BEZPIECZEŃSTWO SYSTEMÓW KONTROLI DOSTĘPU FIRMY INNER RANGE

Andrzej TOMCZAK

„Jakie wszystko staje się proste, gdy się patrzy z daleka, pomija się szczegóły i nic się o nich nie wie"
Bernard Minier

Szerokie zainteresowanie kwestiami bezpieczeństwa systemów kontroli dostępu nastąpiło po uchwaleniu normy PN -EN 60839-11-1:2014-01 *Systemy alarmowe i elektroniczne systemy zabezpieczeń. Część 11-1: Elektroniczne systemy kontroli dostępu. Wymagania dotyczące systemów i komponentów*, która została opublikowana w języku polskim w 2020 r. Zapisano w niej kilka ogólnych wymogów dotyczących bezpieczeństwa, które zależą od stopnia zabezpieczenia wykonywanego systemu kontroli dostępu (SKD). Tablica 1, znajdująca się w tej normie pozwala na przyporządkowanie analizowanego obiektu do odpowiedniego stopnia zabezpieczenia.

Wymogi aktualnej normy na systemy kontroli dostępu

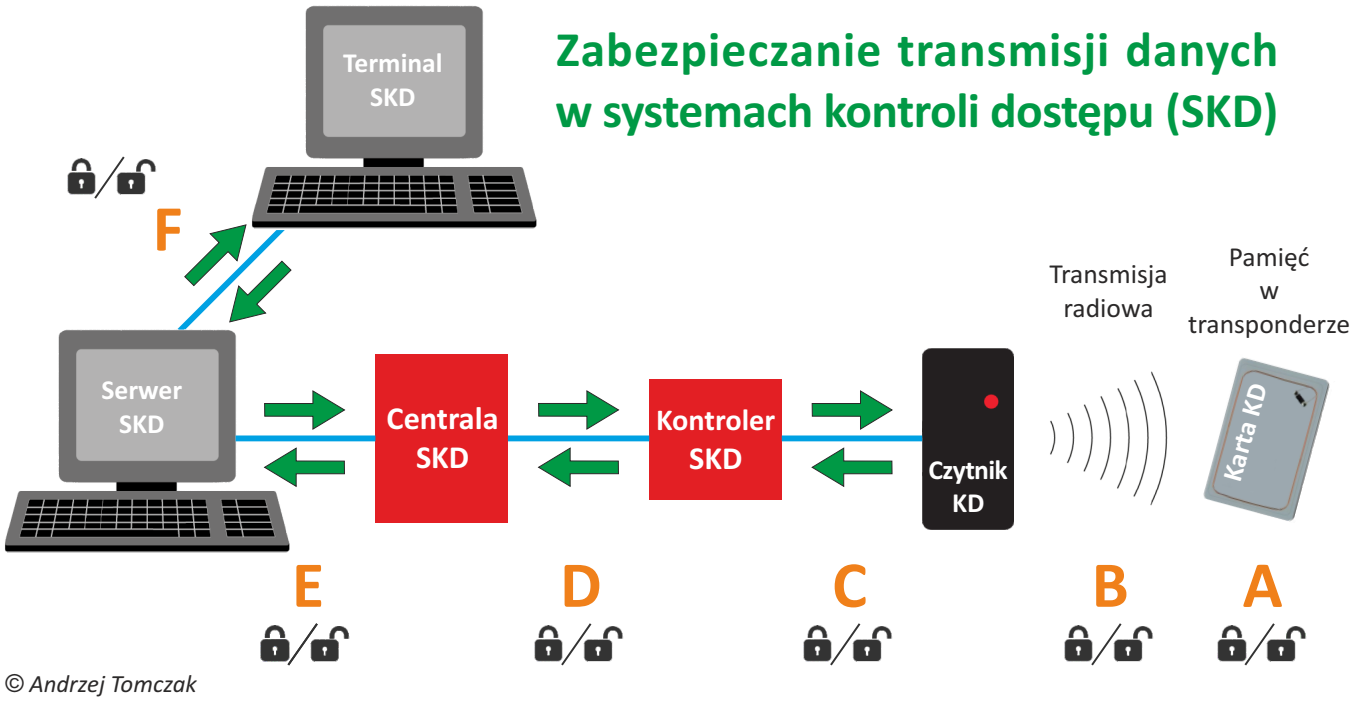
Większość obiektów, w których systemy KD są zainstalowane ze względów bezpieczeństwa, można sklasyfikować w stopniach 3. i 4. Tylko hotele, biura i małe przedsiębiorstwa przyporządkowano do stopni 1. i 2. W zaleceniach dla stosowania 4. stopnia zabezpieczenia wskazano obiekty infrastruktury krytycznej, obiekty wojskowe i rządowe, obszary produkcji krytycznej oraz R&D (obszary, w których prowadzi się prace badawczo-rozwojowe).

