et anticipation du CRA 12

Passer à l'action : réussir la convergence cyber/physique en quatre étapes 14

En synthèse 16

NIS 2 : de quoi parle-t-on, et qui est concerné ?

Publiée au Journal officiel de l'Union européenne en décembre 2022, la directive NIS 2 (Network and Information Security) vise un objectif simple : élever le niveau global de cybersécurité en Europe, face à une cybercriminalité en forte hausse qui touche des organisations de toutes tailles — grands groupes, ETI, PME, collectivités.

Elle succède à la directive NIS 1 en élargissant considérablement son périmètre et en renforçant les obligations : gestion des risques, mesures de sécurité, notification des incidents et responsabilisation des dirigeants.

En France, c'est l'ANSSI (Agence nationale de la sécurité des systèmes d'information) qui pilote sa transposition et publie depuis mars 2026 le Référentiel Cyber France (ReCyF), qui liste les mesures recommandées pour atteindre les objectifs de sécurité de la directive.

Qui est concerné ?

Le changement d'échelle est sans précédent : en France, selon l'ANSSI et la SPAC Alliance, entre 15 000 et 18 000 entités entrent dans le champ de NIS 2 selon les estimations, contre quelques centaines sous NIS 1.

L'assujettissement repose sur deux critères combinés : le secteur d'activité (dix-huit secteurs visés) et la taille de l'entité :

- **Secteurs hautement critiques (annexe I)** : énergie, transports, banque, infrastructures des marchés financiers, santé, eau potable, eaux usées, infrastructures numériques, gestion des services TIC, administration publique, espace.
- **Autres secteurs critiques (annexe II)** : services postaux, gestion des déchets, produits chimiques, denrées alimentaires, fabrication (dispositifs médicaux, électronique, machines, véhicules…), fournisseurs numériques, recherche.
- **Entité importante** : dès 50 salariés, ou plus de 10 millions d'euros de chiffre d'affaires et de bilan annuel.
- **Entité essentielle :** à partir de 250 salariés, ou plus de 50 millions d'euros de chiffre d'affaires, dans les secteurs hautement critiques.

15 - 18 000	18	10 M€ / 2%
entités françaises concernées	secteurs d'activité visés	sanction max. (entités essentielles)

Point capital : dès lors que ces deux critères sont réunis, l'assujettissement est automatique. Contrairement à NIS 1, où les opérateurs étaient désignés individuellement par l'État, il n'y a pas de notification préalable à attendre : chaque organisation doit s'auto-évaluer et s'enregistrer auprès de l'ANSSI (plateforme MonEspaceNIS2). Certains acteurs sont même concernés quelle que soit leur taille (fournisseurs DNS, registres de noms de domaine, opérateurs télécoms, services de confiance qualifiés...).

Les sanctions prévues sont dissuasives et différenciées : jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires mondial pour les entités essentielles, 7 millions d'euros ou 1,4 % pour les entités importantes — avec en outre une responsabilité personnelle des dirigeants. Et l'effet dépasse ce périmètre : les entités assujetties devront exiger des garanties de leurs fournisseurs et sous-traitants, diffusant les exigences de NIS 2 dans toute la chaîne de valeur.



La conformité NIS 2 : une démarche globale, dont le contrôle d'accès est un maillon clé

La directive impose un socle de mesures de gestion des risques qui couvre l'ensemble de l'organisation :

- **Gouvernance et analyse de risques** : politique de sécurité formalisée, cartographie des systèmes critiques, implication et responsabilité des dirigeants.
- **Gestion et notification des incidents** : capacité à détecter, traiter et déclarer les incidents significatifs aux autorités dans des délais courts.
- **Continuité d'activité** : sauvegardes, plans de reprise et gestion de crise pour maintenir les services essentiels.
- **Sécurité de la chaîne d'approvisionnement** : évaluation de la sécurité des fournisseurs et des produits intégrés dans vos systèmes.
- **Hygiène informatique et formation** : sensibilisation des collaborateurs, gestion des mises à jour et des vulnérabilités.
- **Cryptographie et authentification** : chiffrement des données, authentification multifacteur, gestion rigoureuse des identités et des droits.
- **Sécurité physique et environnementale** : protection des locaux, des salles serveurs et des zones sensibles contre les accès non autorisés.



