WHITE PAPER

Por que escolher OSDP em vez de Wiegand no controle de acesso

Maio 2025

Resumo

Embora o Wiegand continue sendo uma interface comum em aplicativos de controle de acesso, ele está se tornando obsoleto rapidamente devido às suas falhas de segurança. As organizações que priorizam a segurança devem fazer a transição para o OSDP para obter melhor proteção contra ataques. O OSDP fornece comunicação criptografada e supervisionada, o que o torna a melhor opção para ambientes seguros. A atualização do seu sistema de controle de acesso para o OSDP oferece maior segurança hoje, mas também prepara a sua organização para o futuro contra ameaças em evolução.

Índice

1 Introdução

Um aspecto crítico dos sistemas de controle de acesso são os protocolos de comunicação que eles usam.

Este artigo técnico explora os dois principais protocolos de comunicação usados entre o leitor e o controlador de porta em sistemas de controle de acesso. Analisamos suas vantagens e desvantagens do ponto de vista da segurança e discutimos como você pode começar a migrar para a opção mais segura.

2 Controle de acesso em soluções de segurança física

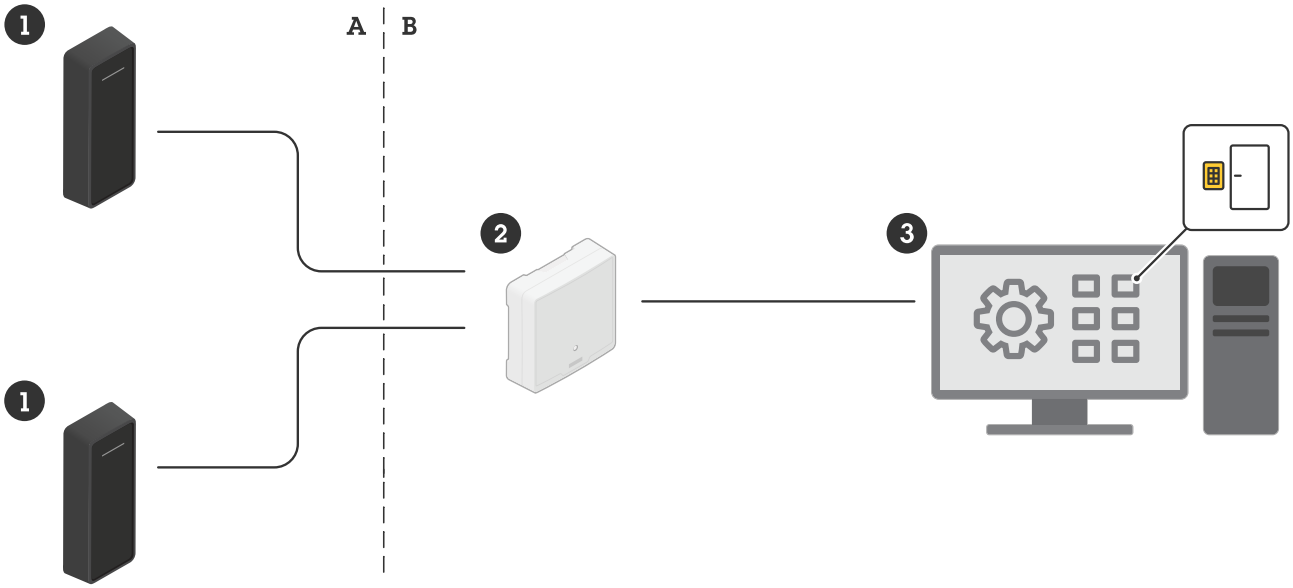
Os sistemas de controle de acesso são essenciais para proteger edifícios, bens e pessoas. Eles garantem que somente pessoas autorizadas possam entrar em áreas seguras, reduzindo os riscos de segurança e aumentando a eficiência operacional. Esses sistemas são amplamente usados em vários setores, incluindo escritórios corporativos, centros de dados, instalações de saúde e instituições governamentais.

Um sistema típico de controle de acesso consiste em três componentes principais.

1 Leitores de controle de acesso: dispositivos que leem as credenciais do usuário e transmitem os dados da credencial para um controlador. As credenciais de usuário típicas incluem cartões-chave, credenciais móveis, números de identificação pessoal e biometria.

2 Controladores de porta: as unidades de decisão que processam os dados das credenciais e determinam se o acesso deve ser concedido ou negado.

