ALCEA
ASSA ABLOY



cybersécurité
des solutions
d'accès sans clé.

alceaglobal.com

sommaire.

4 Introduction.
5 Pourquoi la cybersécurité est-elle essentielle ?
6 La cybersécurité au cœur des infrastructures critiques.
7 accès sans clé : garantir la sécurité des données à chaque étape.
8 Déployer les couches essentielles de cybersécurité.
9 Qu’est-ce que le chiffrement ?
11 Risques et cyberattaques
12 Solutions de verrouillage numériques disponibles sur le marché.
14 Découvrez les solutions d’accès sans clé ALCEA.
16 Atouts de sécurité des solutions d’accès sans clé ALCEA.
18 Comment fonctionne ABLOY CUMULUS ?
20 Guide pratique : les solutions sans clé ALCEA sont-elles faites pour vous ?
21 Votre sûreté, notre priorité
22 Glossaire.



introduction.

La transformation numérique modifie profondément la manière dont les infrastructures critiques sont exploitées et protégées. Dans tous les secteurs d'activité, les organisations déploient des technologies connectées afin de simplifier les opérations quotidiennes, d'améliorer la visibilité sur leurs activités et de mieux contrôler l'accès à leurs sites et à leurs actifs.

À mesure que le contrôle d'accès évolue des solutions mécaniques vers des solutions numériques et sans fil, la cybersécurité devient un enjeu central. Les dispositifs sans fil et les identifiants mobiles offrent de nouvelles possibilités en matière de flexibilité et d'efficacité, mais exigent également une approche différente de la sûreté. La protection ne se limite plus au verrou lui-même : elle englobe désormais les logiciels, les communications, les comportements des utilisateurs et l'architecture globale du système.

Dans ce livre blanc, nous expliquons comment déployer des solutions d'accès sans fil de manière sûre et sécurisée, et présentons les principes essentiels de cybersécurité à prendre en compte dans la gestion des accès.

Protéger les données grâce au chiffrement

Pour de nombreux collaborateurs, le smartphone est déjà un outil de travail essentiel. Il sert à communiquer, planifier, s'authentifier et accompagner les activités quotidiennes, souvent sur plusieurs sites.

L'utilisation du smartphone comme clé numérique s'inscrit naturellement dans cette évolution. Les identifiants numériques permettent aux personnes autorisées d'accéder aux bâtiments et aux zones sécurisées sans clé physique, qu'il s'agisse de sites de proximité ou de sites distants. Les droits d'accès peuvent être gérés de manière centralisée, mis à jour rapidement et adaptés aux besoins opérationnels, tout en garantissant un contrôle rigoureux et une traçabilité complète.

Comprendre les environnements d'accès et les besoins en connectivité

Tous les sites ne présentent pas les mêmes contraintes. Certains sont connectés en permanence, tandis que d'autres fonctionnent avec une connectivité limitée, voire inexistante. Certains nécessitent un pilotage en temps réel, alors que d'autres privilégient la disponibilité et la résilience des installations.

Avant de déployer une solution d'accès numérique, il est essentiel d'évaluer précisément la situation existante : comment les accès sont gérés aujourd'hui, où la connectivité est disponible et où une communication sécurisée entre les équipements et les systèmes est nécessaire. Dans ce contexte, les passerelles jouent un rôle clé en permettant les échanges de données contrôlés, la supervision des systèmes et la gestion sécurisée des points d'accès. Cette analyse préalable permet de concilier sécurité, simplicité d'utilisation et exigences opérationnelles dès le début du projet.

Faire de la cybersécurité un pilier de confiance

La cybersécurité ne repose pas uniquement sur la technologie. Elle dépend également des comportements, des bonnes pratiques et de la responsabilité de chacun. Même les systèmes les plus avancés nécessitent une utilisation adaptée et une gouvernance claire.

La confiance est au cœur de la gestion des accès numériques : confiance dans les équipements qui contrôlent les accès, dans les systèmes qui gèrent les autorisations et dans les utilisateurs qui les exploitent au quotidien. Lorsque la cybersécurité est intégrée dès la conception des solutions, les accès sans fil contribuent à rendre les infrastructures critiques plus sûres, plus efficaces et plus faciles à administrer.

pourquoi la cybersécurité est-elle essentielle ?

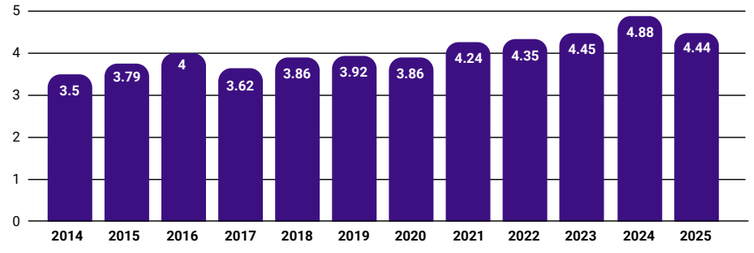
Aujourd'hui, tout est connecté et numérique. Les organisations s'appuient sur des réseaux en ligne et des équipements connectés pour fonctionner efficacement. Cette connectivité accrue favorise la performance et la collaboration, mais elle expose également les entreprises à des risques croissants en matière de cybersécurité.