Pourquoi le contrôle d'accès physique est incontournable ?

C'est dans ce dernier pilier que le contrôle d'accès prend tout son sens — et il est loin d'être accessoire.

La meilleure défense logicielle ne protège de rien si un intrus peut pénétrer physiquement dans une salle serveurs, brancher un équipement sur le réseau ou dérober un poste de travail. NIS 2 impose donc de maîtriser qui accède à quelles zones, quand, et d'en garder la trace : restriction des accès aux zones sensibles selon le principe du moindre privilège, gestion du cycle de vie des badges (arrivées, mobilités, départs), traçabilité et journalisation des passages pour les audits et l'analyse post-incident.

Mais il y a un second enjeu, souvent oublié : le système de contrôle d'accès est lui-même un système d'information, connecté au réseau de l'entreprise. Mal sécurisé, il devient une porte d'entrée pour un attaquant, capable d'ouvrir des portes à distance ou de rebondir vers d'autres systèmes.

Pour être un atout de conformité et non un point faible, votre contrôle d'accès doit donc être :

- **Sécurisé** : communications chiffrées de bout en bout, badges à lecture sécurisée, équipements résistants aux attaques physiques.
- **À jour** : correctifs de sécurité déployés rapidement, versions maintenues, remplacement des systèmes en fin de support.
- **Et si possible certifié** : sa robustesse démontrée par une évaluation indépendante, plutôt que par la seule déclaration du fabricant.

La certification ANSSI : la preuve objective de robustesse

Comment savoir objectivement si une solution de contrôle d'accès est robuste ? C'est précisément le rôle du Visa de sécurité de l'ANSSI et de la certification CSPN (Certification de Sécurité de Premier Niveau). L'ANSSI fait évaluer les produits par un laboratoire indépendant agréé (CESTI), qui tente concrètement d'attaquer le produit : résistance du logiciel, sécurité des communications IP et de terrain, robustesse physique des équipements. Seuls les produits qui résistent obtiennent la certification, valable trois ans sur un périmètre précis décrit dans la Cible de Sécurité. Pour une entité soumise à NIS 2, s'appuyer sur des produits certifiés ANSSI est le moyen le plus solide de démontrer la robustesse de sa chaîne de contrôle d'accès lors d'un audit.

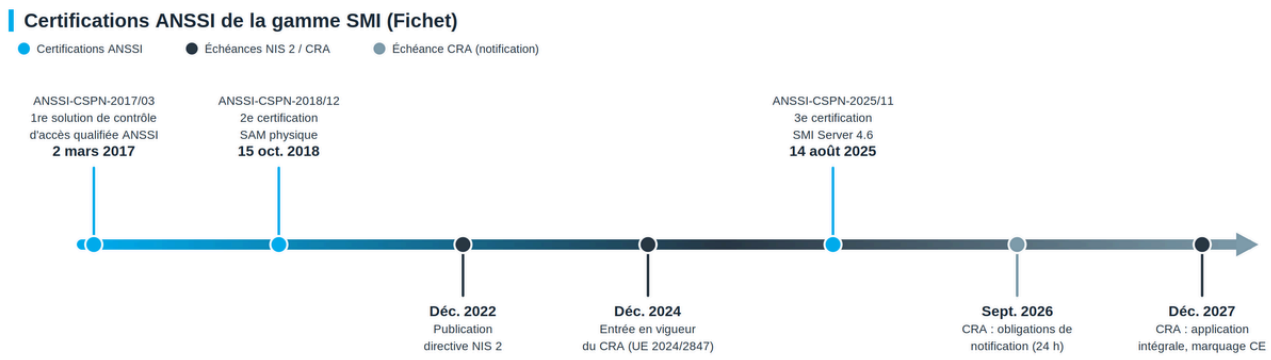


Schéma 1 — Le calendrier réglementaire européen (NIS 2, CRA) face au parcours de certification ANSSI de la gamme SMI.



