WHITE PAPER

Why choose OSDP over Wiegand in access control

May 2025

AXIS COMMUNICATIONS

Summary

While Wiegand remains a common interface in access control applications, it is rapidly becoming obsolete due to its security flaws. Organizations that prioritize security should transition to OSDP for better protection against attacks. OSDP provides encrypted, supervised communication, making it the best choice for secure environments. Upgrading your access control system to OSDP provides better security today but also future-proofs your organization against evolving threats.

Table of Contents

1 Introduction

A critical aspect of access control systems is the communication protocols they use.

This white paper explores the two main communication protocols used between reader and door controller in access control systems. We take a look at their advantages and drawbacks from a security perspective and discuss how you can start migrating to the more secure option.

2 Access control in physical security solutions

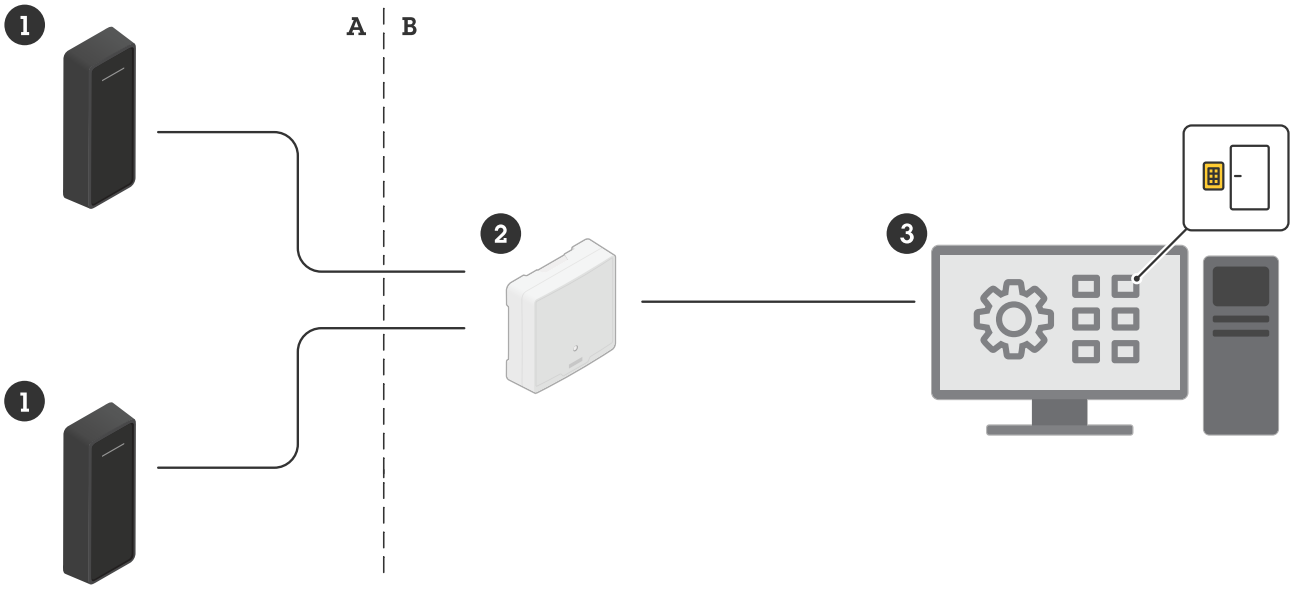
Access control systems are essential for protecting buildings, assets, and people. They ensure that only authorized individuals can enter secure areas, reducing security risks and enhancing operational efficiency. These systems are widely used across various sectors, including corporate offices, data centers, healthcare facilities, and government institutions.

A typical access control system consists of three key components.

1 Access control readers: devices that read user credentials and transmit credential data to a controller. Typical user credentials include keycards, mobile credentials, PINs, and biometrics.

2 Door controllers: the decision-making units that process credential data and determine whether to grant or deny access.

3 Management software: the interface where security administrators configure access policies, monitor activity, and manage users.



In physical access control, readers (1) are installed outside the door (non-secure area, A) and communicate with a door controller (2) installed on the inside (secure area, B).

3 Reader-to-controller communication protocols

Over time, access control protocols have evolved, improving security, functionality, and ease of integration. Let's take a closer look at the two main protocols.

3.1 The legacy standard: Wiegand

Wiegand transmits credential data from the reader to the controller using two data lines. Wiegand has been around for decades and remains widely used, mainly due to its simplicity and legacy system compatibility.

Wiegand's primary drawback is poor security. Most notably, it lacks encryption. The data is transmitted in plain text, making it vulnerable to interception and cloning attacks.