Les cybermenaces évoluent en permanence et peuvent compromettre la sécurité des personnes, perturber les activités d'une entreprise ou affecter des infrastructures essentielles. Face à ces enjeux, la cybersécurité ne peut plus être considérée comme une simple couche de protection supplémentaire. Elle doit être intégrée dès la conception des solutions afin de préserver l'intégrité des systèmes, d'assurer la continuité des opérations et de maintenir la confiance des utilisateurs.

Le saviez-vous ?

La cybercriminalité se divise principalement en deux catégories : les violations de données et les actes de sabotage. Les violations de données visent à obtenir des informations sensibles, qu'il s'agisse de données personnelles, de données stratégiques ou de propriété intellectuelle. Les actes de sabotage, quant à eux, ont pour objectif de perturber le fonctionnement des infrastructures et des opérations critiques. Selon IBM, le coût moyen mondial d'une violation de données a connu une évolution notable en 2025. Pour la première fois en cinq ans, ce coût a diminué pour atteindre 4,44 millions de dollars, grâce à l'utilisation de l'intelligence artificielle et de l'automatisation par les équipes de sécurité, qui détectent et contiennent les incidents plus rapidement. Dans le même temps, les cybercriminels exploitent eux aussi l'IA générative pour mener des campagnes d'hameçonnage plus convaincantes et créer de faux contenus, notamment des deepfakes, toujours plus difficiles à détecter.Malgré cette baisse observée à l'échelle mondiale, les coûts liés aux violations de données ont atteint un niveau record aux États-Unis.
(Source : IBM)

Coût moyen mondial d'une violation de données, de 2014 à 2025
(en millions de dollars américains)



Source : IBM, Cost of a Data Breach Report 2025, ibm.com/reports/data-breach

la cybersécurité au cœur des infrastructures critiques.

Les responsables de la sûreté, de la sécurité des systèmes d'information et des opérations au sein des infrastructures critiques supervisent des activités complexes et interconnectées. De nombreux services devant fonctionner en continu, la résilience, la disponibilité des systèmes ainsi que la protection des biens et des personnes constituent des priorités absolues.

Les infrastructures s'appuient sur des dispositifs connectés pour assurer la surveillance, le suivi des équipements et la gestion des accès, tout en respectant les réglementations et exigences locales. Toute interruption, qu'elle soit d'origine physique ou numérique, peut avoir d'importantes conséquences opérationnelles et compromettre la sûreté des installations.

Du point de vue de la sécurité de l'information, l'évaluation du niveau de cybersécurité reste souvent complexe. Comparer les solutions disponibles et mesurer l'impact réel des différents mécanismes de protection n'est pas toujours évident, d'autant que les menaces et les technologies évoluent en permanence. L'augmentation de la puissance de calcul accroît également les exigences en matière de chiffrement et d'autres mesures de protection, faisant de la sécurité à long terme un enjeu essentiel.

Ce livre blanc met en lumière les principaux enjeux de cybersécurité associés à la gestion des accès sans clé afin d'aider les décideurs des infrastructures critiques à faire des choix éclairés.



accès sans clé : garantir la sécurité des données à chaque étape.

Le chiffrement constitue le fondement de la cybersécurité dans la gestion numérique des accès. Il permet de protéger les données, de vérifier les identités et de garantir que les communications entre les appareils et les systèmes ne peuvent être ni lues ni manipulées par des tiers non autorisés. Dans les solutions d'accès sans fil, le chiffrement assure la confidentialité et l'intégrité des commandes, des identifiants et des mises à jour du système, même lorsqu'ils transitent par des réseaux publics ou partagés. Sans mécanismes de chiffrement robustes, les systèmes de contrôle d'accès numériques seraient exposés aux risques d'interception, de duplication ou de manipulation.

Loin d'être un concept complexe ou abstrait, le chiffrement constitue la première couche essentielle de cybersécurité dans la gestion des accès sans fil. Il crée un environnement numérique de confiance dans lequel les données sont protégées dès leur conception. Sur cette base sécurisée viennent s'ajouter d'autres niveaux de protection, comme l'authentification et l'autorisation, qui garantissent que seuls les utilisateurs et les appareils vérifiés peuvent demander un accès et que les droits accordés sont strictement maîtrisés. Ensemble, ces différentes couches de protection permettent aux systèmes d'accès sans fil de fonctionner de manière fiable, sécurisée et évolutive, même au sein d'environnements critiques où les exigences de sûreté et de continuité d'exploitation sont particulièrement élevées.

Protéger les données grâce au chiffrement

Le chiffrement protège les données en les transformant en informations illisibles pour toute personne ne disposant pas des autorisations nécessaires. Dans les systèmes d'accès sans fil, il permet de sécuriser les communications entre les dispositifs d'accès, les passerelles, les appareils mobiles et les plateformes de gestion.

