DOCUMENTO TÉCNICO

Por qué elegir OSDP en lugar de Wiegand para el control de acceso

Mayo 2025

AXIS COMMUNICATIONS

Resumen

Si bien Wiegand continúa siendo una interfaz común en las aplicaciones de control de acceso, se está volviendo obsoleta rápidamente debido a sus fallos de seguridad. Las organizaciones que priorizan la seguridad deberían migrar a OSDP para mejorar la protección contra ataques. OSDP proporciona comunicación cifrada y supervisada, representando la mejor opción para entornos seguros. Actualizar su sistema de control de acceso a OSDP ofrece mayor seguridad hoy, pero también protege a su organización contra futuras amenazas.

Índice

1 Introducción

Un aspecto fundamental de los sistemas de control de acceso son los protocolos de comunicación que emplean.

Este informe técnico explora los dos principales protocolos de comunicación utilizados entre el lector y el controlador de puerta en los sistemas de control de acceso. Analizamos sus ventajas e inconvenientes desde una perspectiva de seguridad y explicamos cómo puede empezar a migrar a la opción más segura.

2 Control de acceso en soluciones de seguridad física

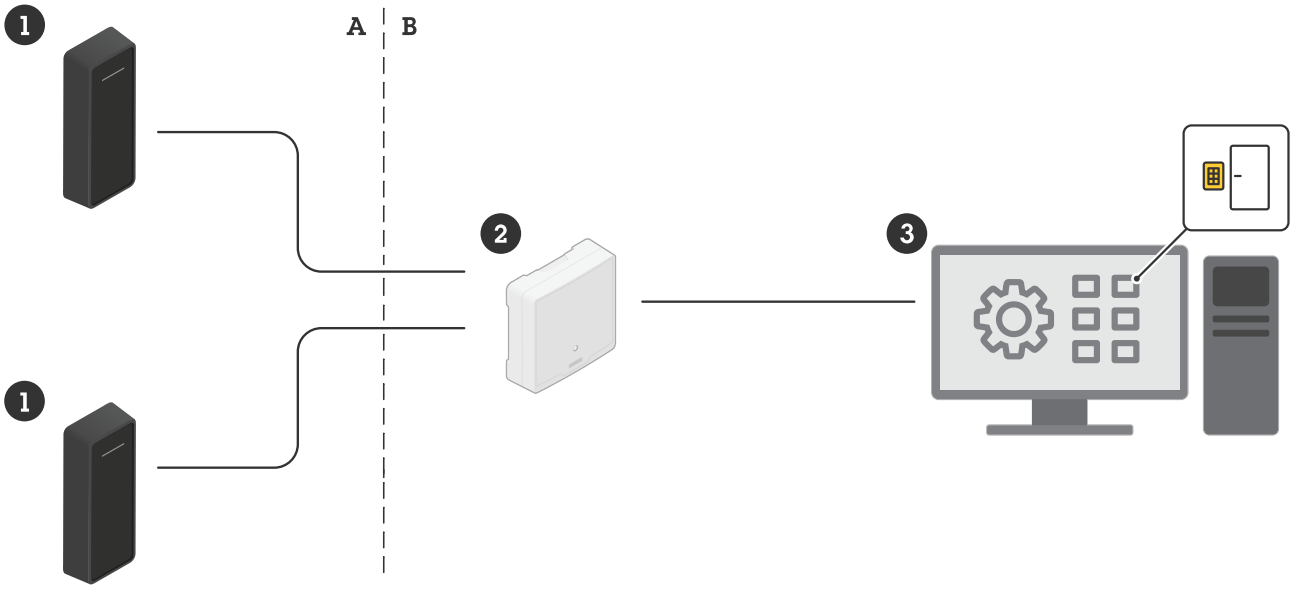
Los sistemas de control de acceso son esenciales para proteger edificios, activos y personas. Garantizan que solo las personas autorizadas puedan acceder a áreas seguras, lo que reduce los riesgos de seguridad y mejora la eficiencia operativa. Estos sistemas se utilizan ampliamente en varios sectores, como oficinas corporativas, centros de datos, centros de salud e instituciones gubernamentales.

Un sistema de control de acceso típico consta de tres componentes clave.

1 Lectores de control de acceso: dispositivos que leen las credenciales del usuario y transmiten sus datos a un controlador. Las credenciales de usuario típicas incluyen tarjetas de acceso, credenciales móviles, PIN y biometría.

