LIVRE BLANC

Raisons du choix d'OSDP plutôt que de Wiegand pour le contrôle d'accès

Mai 2025

Avant-propos

Si Wiegand reste une interface courante dans les applications de contrôle d'accès, elle devient rapidement obsolète en raison de ses failles de sécurité. Les sociétés qui accordent la priorité à la sécurité devraient passer à OSDP pour une meilleure protection contre les attaques. OSDP assure une communication cryptée et supervisée, ce qui en fait le meilleur choix pour les environnements sécurisés. La mise à niveau de votre système de contrôle d'accès vers OSDP offre une meilleure sécurité aujourd'hui, mais protège également votre société contre l'évolution des menaces.

Table des matières

1 Introduction

Les protocoles de communication utilisés par les systèmes de contrôle d'accès constituent un aspect essentiel de ces derniers.

Ce livre blanc explore les deux principaux protocoles de communication utilisés entre le lecteur et le contrôleur de porte dans les systèmes de contrôle d'accès. Nous examinons leurs avantages et leurs inconvénients du point de vue de la sécurité et discutons de la manière dont vous pouvez commencer à migrer vers l'option la plus sûre.

2 Le contrôle d'accès dans les solutions de sécurité physique

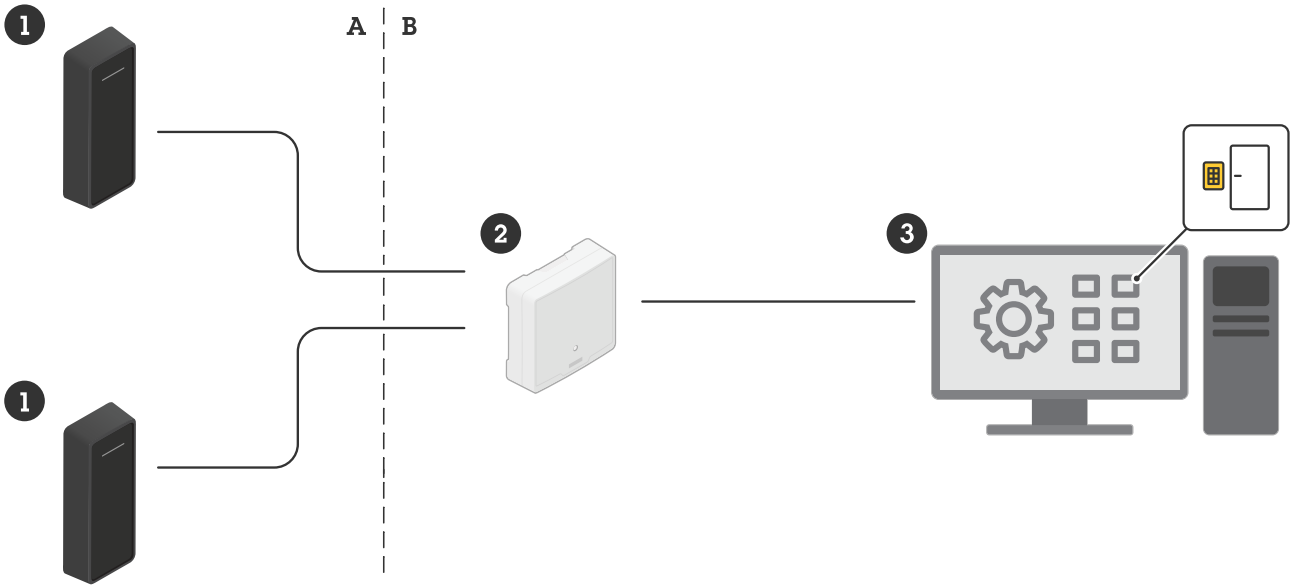
Les systèmes de contrôle d'accès sont essentiels pour protéger les bâtiments, les biens et les personnes. Ils garantissent que seules les personnes autorisées peuvent accéder aux zones sécurisées, réduisant ainsi les risques de sécurité et améliorant l'efficacité du fonctionnement. Ces systèmes sont largement utilisés dans divers secteurs, notamment dans les bureaux des entreprises, les centres de données, les établissements de santé et les administrations.

Un système de contrôle d'accès classique se compose de trois éléments essentiels.

1 Lecteurs de contrôle d'accès : périphériques qui lisent les données d'identification des utilisateurs et les transmettent à un contrôleur. Les informations d'identification des utilisateurs comprennent généralement des cartes d'accès, des informations d'identification mobiles, des codes PIN et des données biométriques.

2 Contrôleurs de porte : unités décisionnelles qui traitent les données d'identification et déterminent s'il convient d'accorder ou de refuser l'accès.