Ainsi, les identifiants d'accès, les commandes et les informations d'état restent protégés, même si les échanges de données venaient à être interceptés. Un chiffrement robuste garantit à la fois la confidentialité et l'intégrité des données : celles-ci ne peuvent être ni lues, ni modifiées, ni réutilisées à des fins malveillantes sans être détectées. Pour les infrastructures critiques, cette protection est essentielle afin d'empêcher tout accès non autorisé et de renforcer la confiance dans les systèmes d'accès numériques opérant dans des environnements exposés ou isolés.

Sécuriser les équipements grâce aux mises à jour du firmware

La cryptographie joue également un rôle clé dans la protection à long terme des dispositifs d'accès. Les serrures connectées, cadenas électroniques et contrôleurs s'appuient sur un firmware, c'est-à-dire le logiciel embarqué qui pilote leur fonctionnement.

Les mécanismes sécurisés de mise à jour du firmware garantissent que seuls des logiciels authentifiés peuvent être installés sur les équipements. Grâce à la vérification cryptographique, toute tentative d'installation d'un logiciel modifié ou malveillant est bloquée. Ces mises à jour permettent également de corriger les vulnérabilités et de renforcer en continu le niveau de cybersécurité.

En associant un chiffrement robuste à des processus sécurisés de mise à jour du firmware, les solutions d'accès sans clé et sans fil maintiennent un niveau élevé de protection tout au long de leur cycle de vie, contribuant ainsi à la sûreté des opérations et à la résilience des infrastructures critiques.

déployer les couches essentielles de cybersécurité.

L’association de plusieurs couches de cybersécurité permet de renforcer la sûreté physique des installations. Trois mécanismes essentiels doivent être mis en œuvre : le chiffrement, l’authentification et l’autorisation..

1. Chiffrement
Le chiffrement protège les données échangées entre les appareils en les rendant illisibles pour toute personne non autorisée. Il garantit la confidentialité et l’intégrité des informations transmises au sein du système de gestion des accès.

2. Authentification
L’authentification vérifie l’identité de l’utilisateur et du système de gestion des accès avant toute attribution ou utilisation de droits d’accès. Elle peut s’appuyer sur l’identification dans l’application, la sécurisation de l’appareil (mot de passe, code PIN) ou encore des données biométriques telles que l’empreinte digitale ou la reconnaissance faciale. En cas d’échec de la vérification, l’accès est refusé.

3. Autorisation
L’autorisation détermine les actions qu’un utilisateur est autorisé à réaliser ainsi que les droits d’accès qui lui sont accordés. Par exemple, elle peut empêcher le partage de droits d’accès avec d’autres personnes et garantir que chaque utilisateur ne puisse utiliser que ses propres autorisations. Ce contrôle contribue à renforcer la sûreté des installations et des opérations.

qu’est-ce que le chiffrement ?

Le chiffrement consiste à rendre les données illisibles pour toute personne non autorisée. Il protège les informations échangées entre les appareils en les transformant en un format incompréhensible sans la clé appropriée. Il existe deux principales méthodes de chiffrement : le chiffrement symétrique, qui utilise une même clé pour chiffrer et déchiffrer les données, et le chiffrement asymétrique, qui repose sur des clés uniques propres à chaque appareil.

Dans les solutions d’accès sans clé ALCEA, le chiffrement asymétrique protège les droits d’accès et les communications entre le système de gestion des accès, les passerelles, les dispositifs d’accès et les identifiants mobiles. Les données sont ainsi chiffrées de bout en bout et ne peuvent être lues que par les systèmes autorisés.

Chaque dispositif d’accès dispose de ses propres clés cryptographiques. Ainsi, une information destinée à un équipement ne peut pas être déchiffrée par un autre. Cette isolation limite l’impact d’une éventuelle compromission et contribue à la protection des systèmes d’accès déployés dans les infrastructures critiques.



quels sont les risques et les cyberattaques ?

Attaques par force brute

Lors d'une attaque par force brute, un attaquant tente d'obtenir un accès en essayant systématiquement différents mots de passe ou identifiants. Dans les systèmes de contrôle d'accès bien conçus, ce risque est limité grâce à un chiffrement robuste et à la protection des identifiants. Les informations d'identification chiffrées ne peuvent pas être exploitées efficacement par de simples tentatives de devinette. Bien que ce type d'attaque soit théoriquement possible, contourner les mécanismes de chiffrement modernes nécessiterait un niveau de temps et de ressources irréaliste, ce qui les rend inefficaces dans des conditions réelles.

Vol ou perte d'appareils : serrures, smartphones et identifiants

La perte ou le vol d'équipements constitue un risque réaliste dans les environnements opérationnels. Les systèmes d'accès sans fil sont conçus pour en limiter l'impact. Chaque appareil utilise des clés cryptographiques uniques, ce qui signifie qu'une serrure compromise ne peut pas affecter les autres appareils ni l'ensemble du système.

Les appareils mobiles reposent sur le même principe. Les smartphones s'appuient sur des mécanismes de sécurité intégrés tels que les codes PIN, les mots de passe et l'authentification biométrique. Les droits d'accès sont limités dans le temps et peuvent être révoqués à distance en cas de perte ou de compromission de l'appareil. Cela garantit que les risques restent maîtrisés, même dans des environnements distribués.