SMI : pionnier et triple certifié

La sécurité certifiée est dans l'ADN de Fichet Group. Acteur historique de la haute sécurité physique (coffres-forts, portes blindées, cloisons sécurisées certifiés), Fichet Group applique la même exigence à son électronique de sécurité : nos solutions sont toujours certifiées, dans le monde physique comme dans le monde numérique. C'est ce qui a fait de Fichet Group l'un des tout premiers acteurs du contrôle d'accès à obtenir une certification : SMI a été la première solution de contrôle d'accès qualifiée par l'ANSSI.

Cette exigence s'inscrit dans la durée : SMI a été certifié trois fois : une première certification historique le 2 mars 2017 (ANSSI-CSPN-2017/03), une deuxième le 15 octobre 2018 (ANSSI-CSPN-2018/12) marquant l'évolution vers la SAM physique, puis SMI Server 4.6 le 14 août 2025 (référence ANSSI-CSPN-2025/11).

Cette troisième certification, réalisée selon le référentiel ANSSI le plus récent, couvre pour la première fois la résistance du matériel aux attaques physiques, la sécurité du logiciel de gestion du contrôle d'accès (GAC) et un renforcement de la sécurité des communications. Grâce à l'accord de reconnaissance mutuelle entre l'ANSSI et le BSI allemand, elle est également reconnue en Allemagne.

1ère	3x	14/08/25
solution de contrôle d'accès qualifiée ANSSI	**certifiée (2017, 2018, 2025)**	**date de la certification SMI Server 4.6**

La réponse de Fichet Group : souveraine, certifiée de bout en bout



Conçu, développé et fabriqué en France

Fichet Group s'attache à concevoir, développer et fabriquer ses solutions d'électronique de sécurité en France, dans ses deux centres de R&D et de tests. Le logiciel SMI Server, les UTL-IP SM400, les contrôleurs SM100+ et les lecteurs ProStyl sont développés et produits par Fichet Group, cartes électroniques comprises. Ce choix industriel est un gage de souveraineté numérique : il garantit la maîtrise complète de la chaîne d'approvisionnement et écarte le risque de compromission de la supply chain — composants d'origine incertaine, portes dérobées, dépendance à des législations extraterritoriales. Une exigence directement alignée avec le pilier « sécurité de la chaîne d'approvisionnement » de NIS 2.

Un engagement collectif : Fichet Group, membre de la SPAC

Fichet Group est membre de la SPAC (Smart Physical Access Control) Alliance, l'alliance européenne qui promeut la sécurisation et l'interopérabilité du contrôle d'accès physique, notamment via les protocoles sécurisés comme SSCP, et qui accompagne la filière dans la mise en conformité NIS 2. Cette implication traduit la conviction de Fichet Group : la cybersécurité du contrôle d'accès est un enjeu de filière, qui se construit sur des standards ouverts, évalués et souverains.

Une chaîne certifiée, du logiciel au badge

La certification CSPN de SMI Server 4.6 ne porte pas sur un composant isolé, mais sur la chaîne complète : le superviseur logiciel, les concentrateurs SM400/SM400-L, les contrôleurs SM100+ équipés d'une carte SAM physique certifiée EAL5+, et les lecteurs ProStyl avec lecture sécurisée de badges DESFire EV2/EV3. Les communications sont chiffrées de bout en bout, du réseau IP jusqu'au bus de terrain. La solution se déploie sur votre propre infrastructure (On-Premise), en pleine maîtrise de vos données, en architecture multi-sites et multi-sociétés.