3 Logiciel de gestion : interface dans laquelle les administrateurs de la sécurité configurent les politiques d'accès, surveillent l'activité et gèrent les utilisateurs.



Dans le contrôle d'accès physique, les lecteurs (1) sont installés à l'extérieur de la porte (zone non sécurisée, A) et communiquent avec un contrôleur de porte (2) installé à l'intérieur (zone sécurisée, B).

3 Protocoles de communication lecteur-contrôleur

Au fil du temps, les protocoles de contrôle d'accès ont évolué, améliorant la sécurité, la fonctionnalité et la facilité d'intégration. Examinons de plus près les deux principaux protocoles.

3.1 L'ancienne norme : Wiegand

Wiegand transmet les données d'identification du lecteur au contrôleur en utilisant deux lignes de données. Le système Wiegand existe depuis des décennies et reste largement utilisé, principalement en raison de sa simplicité et de sa compatibilité avec les systèmes existants.

Le principal inconvénient de Wiegand est la faiblesse de sa sécurité. Le plus important est qu'il n'a pas de cryptage. Les données sont transmises en clair, ce qui les rend vulnérables à l'interception et aux attaques par clonage.

3.2 L'alternative sûre : OSDP

L'Open Supervised Device Protocol (OSDP) a été développé par la Security Industry Association (SIA) pour améliorer l'interopérabilité entre les produits de contrôle d'accès et de sécurité. OSDP a été approuvé en tant que norme internationale par la Commission électrotechnique internationale et introduit le cryptage AES-128, la communication bidirectionnelle et la surveillance des périphériques en temps réel. Comme OSDP permet au contrôleur de renvoyer des commandes au lecteur, il active également des fonctions telles que le contrôle des LED, l'activation de l'avertisseur sonore et la détection de vandalisme.

L'une des principales caractéristiques d'OSDP est le mode Secure Channel, qui permet la transmission sécurisée des données brutes entre les lecteurs de cartes à puce et les contrôleurs. Ceci est particulièrement utile pour les méthodes d'authentification avancées, telles que la validation biométrique et mobile.

3.2.1 OSDP Vérifié

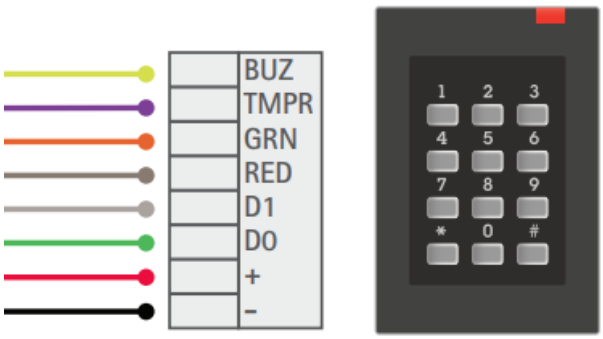
Le programme OSDP Verified de SIA est une démarche de test complète qui valide la conformité d'un périphérique à la norme OSDP et aux profils de performance associés. SIA tient à jour une liste des périphériques vérifiés qui ont été testés et jugés conformes aux critères de la norme et aux profils indiqués dans la liste. Les périphériques figurant sur la liste peuvent utiliser la marque OSDP Verified dans leur matériel marketing.

La marque OSDP Verified donne aux intégrateurs, aux prescripteurs et aux praticiens l'assurance que les périphériques conformes OSDP fonctionneront comme prévu pour divers types d'utilisation de contrôle d'accès.

4 Comparaison des lecteurs Wiegand et OSDP

Les lecteurs ont des avantages et des inconvénients différents selon le protocole de communication qu'ils utilisent.

4.1 Lecteurs Wiegand



Un lecteur Wiegand et son câblage, qui comprend des câbles supplémentaires pour l'avertisseur, la détection de vandalisme et les LED.

