

BIAŁA KSIĘGA

Maj 2025

Streszczenie

Chociaż Wiegand pozostaje powszechnie stosowanym interfejsem w zastosowaniach kontroli dostępu, jego atrakcyjność maleje przez wady obniżające bezpieczeństwo. Organizacje, dla których bezpieczeństwo jest priorytetem, powinny przejść na protokół OSDP, aby lepiej chronić się przed atakami. OSDP zapewnia szyfrowaną, nadzorowaną komunikację, co czyni go pierwszym wyborem w środowiskach o wysokim poziomie bezpieczeństwa. Modernizacja systemu kontroli dostępu do stosowania protokołu OSDP oznacza wyższe bezpieczeństwo dziś i w przyszłości, kiedy zagrożenia będą się zmieniać.

Spis treści

1	Wprowadzenie	4
2	Kontrola dostępu w rozwiązaniach bezpieczeństwa	4
3	Protokoły komunikacyjne czytnika z kontrolerem	4
3.1	Dotychczasowy standard: Wiegand	4
3.2	Bezpieczna alternatywa: OSDP	5
3.2.1	Program OSDP Verified	5
4	Porównanie czytników Wiegand i OSDP	5
4.1	Czytniki Wiegand	5
4.2	Czytniki OSDP	6
4.3	Użyteczność	6
4.4	Bezpieczeństwo	7
5	Zalecenia	8
6	Przejsście z protokołu Wiegand na OSDP	8
6.1	Opcja 1: zastąpienie czytników Wiegand czytnikami OSDP	8
6.2	Opcja 2: zastosowanie konwertera Wiegand-OSDP	9

1 Wprowadzenie

Krytycznie ważnym aspektem systemów kontroli dostępu są stosowane przez nie protokoły komunikacyjne.

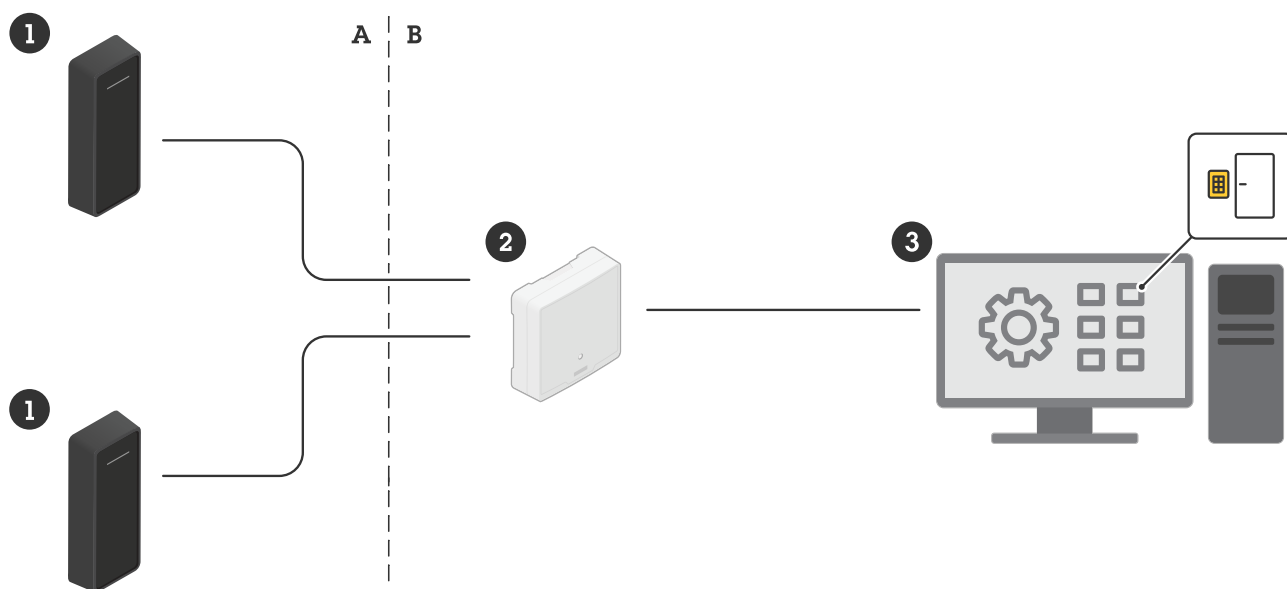
W niniejszej specyfikacji omówiono dwa główne protokoły komunikacyjne wykorzystywane w komunikacji pomiędzy czytnikiem a kontrolerem drzwiowym w systemach kontroli dostępu. Przyjrzymy się ich zaletom i wadom w kontekście bezpieczeństwa i powiemy, jak przejść do bezpieczniejszej opcji.