W przypadku normy na systemy KD, stopnień zabezpieczenia jest przypisywany do chronionych obszarów, w związku z tym w danym systemie mogą występować przejścia kontroli dostępu wykonane w różnych stopniach zabezpieczenia; z reguły od stopnia 2. do 4. Oczywistym jest, że komponenty wykorzystywane wspólnie, np. centrale czy kontrolery, muszą być wykonane w najwyższym zastosowanym stopniu zabezpieczenia. W normie postawiono szereg wymagań dotyczących m.in. bezpieczeństwa identyfikatorów i szyfrowania komunikacji. Przykładowo: w 3. i 4. stopniu zabezpieczenia informacja przechowywana w identyfikatorze powinna być zabezpieczona przed nieautoryzowaną modyfikacją lub kopiowaniem. Jak również komunikacja radiowa pomiędzy czytnikiem a identyfikatorem powinna być szyfrowana (w stopniu 4. zawsze,

Klasyfikacja stopnia zabezpieczenia
(wg PN-EN 60839-11-1:2014-01, Tablica 1)

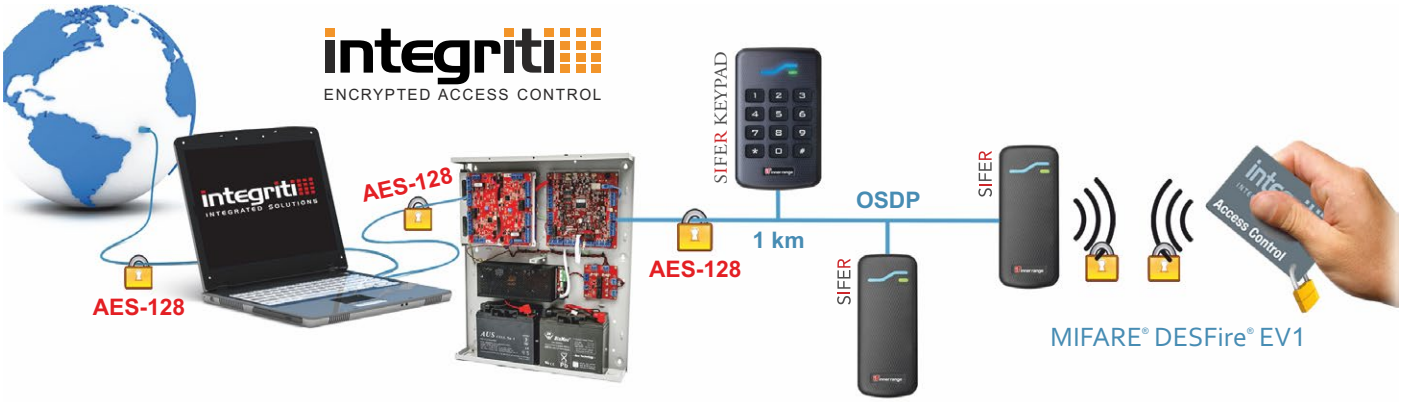
Stopień	1	2	3	4
Poziom ryzyka	niski	niski do średniego	średni do wysokiego	wysoki
Zastosowanie	organizacja ruchu, zabezpieczanie zasobów niskiej wartości	organizacja ruchu, zabezpieczanie zasobów niskiej do średniej wartości	w mniejszym stopniu organizacja ruchu, zabezpieczanie zasobów handlowych od średniej do wysokiej wartości	głównie zabezpieczanie bardzo wysokich wartości handlowych albo infrastruktury krytycznej
Umiejętności/wiedza intruzów/atakujących	niski poziom umiejętności, niski poziom wiedzy o SKD, brak wiedzy o identyfikatorach i technologii IT małe środki finansowe na dokonanie ataków	średni poziom umiejętności i wiedzy o SKD, niski poziom wiedzy o identyfikatorach i technologii IT małe do średnich środki finansowe na dokonanie ataków	wysoki poziom umiejętności i wiedzy o SKD, średni poziom wiedzy o identyfikatorach i technologii IT średnie środki finansowe na dokonanie ataków	bardzo wysoki poziom umiejętności i wiedzy o SKD, wysoki poziom wiedzy o identyfikatorach i technologii IT duże środki finansowe na dokonanie ataków
Typowe przykłady	hotele	biura, małe przedsiębiorstwa	przemysł, administracja, obiekty finansowe	obszary wysoce wrażliwe (obiekty wojskowe, rządowe, R&D, obszary produkcji krytycznej)