Schéma 2 — L'architecture SMI certifiée ANSSI, du superviseur au badge.

Le « mode transparent » : vos clés de chiffrement hors d'atteinte

Cette architecture repose sur un principe de conception qui fait la différence sur le terrain : la lecture sécurisée en mode transparent. Dans une installation classique, le lecteur de badge fixé en façade contient les clés secrètes de chiffrement : arraché du mur, il peut livrer ces clés à un attaquant.

Avec SMI, le lecteur perd ce rôle de « détenteur de secrets » et se comporte comme une simple passerelle étanche : le dialogue cryptographique s'effectue directement entre le badge DESFire EV2/EV3 et le concentrateur situé en zone sécurisée, via un protocole chiffré et signé qui interdit toute attaque par rejeu ou injection de trames sur le câblage de terrain.

Les clés de l'organisation, elles, sont stockées de manière inviolable dans un module SAM physique — une puce cryptographique analogue à celle d'une carte bancaire — logé au cœur du concentrateur, à l'intérieur du bâtiment : aucun humain ni programme malveillant ne peut les en extraire.

Ce cloisonnement par niveaux garantit aussi la résilience opérationnelle exigée par NIS 2 : en cas de coupure réseau complète avec le serveur central, les concentrateurs SM400 et SM100+ continuent d'assurer localement le contrôle d'accès en temps réel, sans aucune dégradation de la sécurité.

Rester conforme dans la durée : SML, veille R&D et anticipation du CRA

Une certification photographie la robustesse d'un produit à un instant donné ; or les menaces, elles, évoluent en permanence. Parce que Fichet Group a pour ambition d'adresser le marché de la haute sécurité, sa R&D monitore en continu les vulnérabilités : veille sur les failles publiées, scans automatisés à chaque version (SonarQube, OWASP), détection des librairies obsolètes et tests de sécurité sur les produits.

Le fruit de cette veille est mis à disposition des clients via le SML (Service de Maintenance Logicielle) : les clients sous contrat SML disposent en permanence de versions à jour et disponibles de SMI Server, dont la compatibilité avec les évolutions de Windows et SQL Server est validée par Fichet Group. C'est le mécanisme concret qui permet de satisfaire l'exigence NIS 2 de maintien à jour des logiciels — avec un modèle forfaitaire qui maîtrise les coûts.