2 Kontrola dostępu w rozwiązaniach bezpieczeństwa

Systemy kontroli dostępu są niezbędne do ochrony budynków, mienia i osób. Dzięki nim wyłącznie upoważnione osoby mają dostęp do zabezpieczonych obszarów, co podnosi bezpieczeństwo i wydajność pracy. Systemy te są szeroko stosowane w różnych sektorach, w biurach, centrach przetwarzania danych, placówkach ochrony zdrowia oraz instytucjach rządowych i samorządowych.

Typowy system kontroli dostępu składa się z trzech kluczowych elementów.

- 1 Czytniki kontroli dostępu: urządzenia odczytujące dane uwierzytelniające użytkownika i przesyłające je do kontrolera. Najczęściej wykorzystywane dane uwierzytelniające użytkownika obejmują karty, mobilne dane uwierzytelniające, kody PIN i dane biometryczne.
- 2 Kontrolery drzwiowe: moduły decyzyjne przetwarzające dane uwierzytelniające i decydujące o przyznaniu lub odmowie dostępu.
- 3 Oprogramowanie zarządzające: interfejs, w którym administratorzy konfiguruje zasady dostępu, monitorują aktywność i zarządzają danymi użytkowników.



W systemie kontroli dostępu czytniki (1) są instalowane na zewnątrz drzwi (obszar niezabezpieczony, A) i komunikują się z kontrolerem drzwiowym (2) zainstalowanym wewnątrz (obszar zabezpieczony, B).

3 Protokoły komunikacyjne czytnika z kontrolerem

Z biegiem czasu protokoły kontroli dostępu ewoluowały ku poprawie bezpieczeństwa, funkcjonalności i łatwości integracji. Przyjrzymy się bliżej dwóm głównym protokołom.

3.1 Dotychczasowy standard: Wiegand

Wiegand przesyła dane uwierzytelniające z czytnika do kontrolera poprzez dwie linie danych. Standard Wiegand istnieje od dziesięcioleci i jest nadal szeroko stosowany głównie ze względu na swoją prostotę i zgodność ze starszymi systemami.

Główną wadą standardu Wiegand jest niski poziom bezpieczeństwa. Przede wszystkim nie ma szyfrowania. Dane są przesyłane w postaci zwykłego tekstu, a przez to podatne na przechwytywanie i ataki klonowania.

3.2 Bezpieczna alternatywa: OSDP

Protokół OSDP (Open Supervised Device Protocol) został opracowany przez stowarzyszenie Security Industry Association (SIA) w celu poprawy współpracy różnych produktów w dziedzinie kontroli dostępu i bezpieczeństwa. OSDP został zatwierdzony jako międzynarodowy standard przez Międzynarodową Komisję Elektrotechniczną (IEC) i wprowadza szyfrowanie AES-128, dwukierunkową komunikację i monitorowanie urządzeń w czasie rzeczywistym. Ponieważ protokół OSDP umożliwia kontrolerowi wysyłanie poleceń zwrotnych do czytnika, dostępne są również takie funkcje jak sterowanie wskaźnikami LED, załączanie brzęczyka i wykrywanie sabotażu.

Kluczową cechą protokołu OSDP jest tryb Secure Channel umożliwiający bezpieczną transmisję nieprzetworzonych danych uwierzytelniających pomiędzy czytnikami kart inteligentnych i kontrolerami. Jest to szczególnie przydatne w przypadku zaawansowanych metod uwierzytelniania w rodzaju uwierzytelniania biometrycznego i mobilnego.