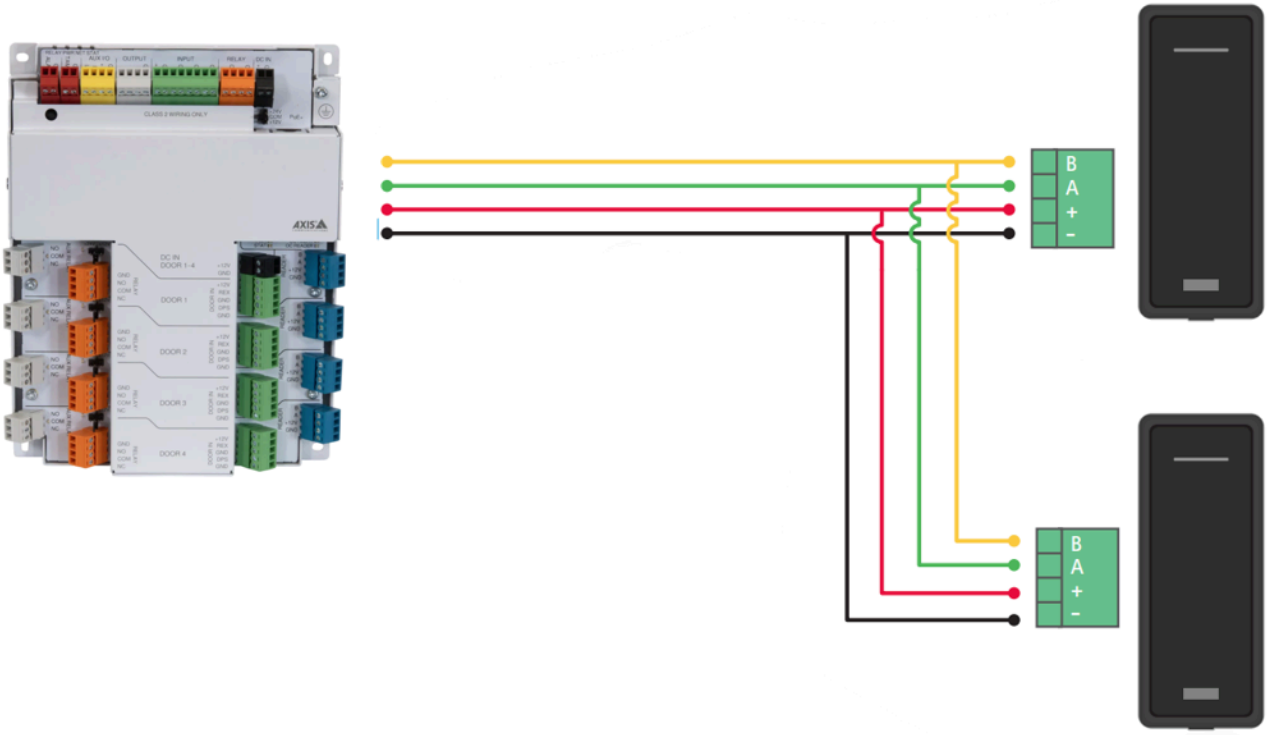
Avantages :

- Simple et largement compatible avec d'anciens systèmes.

Inconvénients :

- Pas de cryptage. Les données sont transmises en clair, ce qui facilite leur interception.
- Communication à sens unique. Le contrôleur ne peut pas renvoyer de commandes au lecteur. Cela signifie qu'il n'y a aucun moyen de détecter si un lecteur a été saboté ou remplacé puisqu'il n'est pas supervisé.
- Câblage complexe. Un lecteur utilisant les protocoles Wiegand nécessite des câbles supplémentaires pour l'avertisseur du lecteur, la détection de vandalisme et les LED.
- La distance maximale du câble est d'environ 150 m (500 pieds).

4.2 Lecteurs OSDP



Lecteurs OSDP (à droite) et leur câblage à un contrôleur de porte (à gauche). Les fonctions telles que le contrôle par LED, l'activation d'un avertisseur et la supervision du lecteur ne nécessitent pas de câbles supplémentaires.

OSDP utilise un câblage RS-485. C'est une norme de communication série permettant de transmettre des données sur de longues distances à l'aide de câbles à paires torsadées. Il est couramment utilisé dans les systèmes qui nécessitent une communication fiable et multipoint. Ses principales caractéristiques sont la transmission à longue distance et la capacité multipoint.

Avantages :

- La communication cryptée empêche l'interception des données d'identification.
- OSDP permet au contrôleur de renvoyer des commandes au lecteur. Cet échange de données bidirectionnel permet la supervision et la configuration à distance. Il simplifie également le câblage.
- Le câblage RS-485 permet d'utiliser des câbles de longueur maximale.
- La fonction Multidrop active plusieurs lecteurs qui partagent une même connexion.