2 Controladores de puerta: las unidades de toma de decisiones que procesan los datos de las credenciales y determinan si se concede o deniega el acceso.

3 Software de gestión: la interfaz donde los administradores de seguridad configuran las políticas de acceso, supervisan la actividad y gestionan usuarios.



En el control de acceso físico, los lectores (1) se instalan en el exterior de la puerta (área no segura, A) y se comunican con un controlador de puerta (2) instalado en el interior (área segura, B).

3 Protocolos de comunicación lector-controlador

Con el tiempo, los protocolos de control de acceso han evolucionado, mejorando la seguridad, la funcionalidad y la facilidad de integración. Analicemos con más detalle los dos protocolos principales.

3.1 El estándar heredado: Wiegand

Wiegand transmite los datos de las credenciales del lector al controlador por medio de dos líneas de datos. Wiegand existe desde hace décadas y continúa siendo ampliamente utilizado, principalmente debido a su sencillez y compatibilidad con sistemas heredados.

La principal desventaja de Wiegand es su baja seguridad. Especialmente, carece de cifrado. Los datos se transmiten en texto sin formato, haciéndolos vulnerables a ataques de interceptación y clonación.

3.2 La alternativa segura: OSDP

El Protocolo abierto de dispositivos supervisados (OSDP) fue desarrollado por la Asociación de la Industria de Seguridad (SIA) para mejorar la interoperabilidad entre los productos de control de acceso y seguridad. OSDP ha sido aprobado como estándar internacional por la Comisión Electrotécnica Internacional e introduce el cifrado AES-128, la comunicación bidireccional y la monitorización de dispositivos en tiempo real. Dado que OSDP permite al controlador enviar órdenes al lector, también habilita funciones como el control de LED, la activación del avisador acústico y la detección de manipulaciones.

Una característica clave del OSDP es el modo Canal seguro, que permite la transmisión segura de datos de credenciales sin procesar entre lectores de tarjetas inteligentes y controladores. Esto resulta particularmente útil para métodos de autentificación avanzados, como la validación biométrica y de credenciales móviles.

3.2.1 OSDP Verified

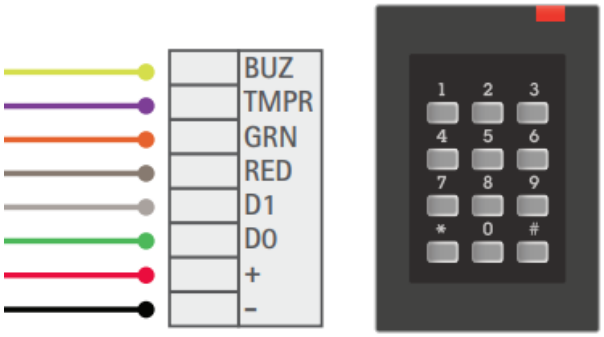
El programa SIA OSDP Verified es una iniciativa integral de pruebas que valida la conformidad de un dispositivo con el estándar OSDP y los perfiles de rendimiento relacionados. SIA mantiene una lista de dispositivos verificados que han sido probados y cumplen con los criterios del estándar y los perfiles indicados en la lista. Los dispositivos de la lista pueden usar la marca OSDP Verified en materiales de marketing.

La marca OSDP Verified inspira confianza a los integradores, especificadores y profesionales de que los dispositivos OSDP funcionarán según lo previsto en distintos tipos de casos de uso de control de acceso.

4 Comparativa de lectores Wiegand y OSDP

Los lectores presentan distintas fortalezas y debilidades según el protocolo de comunicación que utilizan.

4.1 Lectores Wiegand



Un lector Wiegand y su cableado, incluyendo cables adicionales para el avisador acústico, la detección de manipulaciones y los LED.