3 Software de gerenciamento: a interface em que os administradores de segurança configuram as políticas de acesso, monitoram as atividades e gerenciam os usuários.



No controle de acesso físico, os leitores (1) são instalados do lado de fora da porta (área não segura, A) e comunicam-se com um controlador de porta (2) instalado do lado de dentro (área segura, B).

3 Protocolos de comunicação entre leitor e controlador

Com o passar do tempo, os protocolos de controle de acesso evoluíram, melhorando a segurança, a funcionalidade e a facilidade de integração. Vamos dar uma olhada mais de perto nos dois principais protocolos.

3.1 O padrão legado: Wiegand

O Wiegand transmite dados de credenciais do leitor para o controlador usando duas linhas de dados. O Wiegand existe há décadas e continua sendo amplamente usado, principalmente devido à sua simplicidade e à compatibilidade com sistemas legados.

A principal desvantagem do Wiegand é a falta de segurança. Mais notavelmente, ele não tem criptografia. Os dados são transmitidos em texto simples, o que os torna vulneráveis a ataques de interceptação e clonagem.

3.2 A alternativa segura: OSDP

O Open Supervised Device Protocol (OSDP) foi desenvolvido pela SIA (Security Industry Association) para melhorar a interoperabilidade entre os produtos de controle de acesso e segurança. O OSDP foi aprovado como um padrão internacional pela Comissão Eletrotécnica Internacional e introduz a criptografia AES-128, a comunicação bidirecional e o monitoramento de dispositivos em tempo real. Como o OSDP permite que o controlador envie comandos de volta ao leitor, ele também ativa recursos como controle de LED, ativação de campainha e detecção de manipulação.

Um recurso importante do OSDP é o modo de canal seguro, que permite a transmissão segura de dados brutos de credenciais entre leitores e controladores de cartões inteligentes. Isso é particularmente útil para métodos avançados de autenticação, como validação biométrica e de credenciais móveis.

3.2.1 OSDP Verified

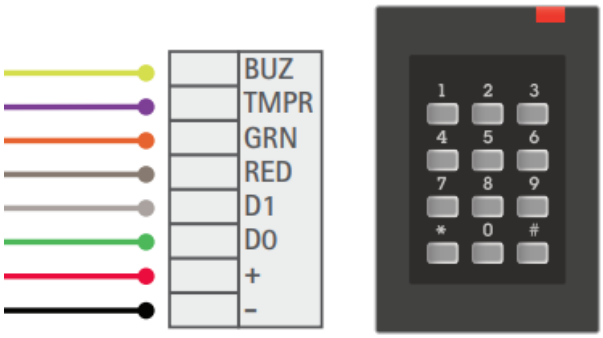
O programa SIA OSDP Verified é uma iniciativa abrangente de testes que valida que um dispositivo está em conformidade com o padrão OSDP e os perfis de desempenho relacionados. A SIA mantém uma lista de dispositivos verificados que foram testados e que atendem aos critérios do padrão e aos perfis indicados na lista. Os dispositivos da lista podem usar a marca OSDP Verified em materiais de marketing.

A marca OSDP Verified inspira confiança em integradores, especificadores e profissionais de que os dispositivos OSDP funcionarão como previsto para vários tipos de casos de uso de controle de acesso.

4 Comparação entre os leitores Wiegand e OSDP

Os leitores têm diferentes pontos fortes e fracos com base no protocolo de comunicação que usam.

4.1 Leitores Wiegand



Um leitor Wiegand e sua fiação, incluindo cabos extras para campainha, detecção de manipulação e LEDs.

Vantagens:

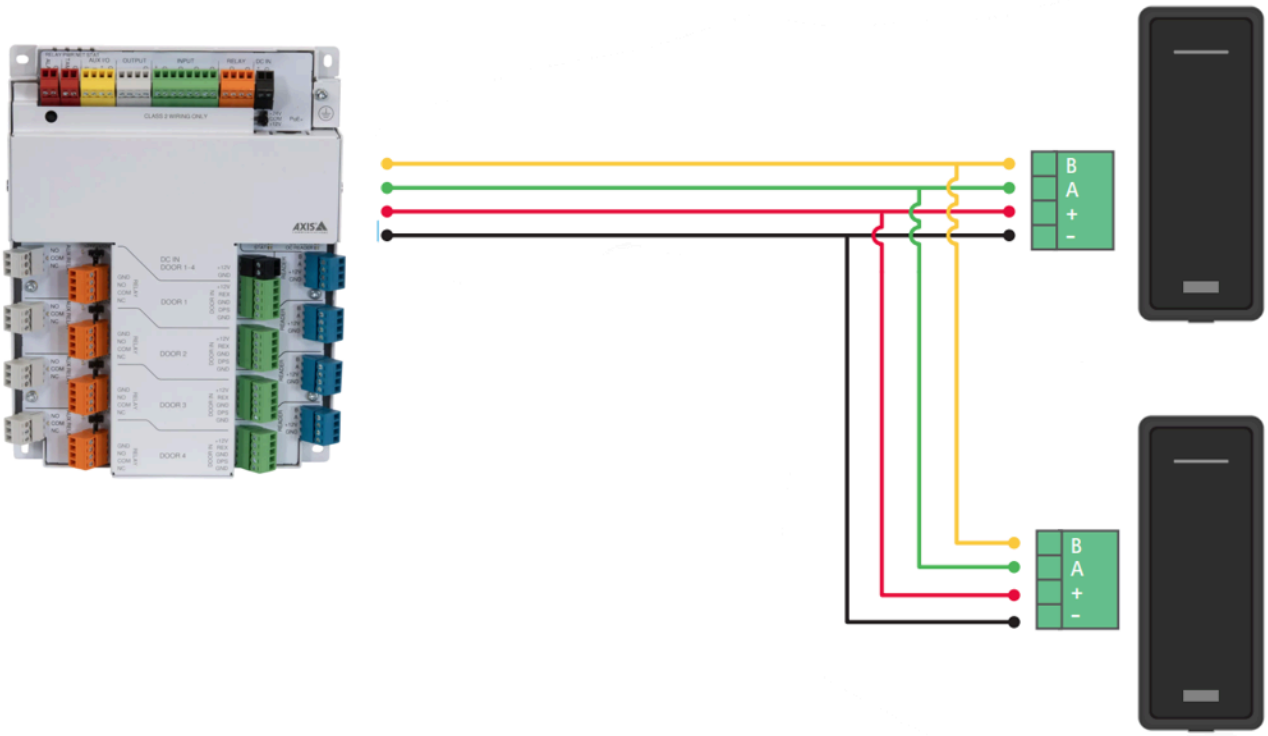
- Simples e amplamente compatível com sistemas mais antigos.

Desvantagens:

- Não tem criptografia. Os dados são transmitidos em texto simples, o que facilita a interceptação.

- Comunicação unidirecional. O controlador não pode enviar comandos de volta para o leitor. Isso significa que não há nenhuma maneira de detectar se um leitor foi manipulado ou substituído, pois ele não é supervisionado.
- Fiação complexa. Um leitor que usa os protocolos Wiegand precisa de cabos extras para a campainha do leitor, a detecção de manipulação e os LEDs.
- A distância máxima do cabo é de 500 pés (~150 metros).

4.2 Leitores do OSDP



Leitores de OSDP (direita) e sua fiação para um controlador de porta (esquerda). Recursos como controle de LED, ativação de campainha e supervisão do leitor não precisam de cabos extras.

O OSDP usa fiação RS-485. Esse é um padrão de comunicação serial para transmissão de dados em longas distâncias usando cabos de par trançado. É comumente usado em sistemas que exigem comunicação confiável e multiponto. Os principais recursos incluem a transmissão de longa distância e o recurso multiponto.

Vantagens:

- A comunicação criptografada impede a interceptação de credenciais.
- O OSDP permite que o controlador envie comandos de volta ao leitor. Essa troca de dados bidirecional permite a supervisão e a configuração remota. Isso também simplifica a fiação.
- A fiação RS-485 ativa uma distância máxima maior do cabo.
- O multiponto possibilita que vários leitores compartilhem uma única conexão.