Ingénierie sociale et facteur humain

Certaines attaques ciblent les personnes plutôt que la technologie. L'ingénierie sociale vise à manipuler les utilisateurs pour qu'ils divulguent leurs identifiants ou contournent les procédures de sécurité, ce qui en fait l'un des risques les plus fréquents dans la pratique.

Les systèmes de contrôle d'accès réduisent cette exposition en limitant le recours aux informations partagées et aux processus manuels. Une authentification forte, une gestion stricte des autorisations et une administration centralisée des accès contribuent à prévenir les usages abusifs. Associées à des procédures claires et à la sensibilisation des utilisateurs, ces mesures réduisent considérablement l'impact des erreurs humaines.

Vulnérabilités logicielles et composants open source

Les solutions modernes de contrôle d'accès reposent sur des logiciels, y compris des composants open source. Bien qu'ils favorisent la flexibilité et l'innovation, des vulnérabilités peuvent apparaître si elles ne sont pas gérées de manière proactive.

Une cybersécurité efficace repose sur une surveillance continue, des pratiques de développement sécurisées et la capacité à déployer rapidement des mises à jour. Une connectivité maîtrisée et une architecture système robuste permettent de corriger efficacement les vulnérabilités, garantissant ainsi la sécurité et la confiance sur le long terme.

solutions de verrouillage numériques disponibles sur le marché.

Les solutions de verrouillage numérique sont largement utilisées pour sécuriser les infrastructures critiques, offrant un meilleur contrôle des accès, une traçabilité accrue et une protection renforcée des actifs sensibles. Elles peuvent être déployées dans des environnements filaires ou sans fil, selon les conditions du site, les exigences opérationnelles et les besoins en matière de sécurité.

Dans les infrastructures critiques, les conditions physiques et la connectivité varient considérablement. Certains sites sont connectés, tandis que d'autres sont isolés ou disposent d'un accès réseau limité. Les solutions filaires peuvent offrir une connectivité continue, mais elles sont souvent contraintes par les exigences d'installation, les emplacements fixes et la disponibilité des infrastructures. Les solutions sans fil répondent à nombre de ces limitations en permettant un déploiement flexible dans des environnements étendus et géographiquement dispersés.

Les serrures Bluetooth® alimentées par batterie sont couramment utilisées dans les solutions d'accès sans clé, car elles associent la flexibilité du sans-fil à une excellente autonomie énergétique. Conçues spécifiquement pour les accès numériques, elles prennent en charge une gestion sécurisée des identifiants, un déploiement à grande échelle et un fonctionnement durable dans des environnements exigeants. Lorsque les dispositifs d'accès sont développés dès l'origine pour un usage sans clé, ils offrent une meilleure expérience utilisateur, un niveau de sécurité supérieur et une plus grande robustesse que les solutions adaptées à partir de concepts de verrouillage traditionnels. Par ailleurs, les solutions modernes d'accès sans clé sont conçues pour fonctionner en parfaite complémentarité avec les systèmes de verrouillage mécanique éprouvés. Elles permettent ainsi aux organisations de faire évoluer progressivement leurs installations, à leur propre rythme, sans compromettre la sécurité ni la continuité des opérations.

Créer un écosystème d'accès numérique connecté

Les solutions modernes de verrouillage numérique s'intègrent dans un écosystème d'accès connecté, où serrures, identifiants mobiles, composants de connectivité sécurisés et logiciels de gestion fonctionnent ensemble au sein d'une même infrastructure.

Ces différents éléments permettent une communication sécurisée entre les dispositifs d'accès et les systèmes centraux. Ils facilitent la supervision, la mise à jour des droits d'accès et la gestion des autorisations sur plusieurs sites, y compris dans des environnements où la connectivité est limitée ou intermittente.

En associant des dispositifs d'accès Bluetooth® à une connectivité assurée par des passerelles sécurisées, les organisations bénéficient d'une meilleure visibilité sur leurs installations et d'une réactivité accrue face à des événements tels que les tentatives d'accès non autorisées ou les actes de sabotage. Cette approche réduit la nécessité des interventions sur site et renforce la capacité à surveiller et protéger les infrastructures critiques en temps réel.

Conçu pour les réalités des infrastructures critiques

Les solutions d'accès sans clé doivent être conçues pour répondre aux exigences spécifiques des infrastructures critiques : cycles de vie longs, environnements difficiles, sites isolés et exigences élevées en matière de sûreté et de cybersécurité.

Les dispositifs d'accès sont conçus pour fonctionner pendant plusieurs années sur batterie et prendre en charge des milliers de cycles d'ouverture sans compromettre leurs performances. Les systèmes peuvent également fonctionner aussi bien en ligne que hors ligne, permettant une utilisation sécurisée des droits d'accès même en l'absence de couverture réseau. Lorsque la connectivité est disponible, les passerelles assurent la synchronisation des données, la supervision et les mises à jour du système.

Ces capacités permettent aux organisations de déployer des solutions de verrouillage numérique flexibles, résilientes et évolutives, capables de répondre aux besoins actuels tout en s'adaptant aux futures exigences opérationnelles et de sécurité.



découvrez les solutions d’accès sans clé ALCEA.