natomiast w stopniu 3. wtedy, gdy identyfikator jest stosowany jako jedyna metoda rozpoznawania). W normie postawiono również wymagania na transmisję danych wewnątrz systemu KD. I tak, w stopniu 3. i 4. komunikacja pomiędzy kontrolerem (centralą) a czytnikiem powinna być szyfrowana. Wyjątkowo w stopniu 3. można odstąpić od szyfrowania pod warunkiem mechanicznego zabezpieczenia łączy komunikacyjnych między czytnikiem i centralą (kontrolerem) np. poprzez prowadzenie przewodów w osłonie rurek metalowych. Dodatkowo w stopniach 3. i 4. wprowadzono wymóg szyfrowania transmisji pomiędzy komponentami systemu kontroli dostępu przy korzystaniu z sieci współdzielonych z innymi użytkownikami. Dotyczy to np. komponentów SKD podłączanych do współdzielonych sieci komputerowych. Na rys. 1 za pomocą symbolu kłódki zaznaczono miejsca, w których może wystąpić wymóg zabezpieczenia danych.



© *Andrzej Tomczak*

Rys. 1. Miejsca newralgiczne z punktu widzenia bezpieczeństwa transmisji danych w SKD



Rys. 2. Szyfrowanie End-To-End w systemie Integriti firmy Inner Range

Bezpieczne technologie identyfikacji

Dla bezpieczeństwa obiektu zabezpieczonego systemem KD niewątpliwie ważny będzie dobór typu identyfikatora i jego prawidłowa implementacja w systemie (**A**). Zdarzają się bowiem sytuacje, że z założenia „bezpieczny" identyfikator, nieprawidłowo zaimplementowany, staje się całkowicie niezabezpieczonym identyfikatorem. Takim przykładem jest nieuruchamianie dostępnych zabezpieczeń identyfikatora lub korzystanie do identyfikacji z numeru seryjnego (UID, CSN)[1], zamiast informacji, które można zapisać w pamięci identyfikatora i odpowiednio zabezpieczyć. Aktualnie za „najbezpieczniesze" identyfikatory uważa się te, które wykorzystują technologie **Seos** firmy HID, **Advant** firmy Legic i **Mifare Desfire EV1**, **EV2** i **EV3** firmy NXP Semiconductors.

W przypadku produktów firmy Legic występują dodatkowe zabezpieczenia technologii identyfikacji. Programowanie identyfikatorów jest możliwe przy użyciu programatora, do którego dostęp jest zabezpieczony specjalną kartą. Kolejnym zabezpieczeniem jest konieczność wstępnego zaprogramowania czytników, aby odczytywały identyfikatory przyporządkowane do danego obiektu. Identyfikatory niezgodne z zastosowanymi czytnikami nie będą ze sobą współpracowały.

Z wyborem technologii identyfikatorów wiąże się zastosowanie odpowiedniej technologii radiowej komunikacji pomiędzy czytnikiem a identyfikatorem (**B**). Za zastosowane zabezpieczenia odpowiada dostawca technologii identyfikacji, ponieważ dostarcza on albo gotowe czytniki (jak np. firma HID), albo komponenty do produkcji czytników (firmy Legic i NXP Semiconductors). W niektórych rozwiązaniach producent systemu kontroli dostępu może mieć wpływ na uruchomienie konkretnego poziomu zabezpieczenia komunikacji pomiędzy czytnikiem a identyfikatorem.

Systemy KD firmy Inner Range mogą wykorzystywać dowolne technologie identyfikacji, a więc również te powyżej wymienione, należące do najbezpieczniejszych, czyli HID Seos, Legic Advant oraz Mifare Desfire EV1, EV2 i EV3, zaś bezpośrednio w ofercie Inner Range występują czytniki, sprzedawane pod nazwą Sifer, oparte na technologii Mifare Desfire EV1 (z szyfrowaniem komunikacji pomiędzy czytnikiem a kontrolerem zgodnie ze standardem OSDP).