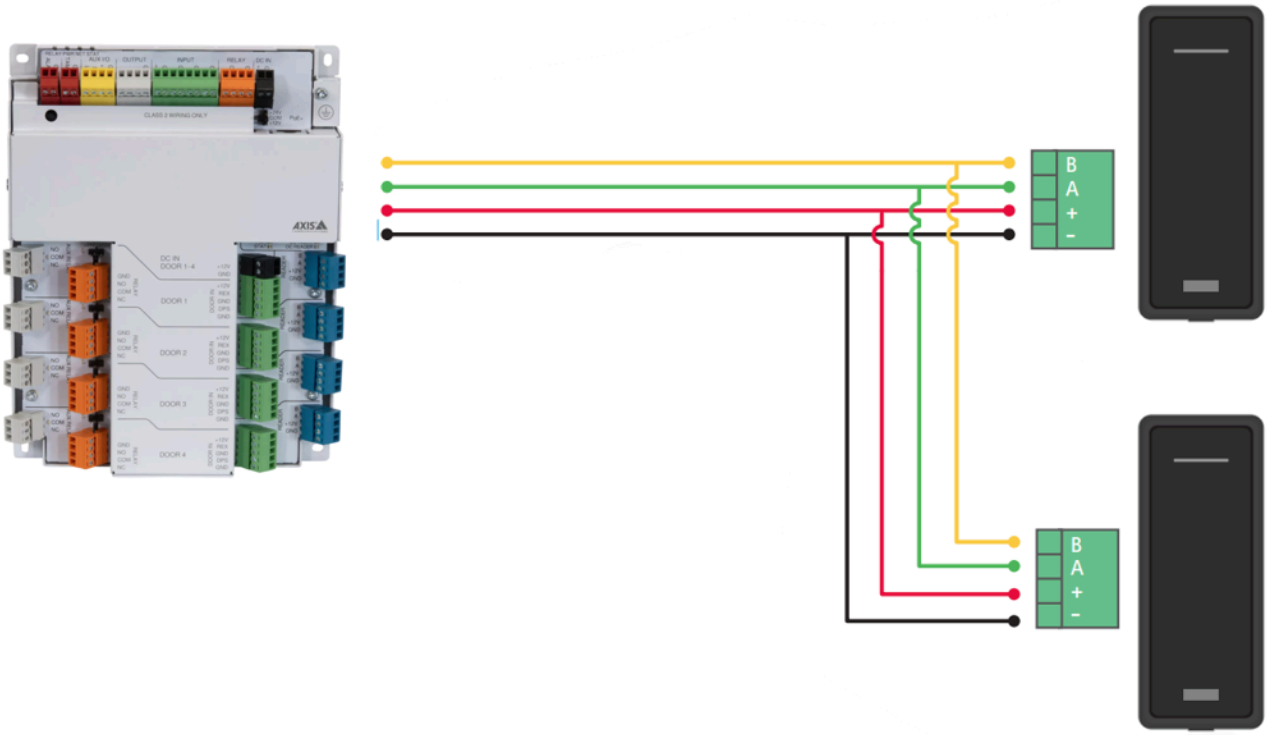
Ventajas:

- Sencillo y ampliamente compatible con sistemas antiguos.

Desventajas:

- Sin cifrado. Los datos se transmiten en texto sin formato, facilitando su interceptación.
- Comunicación unidireccional. El controlador no puede enviar órdenes al lector. Esto significa que no hay forma de detectar si un lector ha sido manipulado o reemplazado; el lector no está supervisado.
- Cableado complejo. Un lector que utiliza los protocolos Wiegand necesita cables adicionales para el avisador acústico, la detección de manipulaciones y los LED.
- La distancia máxima del cable es de ~150 metros (500 pies).

4.2 Lectores OSDP



Lectores OSDP (derecha) y su cableado a un controlador de puerta (izquierda). Funciones como el control de LED, la activación del avisador acústico y la supervisión de lectores no requieren cables adicionales.

El OSDP utiliza cableado RS-485. Este es un estándar de comunicación en serie para la transmisión de datos a largas distancias mediante cables de par trenzado. Se utiliza comúnmente en sistemas que requieren una comunicación multipunto fiable. Sus características clave incluyen transmisión a larga distancia y capacidad multipunto.

Ventajas:

- La comunicación cifrada evita la interceptación de credenciales.
- El OSDP permite que el controlador envíe órdenes al lector. Este intercambio de datos bidireccional permite la supervisión y configuración remota. También simplifica el cableado.
- El cableado RS-485 habilita una mayor distancia máxima entre cables.
- La conexión multipunto permite que varios lectores compartan una misma conexión.