3.2.1 Program OSDP Verified

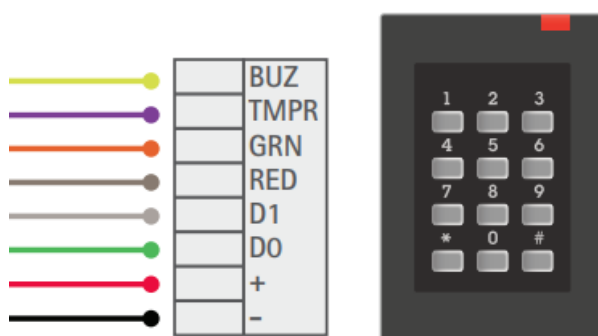
Program SIA OSDP Verified to kompleksowa inicjatywa testowa, która potwierdza, że urządzenie jest zgodne ze standardem OSDP i powiązаныmi profilami parametrów. Organizacja SIA prowadzi listę zweryfikowanych urządzeń, które przetestowano i uznano za spełniające kryteria standardu i profili wskazanych na liście. W materiałach marketingowych urządzeń znajdujących się na liście można wykorzystywać znak OSDP Verified.

Znak OSDP Verified to zapewnienie złożone wobec integratorów, projektantów i praktyków, że urządzenia OSDP będą działać zgodnie z przeznaczeniem w różnych rodzajach systemów kontroli dostępu.

4 Porównanie czytników Wiegand i OSDP

Czytniki mają wady i zalety zależnie od wykorzystywanego protokołu komunikacyjnego.

4.1 Czytniki Wiegand



Czytnik Wiegand wraz z okablowaniem, w tym dodatkowe kable do brzęczyka, detekcji sabotażu i wskaźników LED.

Zalety:

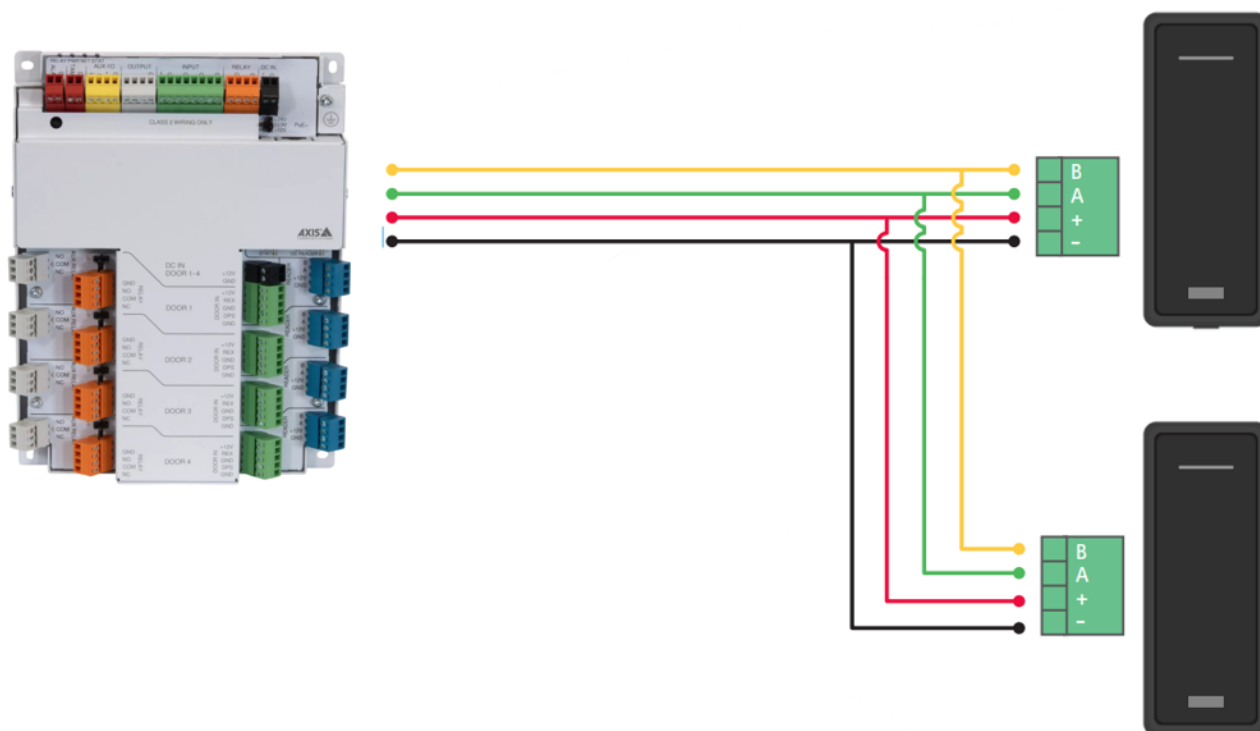
- Prostota i szeroka kompatybilność ze starszymi systemami.