4.3 Capacidade de uso

Tabela 4.1 *Comparação da capacidade de uso com leitores Wiegand e OSDP.*

	Wiegand	OSDP
Segurança	Sem criptografia, vulnerável a invasões	Criptografia AES-128, detecção de manipulação
Comunicação	Unidirecional (leitor para controlador)	Bidirecional
Distância do cabo	até 500 pés (~150 metros)	até 4.000 pés (~1.200 metros)
Multiponto	Não, um dispositivo, um barramento	Sim, suporte a vários dispositivos em um único barramento
Detecção de violações	Não, precisa de fiação adicional	Sim
Supervisão	Não, precisa de fiação adicional	Sim
Integridade dos dados	Susceptível a ataques de repetição de credenciais	Transmissão criptografada e segura
Complexidade da instalação	Fiação complexa (D0/D1 e LEDs, manipulação, campainha)	Fácil (RS-485, A e B)
Escalabilidade	Limitado por restrições de fiação	Pode conectar vários leitores em uma cadeia em série
Melhor caso de uso	Sistemas legados, baixa necessidade de segurança	Instalações modernas e seguras em setores como governo ou empresas

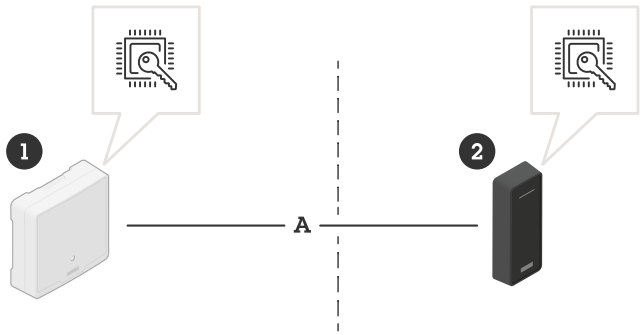
4.4 Segurança

A segurança deve ser a principal prioridade na escolha de um protocolo de controle de acesso. A falta de criptografia do Wiegand o torna suscetível a vários tipos de ataques.

- Interceptação de credenciais. Os invasores podem espionar as linhas de dados e capturar credenciais.
- Ataques de repetição. Uma vez capturada, a mesma credencial pode ser reproduzida para ganhar acesso não autorizado.
- Violação. O sistema não consegue detectar se um leitor foi removido ou substituído.

Em contraste, o OSDP atenua esses riscos criptografando dados com AES-128 (Secure Channel) e fornecendo supervisão do dispositivo. Isso garante que o controlador possa detectar se um leitor foi manipulado e, assim, impedir o acesso não autorizado.

A criptografia mantém os dados seguros, mas a proteção das chaves mantém a criptografia segura. Sem uma proteção forte das chaves, todo o sistema pode estar em risco. É por isso que as chaves do Secure Channel devem ser mantidas em segurança, em um chip de hardware especial em ambas as extremidades: controlador e leitor. Essas áreas de hardware seguras, como elementos seguros, são criadas para impedir que os invasores obtenham as chaves, mesmo que tenham acesso físico ao dispositivo.



Obtenção da segurança de ponta a ponta com armazenamento seguro de chaves no controle de acesso. A chave mestra e a chave base do canal seguro individual (SCBK) são armazenadas em chaves seguras, em dispositivos em cada lado da porta.

1 *Controlador de porta instalado no lado seguro da porta*
2 *Leitor instalado no lado não seguro da porta*
3 *A: Comunicação do OSDP Secure Channel*

Tabela 4.2 *Comparação dos aspectos de segurança com leitores Wiegand e OSDP.*

	Wiegand	OSDP
Criptografia	Nenhum, dados em texto simples	Criptografia AES-128
Interceptação de dados	Credenciais fáceis de interceptar	Criptografado para evitar interceptação
Ataques de repetição	As credenciais podem ser copiadas/ reproduzidas	Impedido por criptografia
Detecção de violações	Não, não consegue detectar leitores com manipulação	Sim, o controlador monitora o status do leitor
Supervisão	Não, o controlador não consegue verificar o status do leitor	Sim, supervisão em tempo real
Conformidade	Não recomendado para ambientes seguros	Atende aos padrões modernos de segurança

5 Recomendações

No cenário de segurança atual, o Wiegand não é mais uma opção viável para novas instalações. As organizações devem fazer a transição para leitores OSDP para obter melhor segurança, confiabilidade e escalabilidade futura.

- Avalie sua infraestrutura atual de controle de acesso. Se estiver usando Wiegand no momento, comece a planejar uma estratégia de migração. Determine se a melhor opção é uma migração OSDP completa ou um conversor de Wiegand para OSDP.
- Para novas instalações, escolha leitores OSDP sempre que possível para garantir uma comunicação criptografada e resistente à manipulação.
- Trabalhe com profissionais de segurança para implementar um sistema de controle de acesso seguro e moderno que proteja contra ameaças.