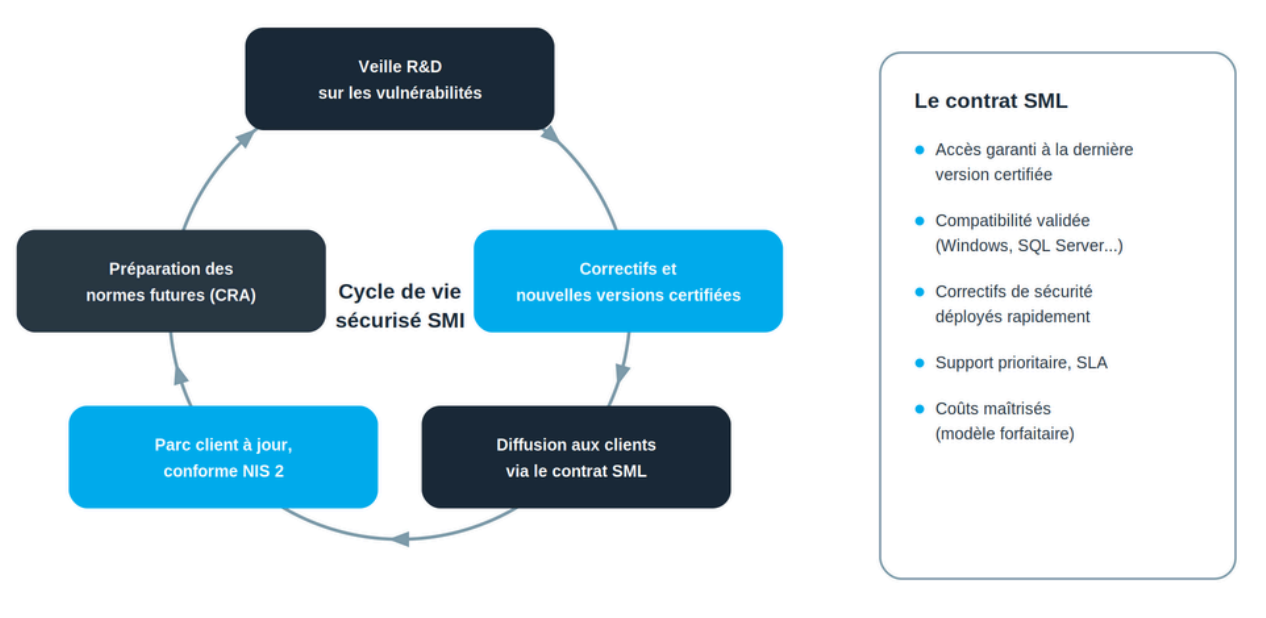


Schéma 3 — Le cycle de vie sécurisé SMI : de la veille R&D au parc client conforme, via le contrat SML.

Le CRA : la prochaine étape, déjà anticipée par Fichet Group

Après NIS 2, qui s'adresse aux organisations, le Cyber Resilience Act (règlement UE 2024/2847) s'adresse aux produits : c'est le premier règlement européen imposant des exigences de cybersécurité obligatoires à tout produit comportant des éléments numériques mis sur le marché de l'UE — logiciels comme matériels connectés — sur l'ensemble de leur cycle de vie. Il impose la sécurité dès la conception, la gestion et la notification des vulnérabilités (alerte sous 24 heures), la transparence via le SBOM (inventaire des composants logiciels) et un marquage CE cybersécurité. Son application est progressive : obligations de notification dès septembre 2026, application intégrale en décembre 2027, avec des sanctions pouvant atteindre 15 millions d'euros ou 2,5 % du chiffre d'affaires mondial.

Pour les clients, le CRA est une garantie supplémentaire : demain, seuls les fabricants capables de démontrer une gestion rigoureuse des vulnérabilités pourront vendre leurs produits en Europe. Fichet Group n'attend pas l'échéance : des développements et des modifications de produits ont d'ores et déjà été initiés pour rendre nos gammes compatibles CRA au plus tôt. La certification CSPN, la fabrication en propre des cartes électroniques et la chaîne CI/CD outillée constituent un socle d'avance considérable, complété par les chantiers en cours : formalisation de la politique de divulgation des vulnérabilités, SBOM au format standard, tests de pénétration renforcés et marquage CE cyber.

Passer à l'action : réussir la convergence cyber / physique en quatre étapes

La mise en conformité de votre sûreté physique est avant tout un travail d'équipe entre la Direction de la Sûreté et la DSI/RSSI — deux mondes qui ont longtemps évolué en parallèle et que NIS 2 oblige à converger. Fichet Group préconise une approche pragmatique en quatre étapes :

1. **CARTOGRAPHIER LES ACTIFS DE SÛRETÉ**	Inventaire exhaustif des équipements (lecteurs, contrôleurs, serveurs, caméras, centrales) et de leurs interconnexions avec le SI de l'entreprise (annuaire Active Directory, télémaintenance…).
2. **DURCIR L'ARCHITECTURE RÉSEAU**	Isoler le réseau de sûreté du réseau bureautique (VLAN, pare-feux), appliquer le moindre privilège sur la console d'administration et la protéger par une authentification multifacteur.
3. **RÉDIGER DES CAHIERS DES CHARGES CYBER-RÉSILIENTS**	Exiger contractuellement une certification étatique (CSPN de l'ANSSI) pour le logiciel et le matériel, proscrire les liaisons de terrain non chiffrées, et imposer un engagement de maintenance cyber dans la durée, aligné sur le CRA.
4. **ORGANISER UNE GOUVERNANCE MIXTE**	réunir Directeur de la Sûreté et RSSI dans un comité dédié, avec un plan conjoint de réponse aux incidents — une perte de liaison avec un contrôleur doit pouvoir être qualifiée immédiatement : malveillance physique ou logique ?