Wady:

- Brak szyfrowania. Dane są przesyłane w postaci zwykłego tekstu, co ułatwia ich przechwycenie.
- Jednokierunkowa komunikacja. Kontroler nie może wysyłać poleceń zwrotnie do czytnika. Oznacza to, że nie ma sposobu na wykrycie, czy doszło do sabotażu lub wymiany czytnika – czytnik nie jest nadzorowany.

- Skomplikowane okablowanie. Czytnik korzystający z protokołów Wiegand potrzebuje dodatkowych kabli do brzęczyka czytnika, wykrywania sabotażu i wskaźników LED.
- Maksymalna długość kabla wynosi 150 m (500 stóp).

4.2 Czytniki OSDP



Czytniki OSDP (po prawej) i okablowanie do kontrolera drzwiowego (po lewej). Funkcje takie jak sterowanie wskaźnikami LED, załączenie brzęczyka i nadzór czytnika nie wymagają dodatkowych kabli.

Protokół OSDP wykorzystuje okablowanie RS-485. Jest to standard komunikacji szeregowej służący do przesyłania danych na duże odległości za pomocą kabla typu skrętka. Jest on powszechnie stosowany w systemach wymagających niezawodnej, wielopunktowej komunikacji. Kluczowe funkcje obejmują transmisję na duże odległości i magistralę multi-drop.

Zalety:

- Szyfrowana komunikacja uniemożliwia przechwytywanie danych uwierzytelniających.
- Protokół OSDP umożliwia kontrolerowi wysyłanie poleceń zwrótnie do czytnika. Ta dwukierunkowa wymiana danych umożliwia nadzór i zdalne konfigurowanie, jak również upraszcza okablowanie.
- Okablowanie RS-485 umożliwia uzyskanie większej maksymalnej długości kabla.
- Magistrala multi-drop umożliwia działanie wielu czytników na jednym współdzielonym połączeniu.

4.3 Użyteczność

Tabela 4.1 Porównanie użyteczności czytników Wiegand i OSDP.

	Wiegand	OSDP
Bezpieczeństwo	Brak szyfrowania, podatność na ataki hakerskie	Szyfrowanie AES-128, wykrywanie sabotażu
Komunikacja	Jednokierunkowa (czytnik do kontrolera)	Dwukierunkowa
Długość kabla	maks. 150 m (500 stóp)	maks. 1200 m (4000 stóp)

	Wiegand	OSDP
Magistrala multi-drop	Brak, jedno urządzenie, jedna magistrala	Tak, obsługa wielu urządzeń na jednej magistrali
Wykrywanie sabotażu	Brak, wymaga dodatkowego okablowania	Tak
Nadzór	Brak, wymaga dodatkowego okablowania	Tak
Integralność danych	Podatność na ataki polegające na powtórnym użyciu przechwyconych danych uwierzytelniających	Szyfrowana, bezpieczna transmisja
Złożoność instalacji	Skomplikowane okablowanie (D0 / D1 i wskaźniki LED, sabotaż, brzęczyk)	Brak skomplikowania (RS-485, A i B)
Skalowalność	Ograniczona przez okablowanie	Możliwość łańcuchowego połączenia wielu czytników
Najlepsze zastosowania	Starsze systemy, niskie wymagania w zakresie bezpieczeństwa	Nowoczesne, bezpieczne instalacje wymagane w instytucjach rządowych, firmach itp.

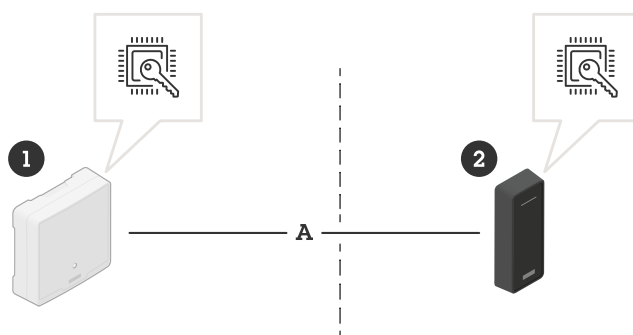
4.4 Bezpieczeństwo

Bezpieczeństwo powinno być najwyższym priorytetem przy wyborze protokołu komunikacyjnego w systemie kontroli dostępu. Brak szyfrowania w protokole Wiegand czyni go podatnym na kilka rodzajów ataków.