Les solutions d’accès sans clé ALCEA sont conçues pour protéger les infrastructures critiques, où les accès doivent être à la fois sûrs, flexibles et fiables, y compris sur des sites isolés, étendus ou soumis à des contraintes exigeantes.

Le portefeuille ALCEA comprend notamment ABLOY CUMULUS, une solution de gestion des accès sans fil spécialement développée pour les infrastructures critiques. Grâce aux identifiants mobiles et à la technologie Bluetooth®, elle permet un accès sécurisé sans clé aux équipements et aux actifs, aussi bien en mode connecté que hors ligne selon les conditions du site.

Dès leur conception, les solutions d’accès sans clé ALCEA intègrent de multiples couches de cybersécurité pour protéger les droits d’accès, les communications et les équipements. Elles offrent ainsi un haut niveau de protection aujourd’hui tout en restant capables de répondre à l’évolution des technologies et des menaces.

Pourquoi les solutions keyless d’ALCEA sont-elles sécurisées ?

La cybersécurité des solutions d’accès sans clé d’ALCEA repose sur une combinaison de chiffrement, d’authentification et de contrôle des autorisations.

Le chiffrement protège l’ensemble des données échangées entre les différents composants du système en les rendant illisibles pour toute personne non autorisée. Les communications entre les dispositifs d’accès, les identifiants mobiles, les composants de connectivité et les plateformes de gestion sont sécurisées à l’aide de méthodes cryptographiques robustes et conformes aux standards du secteur. Les droits d’accès, les commandes et les données des équipements restent ainsi confidentiels et ne peuvent pas être altérés pendant leur transmission.

L’authentification garantit que seuls les utilisateurs et les équipements de confiance peuvent interagir avec le système. Chaque serrure, terminal, application ou composant dispose d’une identité unique et vérifiée, et toutes les interactions sont validées avant qu’un accès ne soit accordé. Les droits d’accès sont attribués pour une durée limitée et peuvent être révoqués de manière centralisée en cas de perte, de vol ou de suspicion de compromission d’un appareil.

L’association de ces mécanismes garantit que seuls les utilisateurs autorisés peuvent accéder aux ressources protégées, que les données restent sécurisées de bout en bout et que l’impact d’un appareil compromis est maîtrisé. Cette approche permet d’assurer une gestion des accès sans clé à la fois sécurisée, résiliente et adaptée aux exigences des infrastructures critiques.



Mises à jour du firmware et correction des vulnérabilités

Les vulnérabilités potentielles sont identifiées grâce à des activités continues de recherche et de tests de sécurité. Lorsqu’une mise à jour est nécessaire, les correctifs de firmware peuvent être déployés de manière sécurisée sur les équipements compatibles.

Les mises à jour sont appliquées dès qu’une connexion est disponible, sans perturber le fonctionnement normal des équipements. Elles permettent de maintenir un haut niveau de cybersécurité dans le temps tout en garantissant la continuité des accès, même dans les environnements où la connectivité réseau est limitée ou intermittente.

atouts de sécurité des solutions d'accès sans clé ALCEA.

Identification sécurisée et simplifiée des utilisateurs

Accès maintenus même sans couverture réseau

Mise à jour du firmware à distance via tout smartphone utilisateur autorisé

Chiffrement de bout en bout des communications

Authentification basée sur une infrastructure PKI mondiale

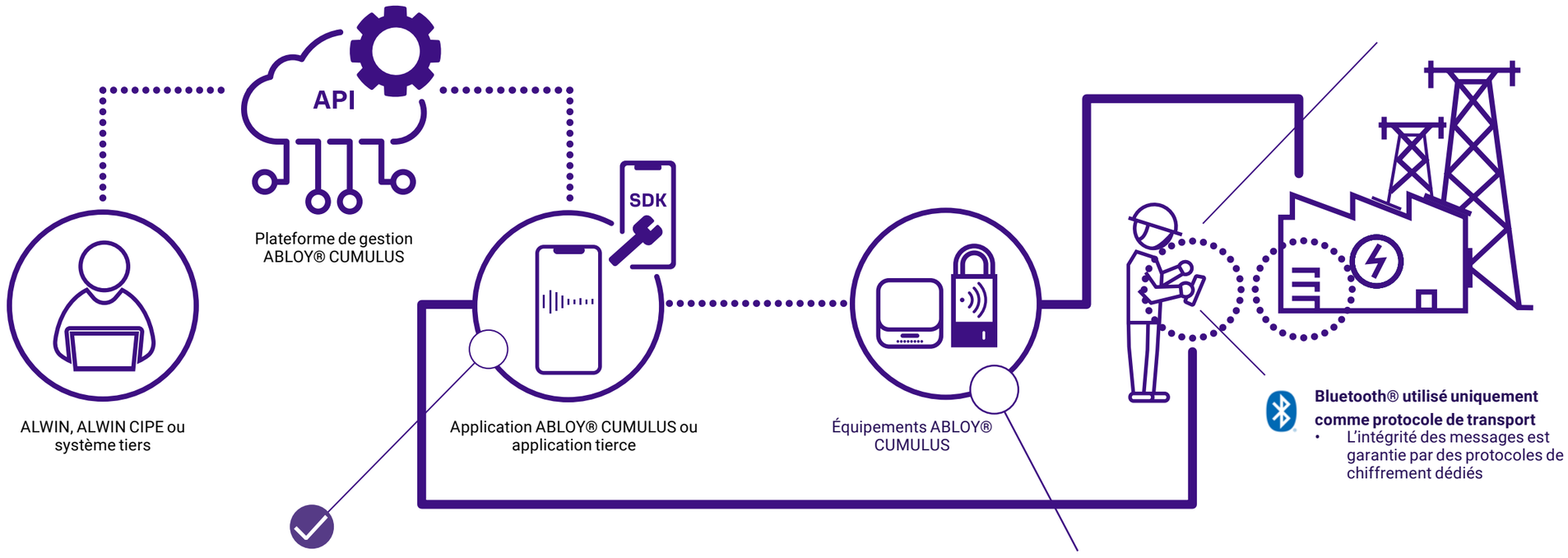
Cybersécurité validée par des organismes indépendants