3.2 The secure alternative: OSDP

The Open Supervised Device Protocol (OSDP) was developed by the Security Industry Association (SIA) to improve interoperability among access control and security products. OSDP has been approved as an international standard by the International Electrotechnical Commission and introduces AES-128 encryption, bidirectional communication, and real-time device monitoring. Because OSDP allows the controller to send commands back to the reader, it also enables features like LED control, buzzer activation, and tamper detection.

A key feature of OSDP is the Secure Channel mode, which allows secure transmission of raw credential data between smart card readers and controllers. This is particularly useful for advanced authentication methods, such as biometric and mobile credential validation.

3.2.1 OSDP Verified

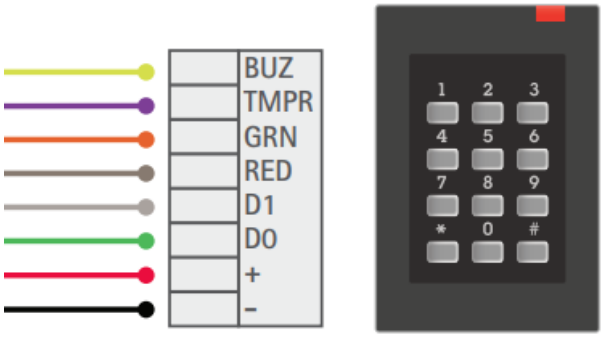
The SIA OSDP Verified program is a comprehensive testing initiative that validates that a device conforms to the OSDP standard and the related performance profiles. SIA keeps a list of verified devices that have been tested and found to meet the criteria for the standard and the profiles indicated within the listing. Devices in the list can use the OSDP Verified mark in marketing materials.

The OSDP Verified mark instills confidence in integrators, specifiers, and practitioners that OSDP devices will work as intended for various types of access control use cases.

4 Comparing Wiegand and OSDP readers

Readers come with different strengths and weaknesses based on the communication protocol they use.

4.1 Wiegand readers



A Wiegand reader and its wiring, including extra cables for buzzer, tamper detection, and LEDs.

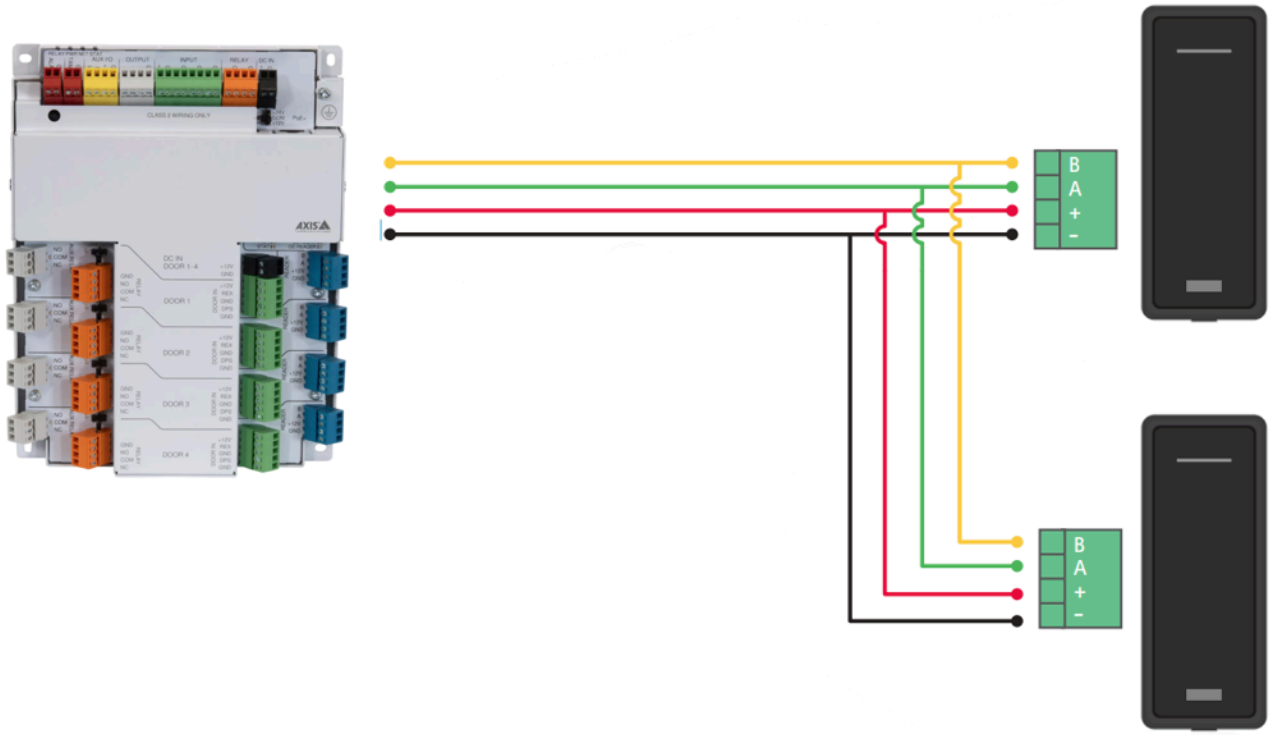
Advantages:

- Simple and widely compatible with older systems.

Drawbacks:

- No encryption. Data is transmitted in plain text, making it easy to intercept.
- One-way communication. The controller can't send commands back to the reader. This means that there is no way of detecting whether a reader has been tampered with or replaced – the reader is unsupervised.
- Complex wiring. A reader using the Wiegand protocols needs extra cables for reader buzzer, tamper detection, and LEDs.
- The maximum cable distance is 500 feet (~150 meters).

4.2 OSDP readers



OSDP readers (right) and their wiring to a door controller (left). Features like LED control, buzzer activation, and reader supervision don't require extra cables.

OSDP uses RS-485 wiring. This is a serial communication standard for transmitting data over long distances using twisted-pair cables. It's commonly used in systems that require reliable, multi-point communication. Key features include long-distance transmission and multi-drop capability.

Advantages:

- Encrypted communication prevents credential interception.
- OSDP allows the controller to send commands back to the reader. This bi-directional data exchange allows supervision and remote configuration. It also simplifies the wiring.
- RS-485 wiring enables longer maximum cable distance.
- Multi-drop enables multiple readers to share a single connection.

4.3 Usability

Table 4.1 *Comparison of usability with Wiegand and OSDP readers.*

	Wiegand	OSDP
Security	No encryption, vulnerable to hacking	AES-128 encryption, tamper detection
Communication	One-way (reader to controller)	Two-way
Cable distance	up to 500 feet (~150 meters)	up to 4000 feet (~1200 meters)
Multi-drop	No, one device one bus	Yes, multi-device supported on one bus
Tamper detection	No, needs additional wiring	Yes
Supervision	No, needs additional wiring	Yes

	Wiegand	OSDP
Data integrity	Susceptible to credential replay attacks	Encrypted, secure transmission
Installation complexity	Complex wiring (D0/D1 and LEDs, tamper, buzzer)	Easy (RS-485, A and B)
Scalability	Limited by wiring constraints	Can connect multiple readers in a daisy-chain
Best use case	Legacy systems, low security needs	Modern secure installations in sectors such as government or enterprise

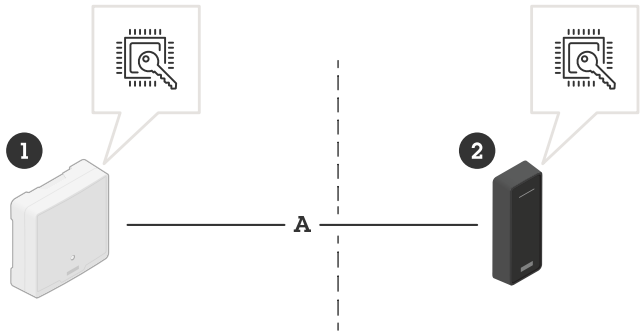
4.4 Security

Security should be the top priority when choosing an access control protocol. Wiegand's lack of encryption makes it susceptible to several types of attacks.

- Credential interception. Attackers can eavesdrop on data lines and capture credentials.
- Replay attacks. Once captured, the same credential can be replayed to gain unauthorized access.
- Tampering. The system can't detect if a reader is removed or replaced.

In contrast, OSDP mitigates these risks by encrypting data with AES-128 (Secure Channel) and providing device supervision. This ensures that the controller can detect if a reader has been tampered with, and thereby prevent unauthorized access.

The encryption keeps the data secure, but protecting the keys keeps the encryption secure. Without strong key protection, the whole system can be at risk. That's why Secure Channel keys should be kept safe, in special hardware chip at both ends: controller and reader. These secure hardware areas, such as secure elements, are built to stop attackers from getting the keys even if they get physical access to the device.



Achieving end-to-end security with secure keystore in access control. The master key and the individual secure channel base key (SCBK) are both stored in secure keystores, in devices on each side of the door.