Systemy KD firmy Inner Range mogą wykorzystywać dowolne technologie identyfikacji, a więc również te powyżej wymienione, należące do najbezpieczniejszych, czyli HID Seos, Legic Advant oraz Mifare Desfire EV1, EV2 i EV3, zaś bezpośrednio w ofercie Inner Range występują czytniki, sprzedawane pod nazwą Sifer, oparte na technologii Mifare Desfire EV1 (z szyfrowaniem komunikacji pomiędzy czytnikiem a kontrolerem zgodnie ze standardem OSDP).

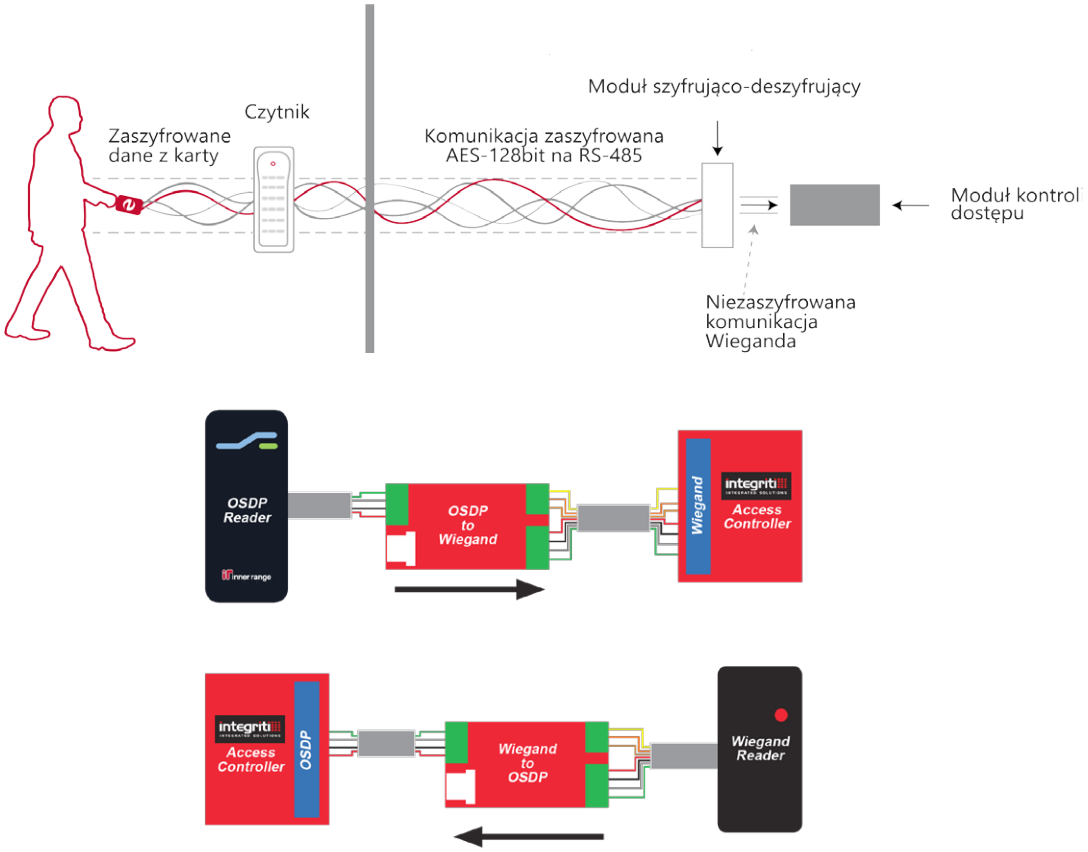
Komunikacja pomiędzy czytnikiem a kontrolerem (centralą) i wewnątrz systemu KD

Kolejnym newralgicznym elementem procesu komunikacji wewnątrz systemu KD jest transmisja danych pomiędzy czytnikiem a kontrolerem (centralą), na schemacie z rys. 1 oznaczonym literą **C**. Wprowadzenie obowiązku szyfrowania tej transmisji w stopniach 3.[2] i 4. wynika z zapisów normy PN-EN 60839-11-1:2014-01; przedtem takiego obowiązku nie było. W większości systemów KD stosowano do komunikacji pomiędzy czytnikiem a kontrolerem łącze nieszyfrowane, oparta na standardzie Wieganda. Aktualnie interfejs Wieganda można stosować w przypadku systemów stopni 1. i 2. oraz wyjątkowo w przypadku stopnia 3., gdy jest zapewnione mechaniczne zabezpieczenie łączy komunikacyjnych między czytnikami i centralą (kontrolerem).