4.3 Facilité d'utilisation

tableau 4.1 *Comparaison des aspects de sécurité avec lecteurs Wiegand et OSDP.*

	Wiegand	OSDP
Sécurité	Pas de cryptage, vulnérable au piratage	Cryptage AES-128, détection de vandalisme
Communication	Unidirectionnel (du lecteur au contrôleur)	Transmission bidirectionnelle
Longueur de câblage	jusqu'à 150 m environ, (500 pieds)	jusqu'à 1 200 m environ, (4 000 pieds)
Multidrop	Non, un périphérique - un bus	Oui, plusieurs périphériques pris en charge sur un seul bus
Détection de vandalisme	Non, nécessite un câblage supplémentaire	Oui
Supervision	Non, nécessite un câblage supplémentaire	Oui
Intégrité des données	Susceptible de faire l'objet d'une attaque par réutilisation des identifiants	Transmission cryptée et sécurisée
Complexité de l'installation	Câblage complexe (D0/D1 et LED, sabotage, avertisseur sonore)	Facile (RS-485, A et B)
Évolutivité	Limité par les contraintes de câblage	Possibilité de connecter plusieurs lecteurs en guirlande
Meilleur cas d'utilisation	Systèmes anciens, faibles besoins en matière de sécurité	Installations modernes sécurisées dans des secteurs tels que l'administration ou les entreprises

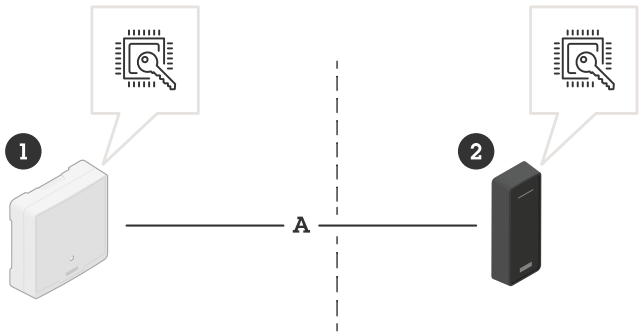
4.4 Sécurité

La sécurité doit être la priorité absolue lors du choix d'un protocole de contrôle d'accès. L'absence de cryptage de Wiegand le rend vulnérable à plusieurs types d'attaques.

- Interception des données d'identification. Les attaquants peuvent espionner les lignes de données et s'emparer des informations d'identification.
- Attaques en différé. Une fois capturé, le même identifiant peut être réutilisé pour obtenir un accès non autorisé.
- Sabotage. Le système ne peut pas détecter si un lecteur est supprimé ou remplacé.

En revanche, OSDP atténue ces risques en chiffrant les données avec AES-128 (Secure Channel) et en assurant la supervision du périphérique . Le contrôleur peut ainsi détecter si un lecteur a été saboté et empêcher ainsi tout accès non autorisé.

Le cryptage sécurise les données, mais la protection des clés sécurise le cryptage. Sans une protection solide des clés, l'ensemble du système peut être menacé. C'est pourquoi les clés du canal sécurisé doivent être conservées en toute sécurité, dans une puce matérielle spéciale aux deux extrémités : contrôleur et lecteur. Ces zones matérielles sécurisées sont conçues en tant qu'éléments sécurisés pour empêcher les pirates d'obtenir les clés même s'ils ont un accès physique au périphérique.



Assurer une sécurité de bout en bout avec un fichier de clés sécurisé en contrôle d'accès. La clé principale et la clé de base individuelle du canal sécurisé (SCBK) sont toutes deux stockées dans les fichiers de clés sécurisés, dans les périphériques de chaque côte de la porte.

1 *Contrôleur de porte installé du côté protégé de la porte*
2 *Lecteur installé du côté non sécurisé de la porte*
3 *A : Communication par canal sécurisé OSDP*

tableau 4.2 *Comparaison des aspects de sécurité avec les lecteurs Wiegand et OSDP.*

	Wiegand	OSDP
Cryptage	Aucune, données en clair	Cryptage AES-128
Interception de données	Interception facile des identifiants	Cryptée pour éviter l'interception
Attaques en différé	Les informations d'identification peuvent être réutilisées plus tard	Impossible en raison du cryptage
Détection de vandalisme	Non, impossible de détecter les lecteurs vandalisés.	Oui, le contrôleur surveille l'état du lecteur.
Supervision	Non, le contrôleur ne peut pas vérifier l'état du lecteur	Oui, supervision en temps réel
Conformité	Non recommandé pour les environnements sécurisés	Conforme aux normes de sécurité modernes

5 Recommandations

Dans le paysage actuel de la sécurité, Wiegand n'est plus une option viable pour les nouvelles installations. Les sociétés devraient passer aux lecteurs OSDP pour plus de sécurité, de fiabilité et d'évolutivité.

- Évaluez votre infrastructure actuelle de contrôle d'accès. Si vous utilisez actuellement Wiegand, commencez à planifier une stratégie de migration. Déterminez si une migration OSDP complète ou un convertisseur Wiegand-OSDP est la meilleure option.
- Pour les nouvelles installations, choisissez autant que possible des lecteurs OSDP afin de garantir une communication cryptée et inviolable.
- Travaillez avec des professionnels de la sécurité pour mettre en place un système de contrôle d'accès sécurisé et moderne qui protège contre les menaces.