Pour vous aider à évaluer une offre, voici les questions clés à poser à votre intégrateur — et les réponses qu'apporte l'architecture SMI :

Question à poser	Objectif NIS 2 / CRA	Réponse de l'architecture SMI
Où sont stockées les clés de chiffrement des badges ?	Éliminer le risque d'extraction physique ou de vol des clés.	En zone sécurisée, dans des puces SAM physiques logées dans les concentrateurs (mode transparent).
Le logiciel de supervision dispose-t-il d'un visa de sécurité étatique ?	Sécuriser la chaîne d'approvisionnement technologique.	Oui : SMI Server est certifié CSPN par l'ANSSI, pour la 3e fois le 14 août 2025.
Comment sont protégés les flux IP sur le réseau ?	Garantir l'intégrité et la confidentialité des échanges.	Par des protocoles standardisés et chiffrés (TLS), du serveur au terrain.
Comment appliquez-vous les correctifs sur les équipements ?	Répondre à l'obligation de support cyber à long terme du CRA.	De manière centralisée et signée numériquement depuis SMI Server, sans déplacement sur site.

Un accompagnement de bout en bout : les services Fichet Group

Parce que chaque installation possède ses propres spécificités, Fichet Group, via son offre de services, accompagne ses clients à chaque étape de leur mise en conformité ANSSI : audit de l'installation existante et de son niveau de cybersécurité, préconisations d'architecture, déploiement des solutions certifiées et migration des systèmes en place.

Cet accompagnement se prolonge dans la durée avec le support et la maintenance des installations — maintenance préventive et corrective, assistance technique et déploiement des mises à jour du contrat SML — afin de garantir un système opérationnel et optimal tout au long de son cycle de vie.

En synthèse

- NIS 2 concerne des milliers d'organisations dans 18 secteurs, et sa conformité repose sur une démarche globale : gouvernance, incidents, continuité, chaîne d'approvisionnement, authentification — et sécurité physique.
- Le contrôle d'accès est un maillon obligatoire de cette démarche : il doit être sécurisé, maintenu à jour, et si possible certifié — car il est lui-même un système d'information exposé.
- La certification ANSSI est la preuve objective de robustesse : SMI, première solution de contrôle d'accès qualifiée par l'ANSSI, a été certifiée trois fois — la dernière le 14 août 2025 pour SMI Server 4.6.
- Fichet Group offre une chaîne souveraine de bout en bout : conçue, développée et fabriquée en France, certifiée du logiciel au badge, déployée sur votre propre infrastructure, et portée par un engagement de filière au sein de la SPAC.
- La convergence cyber/physique se conduit avec méthode : cartographier, durcir le réseau, exiger la certification dans vos cahiers des charges, et gouverner ensemble sûreté et SSI.
- La conformité se maintient dans la durée : veille R&D permanente, versions à jour garanties par le contrat SML, anticipation du Cyber Resilience Act déjà engagée sur nos produits — et l'appui des services Fichet Group pour l'audit, le support et la maintenance de vos installations.

Choisir un contrôle d'accès certifié ANSSI, c'est transformer une contrainte réglementaire en avantage : celui d'un système de sûreté dont la robustesse est prouvée, maintenue et souveraine. Nos équipes se tiennent à votre disposition pour évaluer la conformité de votre installation et construire avec vous votre trajectoire NIS 2.



FICHET

7 RUE PAUL DAUTIER
78140 - VELIZY-VILLACOUBLAY
www.fichetgroup.com