comment fonctionne ABLOY CUMULUS ?

Les identifiants mobiles, ou droits d'accès, sont stockés sur le smartphone de l'utilisateur dans un Secure Enclave, tandis que les informations associées à ces identifiants sont conservées dans le cloud. Toutes les données échangées entre les différents équipements transitent par Internet. Ce qui rend une solution cybersécurisée, c'est la mise en place et le respect de protocoles de sécurité à chaque étape du cycle de vie des identifiants, afin de prévenir les attaques et les accès non autorisés.

Public Key Infrastructure (PKI) and private key identity
- Chiffrement asymétrique sans secret partagé
- Certificats PKI conformes à la norme X.509



Bluetooth® utilisé uniquement comme protocole de transport
- L'intégrité des messages est garantie par des protocoles de chiffrement dédiés

Gestionnaire de services de confiance (TSM)
- Permet l'enregistrement sécurisé d'un appareil mobile
- Les invitations ne peuvent être émises que par l'organisation d'origine

Canal de communication sécurisé de bout en bout
- La serrure fait uniquement confiance à notre système d'administration central
- Réduit les risques d'attaque de type « homme du milieu » (Man-in-the-Middle)

guide pratique : les solutions sans clé ALCEA sont-elles faites pour vous ?

Notre portefeuille de solutions sans clé évolue en permanence pour répondre aux enjeux de sécurité, de connectivité et de pérennité des infrastructures. Les questions suivantes peuvent vous aider à déterminer si une solution d'accès sans clé est adaptée à votre organisation :

- Souhaitez-vous disposer d'informations en temps réel sur vos actifs les plus critiques ?
- Voulez-vous éliminer les risques liés à la perte de clés et supprimer les contraintes de gestion des clés physiques ?
- Avez-vous besoin de suivre les mouvements des collaborateurs, prestataires ou visiteurs au sein de vos sites ?
- Souhaitez-vous gérer les accès, les équipements et les autorisations à distance, où que vous soyez ?
- Pourriez-vous réduire vos coûts d'exploitation et vos déplacements grâce à une logistique simplifiée ?
- Recherchez-vous une solution d'accès capable de s'intégrer à vos systèmes existants ?
- Souhaitez-vous renforcer votre niveau de protection et rester à la pointe de la sécurisation des infrastructures critiques ?

Si vous avez répondu « oui » ou « peut-être » à l'une de ces questions, échangez avec nos spécialistes pour découvrir comment les solutions sans clé ALCEA peuvent répondre à vos enjeux de sécurité et de gestion des accès.

Contactez-nous

Votre sécurité, notre priorité : notre politique de sécurité.

La divulgation responsable des vulnérabilités contribue à garantir que les infrastructures de contrôle d'accès sont continuellement testées et démontrent un niveau de fiabilité élevé. C'est pourquoi ALCEA, en tant que membre du groupe ASSA ABLOY, accorde une importance majeure à la cybersécurité et à la gestion responsable des signalements de vulnérabilités. Nous reconnaissons la contribution précieuse des chercheurs en sécurité et des experts en analyse des vulnérabilités qui participent au renforcement de la sécurité des infrastructures d'accès critiques.

Nos équipes de sécurité collaborent étroitement à l'échelle du groupe ASSA ABLOY, en combinant des expertises issues des domaines de la sécurité physique, du contrôle d'accès numérique et de la cybersécurité. ALCEA participe également activement aux initiatives de collaboration sectorielle et aux travaux de normalisation, contribuant ainsi au développement de technologies d'accès sécurisées, fiables et pérennes pour répondre aux enjeux de demain.