4.3 Usabilidad

Tabla 4.1 *Comparativa de aspectos de usabilidad con lectores Wiegand y OSDP.*

	Wiegand	OSDP
Seguridad	Sin cifrado, vulnerable a ataques informáticos	Cifrado AES-128, detección de manipulaciones
Comunicación	Unidireccional (de lector a controlador)	Bidireccional
Distancia de cableado	hasta ~150 metros (500 pies)	hasta ~1 200 metros (4 000 pies)
Multipunto	No, un dispositivo, un bus	Sí, admite múltiples dispositivos en un bus
Detección de manipulaciones	No, requiere cableado adicional	Sí

	Wiegand	OSDP
Supervisión	No, requiere cableado adicional	Sí
Integridad de los datos	Susceptible a ataques de reproducción de credenciales	Transmisión cifrada y segura
Complejidad de la instalación	Cableado complejo (D0/D1 y LED, manipulación, avisador acústico)	Fácil (RS-485, A y B)
Escalabilidad	Limitado por las restricciones de cableado	Permite conectar varios lectores en cadena.
Caso de uso óptimo.	Sistemas heredados, bajas necesidades de seguridad.	Instalaciones modernas y seguras en sectores como el público o las empresas

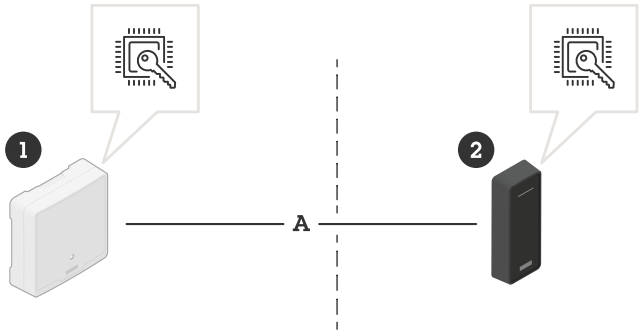
4.4 Seguridad

Al elegir un protocolo de control de acceso, la seguridad debe ser su máxima prioridad. La falta de cifrado de Wiegand lo hace susceptible a diversos tipos de ataques.

- Interceptación de credenciales. Los atacantes pueden interceptar las líneas de datos y capturar credenciales.
- Ataques de repetición. Una vez capturada, la misma credencial puede reproducirse para obtener acceso no autorizado.
- Manipulación. El sistema no puede detectar si se retira o reemplaza un lector.

Por el contrario, OSDP mitiga estos riesgos cifrando los datos con AES-128 (Canal seguro) y ofreciendo la supervisión del dispositivo. Esto garantiza que el controlador pueda detectar si un lector ha sido manipulado y, por lo tanto, evitar el acceso no autorizado.

El cifrado mantiene los datos seguros, pero la protección de las claves mantiene la seguridad del cifrado. Sin una protección sólida de las claves, todo el sistema puede estar en riesgo. Por ese motivo, las claves de canal seguro deben mantenerse seguras en un chip de hardware especial en ambos extremos: el controlador y el lector. Estas áreas de hardware seguras, como los elementos seguros, están diseñadas para impedir que los atacantes obtengan las claves incluso si acceden físicamente al dispositivo.



Uso de un almacén de claves seguro en control de acceso para una seguridad integral. Tanto la clave maestra como la Secure Channel Base Key (SCBK) se guardan en sendos almacenes de claves seguro, en dispositivos colocados a ambos lados de la puerta.

1 *Controlador de puerta instalado en el lado seguro de la puerta.*
2 *Lector instalado en el lado no seguro de la puerta.*
3 *A: Comunicación de canal seguro de OSDP*

Tabla 4.2 *Comparativa de aspectos de seguridad con lectores Wiegand y OSDP.*

	Wiegand	OSDP
Cifrado	Ninguno, datos en texto sin formato	Cifrado AES-128
Interceptación de datos	Credenciales fáciles de interceptar	Cifrado para evitar la interceptación
Ataques de repetición	Las credenciales se pueden copiar/ reproducir	Evitado mediante cifrado
Detección de manipulaciones	No, no se pueden detectar lectores manipulados	Sí, el controlador supervisa el estado del lector
Supervisión	No, el controlador no puede verificar el estado del lector	Sí, supervisión en tiempo real
Cumplimiento normativo	No recomendado para entornos seguros	Satisface los estándares de seguridad modernos

5 Recomendaciones

En el panorama de seguridad actual, Wiegand ha dejado de ser una opción viable para nuevas instalaciones. Las organizaciones deberían migrar a lectores OSDP para mejorar su seguridad, fiabilidad y escalabilidad futura.