1 *Door controller installed on the secure side of the door*
2 *Reader installed on the non-secure side of the door*
3 *A: OSDP secure channel communication*

Table 4.2 *Comparison of security aspects with Wiegand and OSDP readers.*

	Wiegand	OSDP
Encryption	None, plaintext data	AES-128 encryption
Data interception	Easy to intercept credentials	Encrypted to prevent interception

	Wiegand	OSDP
Replay attacks	Credentials can be copied/replayed	Prevented by encryption
Tamper detection	No, cannot detect tampered readers	Yes, controller monitors reader status
Supervision	No, controller cannot verify reader status	Yes, real-time supervision
Compliance	Not recommended for secure environments	Meets modern security standards

5 Recommendations

In today's security landscape, Wiegand is no longer a viable option for new installations. Organizations should transition to OSDP readers for better security, reliability, and future scalability.

- Evaluate your current access control infrastructure. If you're currently using Wiegand, start planning a migration strategy. Determine whether a full OSDP migration or a Wiegand-to-OSDP converter is the best option.
- For new installations, choose OSDP readers whenever possible to ensure encrypted, tamper-resistant communication.
- Work with security professionals to implement a secure, modern access control system that protects against threats.

6 Migrating from Wiegand to OSDP

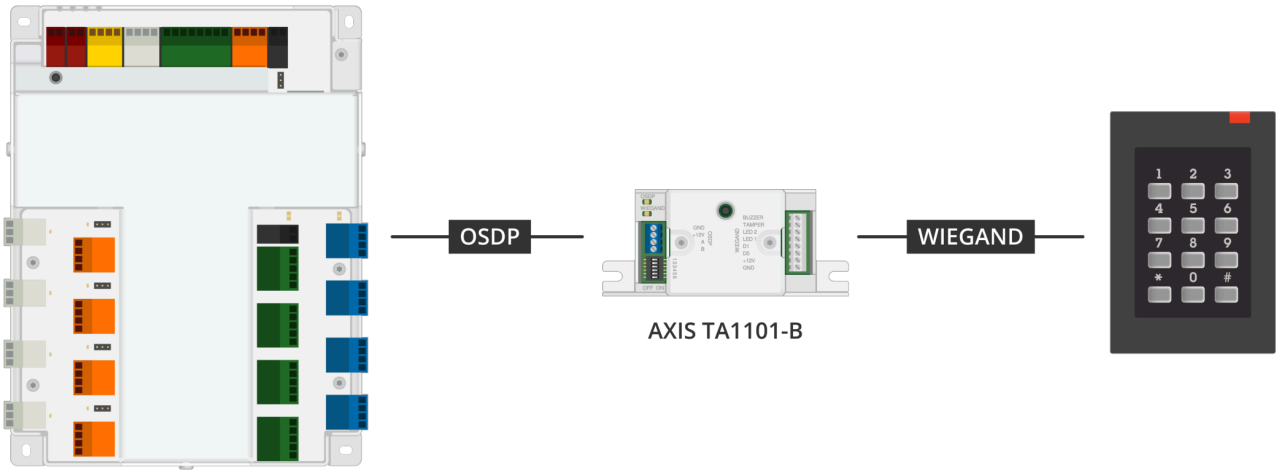
Many organizations still rely on Wiegand readers but want to enhance security without replacing their entire system. There are two practical migration paths. Both options improve security, but direct OSDP implementation is the best long-term investment for organizations looking to future-proof their access control systems.

6.1 Option 1: Replace Wiegand readers with OSDP readers

This is the best long-term solution. By replacing outdated Wiegand readers with OSDP-compliant models, organizations can benefit from encryption, two-way communication, and reader supervision. However, this requires ensuring that the access control panel supports OSDP.

6.2 Option 2: Use a Wiegand-to-OSDP converter

For organizations unable to replace all readers immediately, a Wiegand-to-OSDP converter is a cost-effective alternative. This device encrypts Wiegand data before sending it to an OSDP-compatible controller, improving security without requiring a complete hardware overhaul.



AXIS A1710-B

AXIS TA1101-B

You can improve security by using a Wiegand-to-OSDP converter (middle).

T10227329/EN/M1.7/2505

About Axis Communications

Axis enables a smarter and safer world by improving security, safety, operational efficiency, and business intelligence. As a network technology company and industry leader, Axis offers video surveillance, access control, intercoms, and audio solutions. These are enhanced by intelligent analytics applications and supported by high-quality training.

Axis has around 5,000 dedicated employees in over 50 countries and collaborates with technology and system integration partners worldwide to deliver customer solutions. Axis was founded in 1984, and the headquarters are in Lund, Sweden.