W systemach firmy Inner Range dostępne są oba rozwiązania; transmisja za pośrednictwem nieszyfrowanego interfejsu Wieganda, a od 2016 r. również transmisja za pośrednictwem łącza szyfrowanego **OSDP**. Oprócz tego system Inner Range Integriti ma zagwarantowanie szyfrowanie wewnętrzne opisane na rys. 1 literami **D**, **E** i **F**. Na rys. 2 przedstawiono poglądowo transmisję danych w systemie Integriti, z szyfrowaniem E2E (ang. *End-To-End*), przy

[1] Identyfikatory wykonywane zgodnie ze standardami ISO/IEC obowiązkowo muszą mieć jawny numer seryjny, nazywany UID (ang. *Unique Identifier Number*) lub CSN (ang. *Card Serial Number*).

[2] Za wyjątkiem sytuacji zastosowania mechanicznej ochrony łącz komunikacyjnych np. poprzez prowadzenie przewodów w rurkach metalowych.



Rys. 3. Zastosowanie modułów szyfrująco-deszyfrujących w celu uzyskania szyfrowania komunikacji w systemach, które do tej pory wykorzystywały nieszyfrowaną transmisję Wieganda, na przykładzie konwertera OSDP<>Wiegand firmy Inner Range

Na podstawie materiałów firm Idesco i Inner Range

zastosowaniu czytników Mifare Desfire EV1. Równorzędnie można zastosować technologie HID SEOS i Legic Advant.
W przypadku systemów Inner Range, w których historycznie zastosowano interfejs Wieganda, istnieje możliwość zastosowania szyfrowania OSDP pomiędzy czytnikiem a kontrolerem (centralą). Jeżeli mamy do czynienia z systemem starszej generacji Concept 4000, to najprostszą metodą, (oprócz dość prostej migracji z systemu Concept 4000 do systemu Integriti, która jest polecana, ze względu na kończące się wsparcie dla systemu Concept 4000), jest zastosowanie nowego czytnika z wyjściem szyfrowanym oraz dodatkowego modułu szyfrująco-deszyfrującego, montowanego wewnątrz kontrolera, podłączanego bezpośrednio do wyjścia komunikacji Wieganda na płycie kontrolera (rys. 3).

Właściciele systemu Integriti wyposażonego w moduły kontroli dostępu, obsługujące interfejsy Wieganda, mają do wyboru dwie drogi uzyskania szyfrowania pomiędzy czytnikiem a kontrolerem (**C**). Albo wymiana czytników i zastosowanie powyżej opisanej metody, albo wymiana czytników oraz modułów obsługujących przejścia w kontrolerach na moduły nowej generacji, obsługujące czytniki z szyfrowaną komunikacją OSDP, zaimplementowaną na łączu RS 485. Aktualnie szyfrowana komunikacja OSDP jest wspierana przez wybrane czytniki HID, Legic oraz Mifare Desfire EV1, EV2 i EV3.

Podsumowanie

Jednym z elementów systemu zarządzania bezpieczeństwem Integriti firmy Inner Range jest system kontroli dostępu, który może być wykonywnay w 4. stopniu zabezpieczenia, zgodnie z normą PN-EN 60839-11-1:2014-01. Oczywiście wymaga to wybranie odpowiednich komponentów z szerokiej oferty Inner Range, która jest tak przygotowana, aby można było zaprojektować system w dowolnym stopniu zabezpieczenia. Wewntrzna integracja z sytemami sygnalizacji włamania i napadu, dozoru wizyjnego, sterowania windami i innymi systemami zabezpieczeń oraz zarządzania budynkiem, pozwala tworzyć funkcjonalne i dobrze współpracujce ze sobą systemy zarządzania bezpieczeństwem.

Andrzej TOMCZAK
Ekspert Polskiej Izby Systemów Alarmowych, przedstawiciel PISA w Polskim Komitecie Normalizacyjnym