- Evalúe su infraestructura actual de control de acceso. Si utiliza Wiegand actualmente, comience a planificar una estrategia de migración. Determine si una migración completa a OSDP o un conversor de Wiegand a OSDP es la mejor opción.
- Para nuevas instalaciones, elija siempre que sea posible lectores OSDP para garantizar una comunicación cifrada y a prueba de manipulaciones.
- Trabaje con profesionales de la seguridad para implementar un sistema de control de acceso seguro y moderno que le proteja de las amenazas.

6 Migración de Wiegand a OSDP

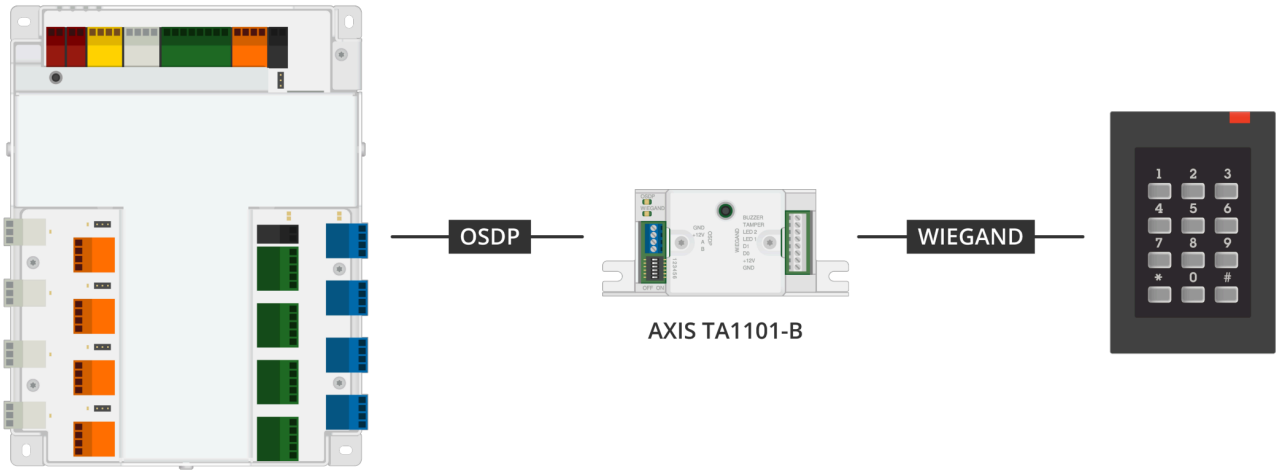
Infinidad de organizaciones dependen aún de los lectores Wiegand, pero desean mejorar la seguridad sin reemplazar todo su sistema. Existen dos vías prácticas de migración. Ambas opciones mejoran la seguridad, pero la implementación directa de OSDP es la mejor inversión a largo plazo para aquellas organizaciones que buscan asegurar el futuro de sus sistemas de control de acceso.

6.1 Opción 1: Sustituir los lectores Wiegand por lectores OSDP

Esta es la mejor solución a largo plazo. Al sustituir los lectores Wiegand obsoletos por modelos compatibles con OSDP, las organizaciones pueden beneficiarse del cifrado, la comunicación bidireccional y la supervisión de lectores. Sin embargo, esto requiere garantizar que el panel de control de acceso sea compatible con OSDP.

6.2 Opción 2: Utilizar un conversor Wiegand a OSDP

Para las organizaciones que no pueden reemplazar todos los lectores inmediatamente, un conversor Wiegand a OSDP es una alternativa rentable. Este dispositivo cifra los datos Wiegand antes de enviarlos a un controlador compatible con OSDP, mejorando la seguridad sin necesidad de realizar una actualización completa del hardware.



AXIS A1710-B

AXIS TA1101-B

Puede mejorar la seguridad utilizando un conversor Wiegand a OSDP (centro).

Acerca de Axis Communications

Axis contribuye a crear un mundo más inteligente y seguro mejorando la seguridad, la operatividad de las empresas y la inteligencia empresarial. Como líder del sector y empresa especializada en tecnología de redes, Axis ofrece videovigilancia, control de acceso, intercomunicadores y soluciones de audio. Su valor se multiplica gracias a las aplicaciones inteligentes de analítica y una formación de primer nivel.

Axis cuenta aproximadamente con 5.000 empleados especializados en más de 50 países y proporciona soluciones a sus clientes en colaboración con sus socios de tecnología e integración de sistemas. Axis fue fundada en 1984 y su sede central se encuentra en Lund (Suecia).aboutaxis_text2