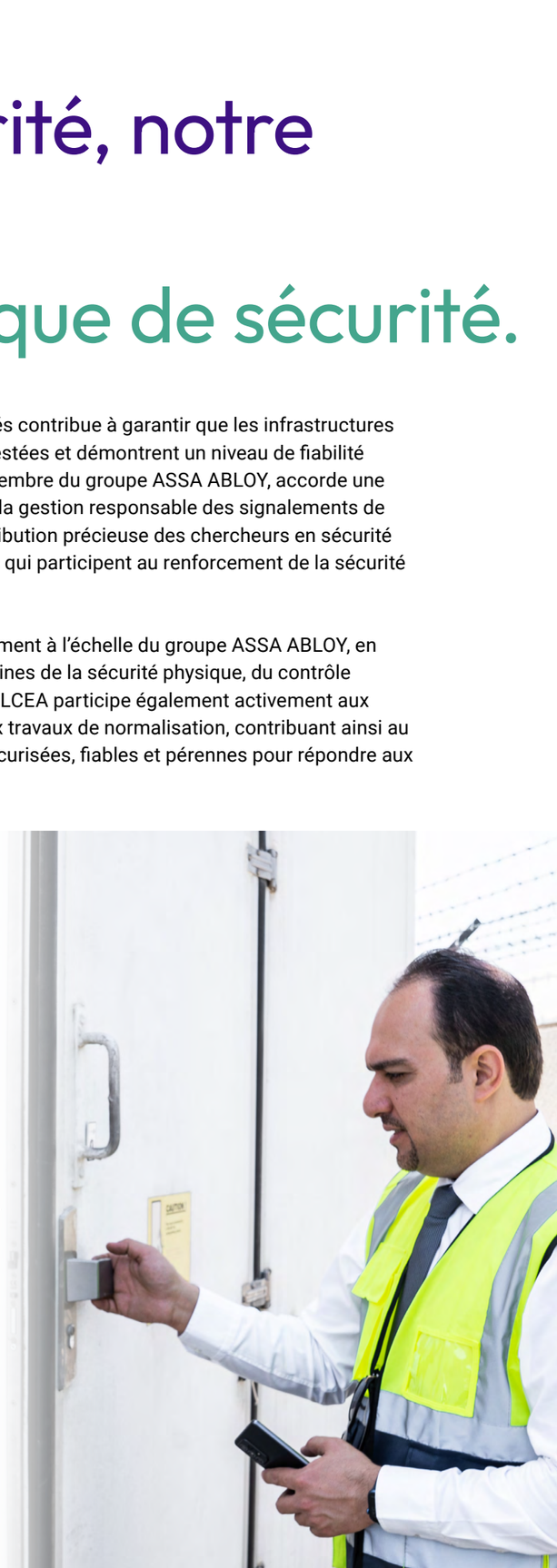
Pour ALCEA, la divulgation responsable des vulnérabilités est essentielle pour améliorer la qualité de ses produits et services, tout en protégeant les clients qui leur font confiance. C'est pourquoi nous avons mis en place une politique de sécurité reposant sur les principes suivants :

ALCEA communique de manière responsable aux clients les vulnérabilités connues ainsi que les correctifs associés, en veillant à protéger à la fois ses clients et ses solutions.

ALCEA encourage le dialogue et la collaboration avec les chercheurs en sécurité, dans l'objectif commun d'améliorer la sécurité et de coordonner la divulgation responsable des vulnérabilités ainsi que des mesures correctives correspondantes.

Consultez notre security policy.