6 Migration de Wiegand vers OSDP

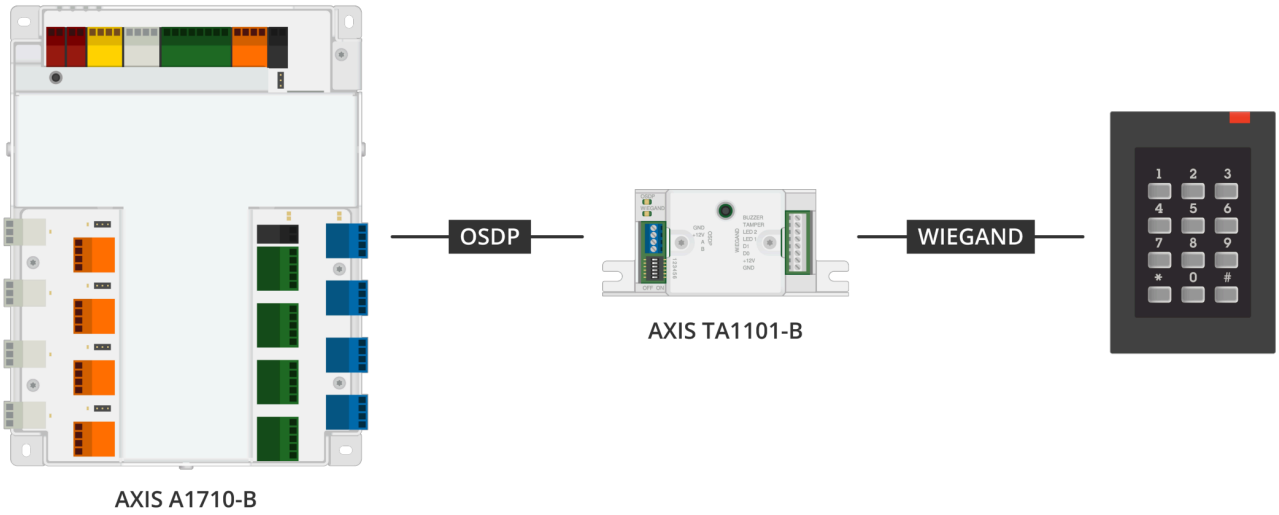
De nombreuses sociétés utilisent encore des lecteurs Wiegand mais souhaitent renforcer la sécurité sans remplacer l'ensemble de leur système. Il existe deux voies pratiques de migration. Les deux options améliorent la sécurité, mais la mise en place directe d'OSDP constitue le meilleur investissement à long terme pour les sociétés qui cherchent à pérenniser leurs systèmes de contrôle d'accès.

6.1 Option 1 : remplacer les lecteurs Wiegand par des lecteurs OSDP

C'est la meilleure solution à long terme. En remplaçant les lecteurs Wiegand obsolètes par des modèles conformes à OSDP, la société peut bénéficier du cryptage, de la communication bidirectionnelle et de la supervision des lecteurs. Toutefois, il faut pour cela s'assurer que le panneau de contrôle d'accès prend en charge OSDP.

6.2 Option 2 : utiliser un convertisseur Wiegand-OSDP

Pour les sociétés qui ne sont pas en mesure de remplacer immédiatement tous les lecteurs, un convertisseur Wiegand-OSDP constitue une solution de rechange rentable. Ce périphérique crypte les données Wiegand avant de les envoyer à un contrôleur compatible OSDP, améliorant ainsi la sécurité sans nécessiter une modification complète du matériel.



AXIS A1710-B

AXIS TA1101-B

Vous pouvez améliorer la sécurité en utilisant un convertisseur Wiegand-OSDP (au milieu).

À propos d'Axis Communications

En améliorant la sûreté, la sécurité, l'efficacité opérationnelle et l'intelligence économique, Axis contribue à un monde plus sûr et plus intelligent. Leader de son secteur dans les technologies sur IP, Axis propose des solutions en vidéosurveillance, contrôle d'accès, visiophonie et systèmes audio. Ces solutions sont enrichies par des applications d'analyse intelligente et soutenues par des formations de haute qualité.

L'entreprise emploie environ 5000 personnes dans plus de 50 pays et collabore avec des partenaires technologiques et intégrateurs de systèmes du monde entier pour fournir des solutions sur mesure à ses clients. Axis a été fondée en 1984, son siège est situé à Lund en Suède.aboutaxis_text2