6 Migração de Wiegand para OSDP

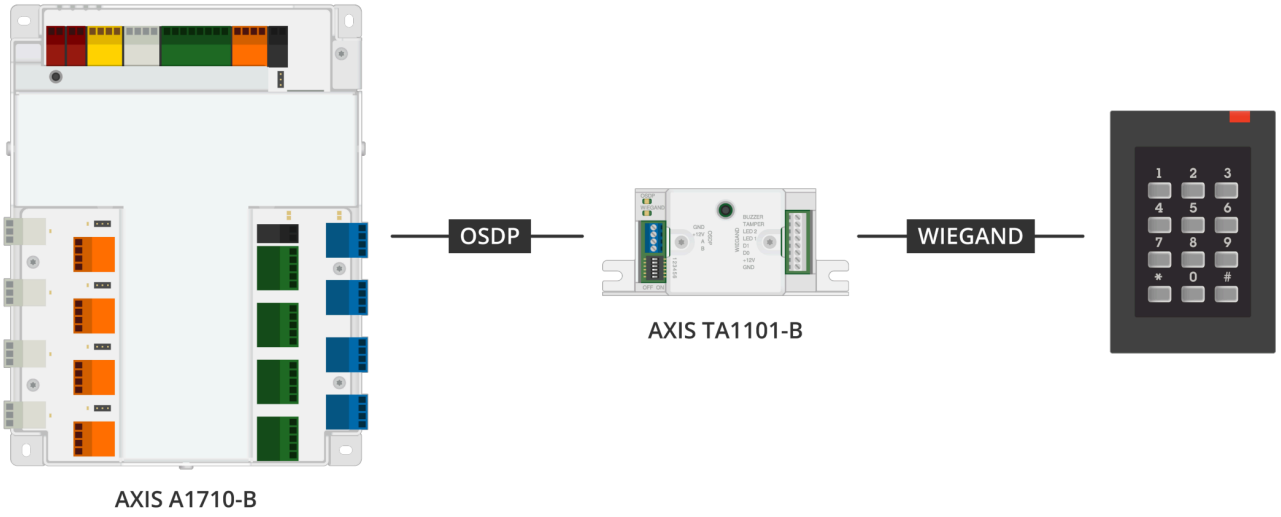
Muitas organizações ainda dependem de leitores Wiegand, mas querem aumentar a segurança sem substituir todo o sistema. Há dois caminhos práticos de migração. Ambas as opções melhoram a segurança, mas a implementação direta do OSDP é o melhor investimento de longo prazo para as organizações que desejam preparar seus sistemas de controle de acesso para o futuro.

6.1 Opção 1: Substituir os leitores Wiegand por leitores OSDP

Essa é a melhor solução de longo prazo. Ao substituir os leitores Wiegand desatualizados por modelos compatíveis com OSDP, as organizações podem se beneficiar da criptografia, da comunicação bidirecional e da supervisão do leitor. No entanto, para isso, é necessário garantir que o painel de controle de acesso seja compatível com OSDP.

6.2 Opção 2: Use um conversor de Wiegand para OSDP

Para organizações que não podem substituir todos os leitores imediatamente, um conversor de Wiegand para OSDP é uma alternativa econômica. Esse dispositivo criptografa os dados Wiegand antes de enviá-los a um controlador compatível com OSDP, melhorando a segurança sem exigir uma revisão completa do hardware.



AXIS A1710-B

AXIS TA1101-B

Você pode aumentar a segurança usando um conversor de Wiegand para OSDP (meio).

Sobre a Axis Communications

A Axis promove um mundo mais inteligente e seguro, melhorando a segurança, a proteção, a eficiência operacional e a inteligência empresarial. Como empresa de tecnologia de rede e líder de mercado, a Axis disponibiliza soluções de videovigilância, controlo de acessos, sistemas de intercomunicação e de áudio. Estas são potenciadas por aplicações de análise inteligentes e apoiadas por uma formação de alta qualidade.aboutaxis_text

A Axis conta com cerca de 5000 empregados dedicados em mais de 50 países e colabora com parceiros tecnológicos e de integração de sistemas em todo o mundo para fornecer soluções aos clientes. A Axis foi fundada em 1984 e está sediada em Lund na Suécia.