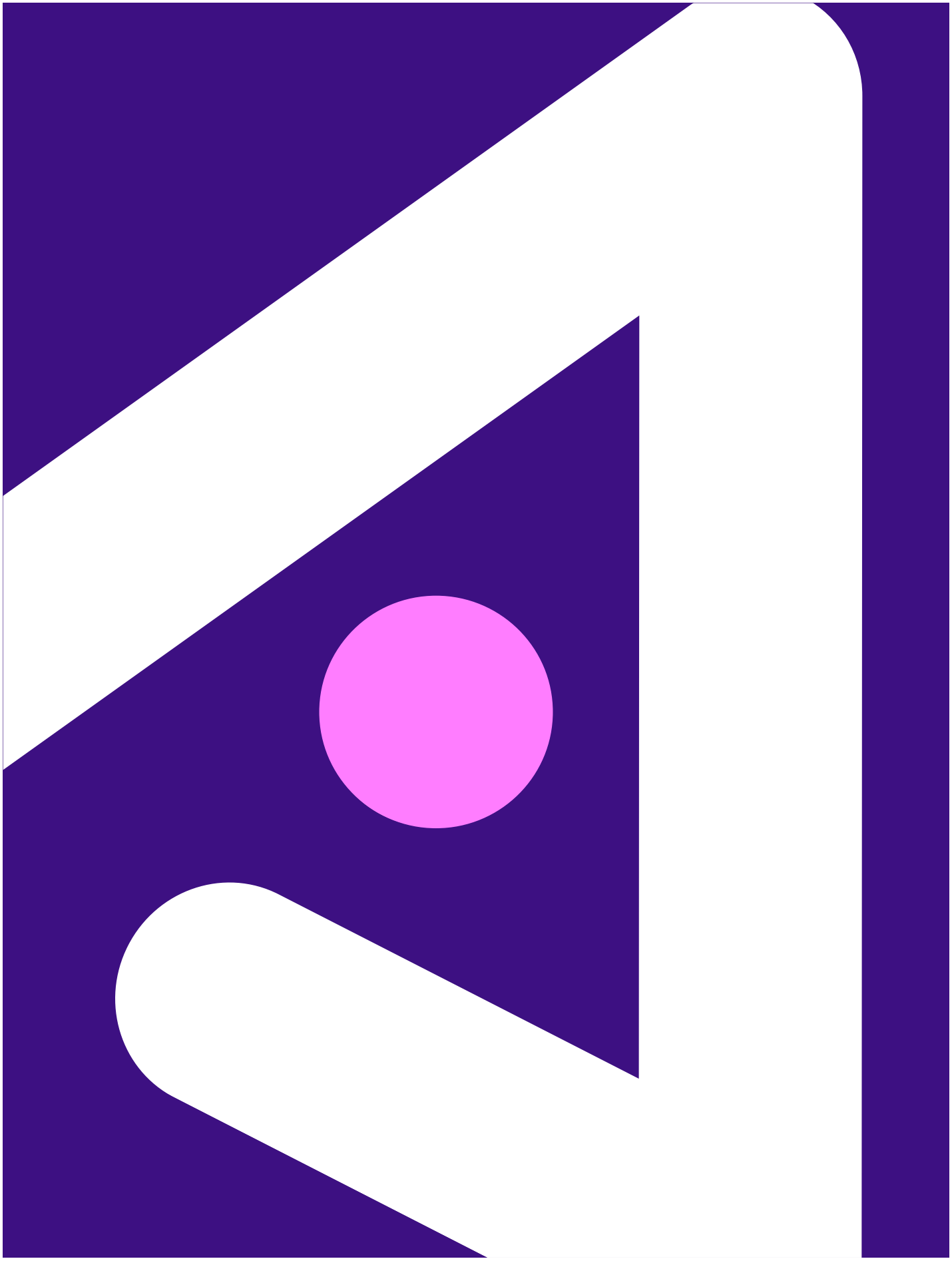
Découvrez notre NIS2 ebook



glossaire.

- **Chiffrement asymétrique** = Méthode de chiffrement utilisant des clés distinctes pour le chiffrement et le déchiffrement des données. Il est également connu sous le nom d'infrastructure à clés publiques (PKI).
- **Authentification** = Couche essentielle de cybersécurité permettant de vérifier l'identité de l'utilisateur et du système de gestion des accès avant toute utilisation des droits d'accès..
- **Autorisation** = Couche essentielle de cybersécurité définissant les actions qu'un utilisateur est autorisé à effectuer ainsi que les droits qui lui sont attribués.
- **BLE (Bluetooth® Low Energy)** = Norme de communication sans fil à faible consommation d'énergie permettant l'échange de données entre appareils.
- **Cloud** = Infrastructure de stockage et de traitement de données hébergée sur des serveurs accessibles à distance via Internet..
- **Chiffrement** = Couche essentielle de cybersécurité consistant à rendre les données illisibles pour toute personne ou tout système non autorisé.
- **Chiffrement de bout en bout (E2EE)** = Méthode de protection des données garantissant que seules les parties autorisées peuvent lire les informations échangées. Les données sont chiffrées par l'émetteur et ne sont déchiffrées que par le destinataire.
- **IoT (Internet des objets)** = Ensemble d'objets et d'équipements connectés capables de communiquer, d'échanger et d'exploiter des données.
- **NFC (Near Field Communication)** = Technologie de communication sans fil à courte portée permettant à des appareils proches d'échanger des informations.

- **PKI (Infrastructure à clés publiques)** = Ensemble de politiques, processus, matériels et logiciels permettant de créer, gérer et distribuer des certificats numériques et des clés cryptographiques.
- **SaaS (Software as a Service)** = Modèle de service dans lequel une application est hébergée dans le cloud et accessible via Internet. Le fournisseur assure l'exploitation, la maintenance et la sécurité de la solution. ABLOY CUMULUS est un exemple de solution SaaS.
- **Chiffrement symétrique** = Méthode de chiffrement dans laquelle une même clé secrète est utilisée pour chiffrer et déchiffrer les données.
- **TSM (Trusted Service Manager)** = Gestionnaire de services de confiance assurant la coordination technique entre les différents acteurs d'un écosystème numérique et permettant l'enregistrement sécurisé des appareils mobiles. Le TSM d'ABLOY CUMULUS garantit l'intégration sécurisée des smartphones utilisateurs.
- **X.509** = Norme internationale définissant les certificats à clé publique utilisés dans de nombreux protocoles Internet sécurisés, tels que HTTPS et TLS. Par exemple, ABLOY CUMULUS utilise un certificat TLS 1.3 pour sécuriser ses communications.



ALCEA specializes in protecting critical infrastructure globally, including energy, water, telecom, transportation, mining, oil, and gas. We provide comprehensive security solutions tailored to your unique needs, from access control and intrusion detection to key and video management. Our experienced specialists deliver customized, digitalized solutions that enhance efficiency, ensure compliance, and offer peace of mind.

© 2026 ALCEA/ASSA ABLOY AB. All rights reserved. This publication is for informational purposes only, without representation or warranty of any kind and the details provided herein are subject to change without advance notice.

alceaglobal.com