- Przechwytywanie danych uwierzytelniających. Włamywacz może podsłuchać linie danych i przechwycić dane uwierzytelniające.
- Powtarzanie ataków. Raz przechwycone dane uwierzytelniające mogą zostać użyte повторно do nieautoryzowanego dostępu.
- Sabotaż. System nie jest w stanie wykryć usunięcia lub wymiany czytnika.

W odróżnieniu od tych zagrożeń protokół OSDP nie dopuszcza do ich powstania poprzez szyfrowanie danych za pomocą algorytmu AES-128 (Secure Channel) oraz zapewnienie nadzoru nad urządzeniem. Dzięki temu kontroler jest w stanie wykryć naruszenie czytnika i zapobiec tym samym nieautoryzowanemu dostępowi.

Szyfrowanie zapewnia bezpieczeństwo danych, a ochrona kluczy bezpieczeństwa szyfrowania. Bez silnej ochrony kluczy cały system jest podatny na zagrożenia. Dlatego też klucze Secure Channel powinny być przechowywane w bezpiecznym miejscu, w specjalnym układzie sprzętowym po obu końcach połączenia: w kontrolerze i w czytniku. Te bezpieczne obszary sprzętowe są skonstruowane w taki sposób, aby uniemożliwić włamywaczom pozyskanie kluczy, nawet jeżeli uzyskają fizyczny dostęp do urządzenia.



Zapewnienie kompleksowego bezpieczeństwa za pomocą bezpiecznego magazynu kluczy w systemie kontroli dostępu. Klucz główny i indywidualny klucz SCBK przechowywane są w bezpiecznych magazynach kluczy w urządzeniach po obu stronach drzwi.

- 1 Kontroler drzwiowy zainstalowany po bezpiecznej stronie drzwi
- 2 Czytnik zainstalowany po niezabezpieczonej stronie drzwi
- 3 A: Komunikacja OSDP Secure Channel

Tabela 4.2 Porównanie aspektów bezpieczeństwa dla czytników Wiegand i OSDP.

	Wiegand	OSDP
Szyfrowanie	Brak, dane w postaci zwykłego tekstu	Szyfrowanie AES-128
Przechwytywanie danych	Łatwe przechwycenie danych uwierzytelniających	Szyfrowanie zapobiegające przechwyceniu
Powtarzanie ataków	Możliwość skopiowania / powtórnego użycia danych uwierzytelniających	Ochrona poprzez szyfrowanie
Detekcja sabotażu	Brak, nie jest możliwe wykrycie sabotażu czytnika	Kontroler monitoruje stan czytnika
Nadzór	Brak, kontroler nie może weryfikować stanu czytnika	Nadzór w czasie rzeczywistym
Zgodność z przepisami	Niezalecany dla środowisk o wysokim poziomie bezpieczeństwa	Spełnia nowoczesne standardy bezpieczeństwa

5 Zalecenia

We współczesnym podejściu do bezpieczeństwa protokół Wiegand nie jest już opcją braną pod uwagę w nowych instalacjach. Organizacje powinny przejść na czytniki OSDP zapewniających wyższe bezpieczeństwo, niezawodność i skalowalność w przyszłości.

- Należy dokonać oceny obecnej infrastruktury kontroli dostępu. Jeżeli stosowany jest protokół Wiegand, należy zaplanować strategię odejścia od niego. Powinno się zdecydować, czy najlepszą opcją jest pełne przejście na protokół OSDP czy zastosowanie konwertera Wiegand-OSDP.
- W przypadku nowych instalacji należy w miarę możliwości wybierać czytniki OSDP, aby zapewnić szyfrowaną komunikację odporną na sabotaż.
- Zaleca się współpracę ze specjalistami ds. bezpieczeństwa celem wdrożenia bezpiecznego, nowoczesnego systemu kontroli dostępu, który chroni przed zagrożeniami.

6 Przejście z protokołu Wiegand na OSDP

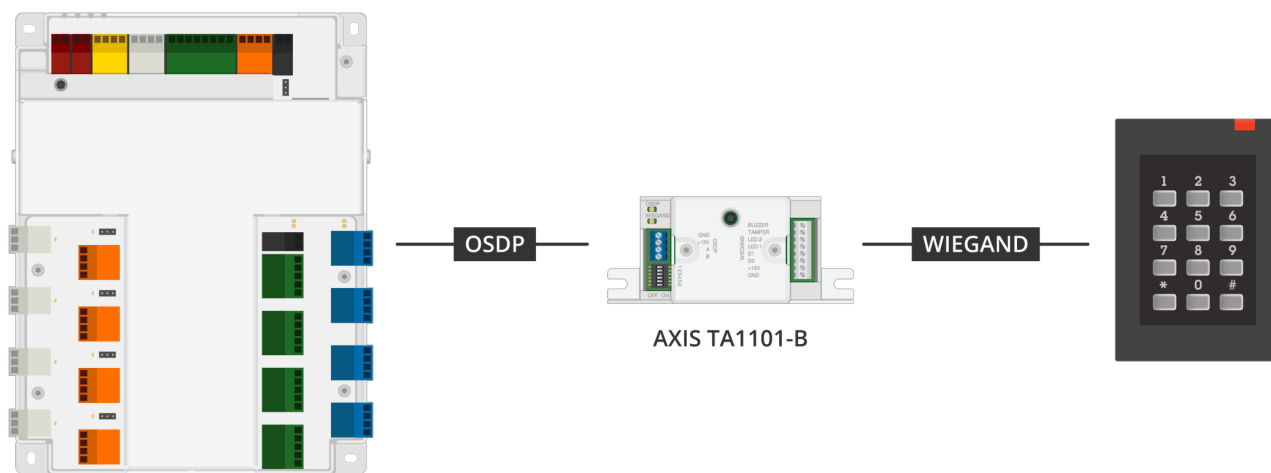
Wiele organizacji nadal korzysta z czytników Wiegand, ale dąży do zwiększenia bezpieczeństwa bez wymiany całego systemu. Istnieją dwie praktyczne ścieżki przejścia do bezpiecznego rozwiązania. Obie opcje poprawiają bezpieczeństwo, ale bezpośrednie wdrożenie protokołu OSDP jest najlepszą długoterminową inwestycją dla organizacji dążących do zabezpieczenia posiadanych systemów kontroli dostępu przed wyzwaniami stawianymi przez przyszłość.

6.1 Opcja 1: zastąpienie czytników Wiegand czytnikami OSDP

Jest to najlepsze rozwiązanie w dłuższej perspektywie czasowej. Wymieniając przestarzałe czytniki Wiegand na modele zgodne z protokołem OSDP, organizacje otrzymują korzyści w postaci szyfrowania, dwukierunkowej komunikacji i nadzoru nad czytnikami. Wymaga to jednak zapewnienia obsługi protokołu OSDP w centralce kontroli dostępu.

6.2 Opcja 2: zastosowanie konwertera Wiegand-OSDP

Dla organizacji, które nie są w stanie natychmiast wymienić wszystkich czytników, opłacalną alternatywą jest konwerter Wiegand-OSDP. Urządzenie to szyfruje dane Wiegand przed wysłaniem ich do kontrolera zgodnego z OSDP, co podwyższa bezpieczeństwo bez konieczności całkowitej wymiany sprzętu.



AXIS A1710-B

Możliwość zwiększenia bezpieczeństwa przy użyciu konwertera Wiegand-OSDP (w środku).

O firmie Axis Communications

Axis wspiera rozwój inteligentnego oraz bezpiecznego świata przez poprawę bezpieczeństwa, ochrony, efektywności działania i wiedzy biznesowej. Jako firma zajmująca się technologiami sieciowymi oraz lider branży, Axis oferuje rozwiązania z zakresu dozoru wizyjnego, kontroli dostępu, systemów domofonowych i systemów audio. Ich rozszerzeniem i uzupełnieniem są inteligentne aplikacje analityczne oraz wysokiej jakości szkolenia.

Axis zatrudnia około 5000 pracowników w ponad 50 krajach oraz współpracuje z partnerami z obszaru technologii i integracji systemów na całym świecie w celu dostarczania swoich rozwiązań klientom. Firma została założona w 1984 roku i ma swoją siedzibę w Lund w Szwecji.