

Technologia IronLogic Protected

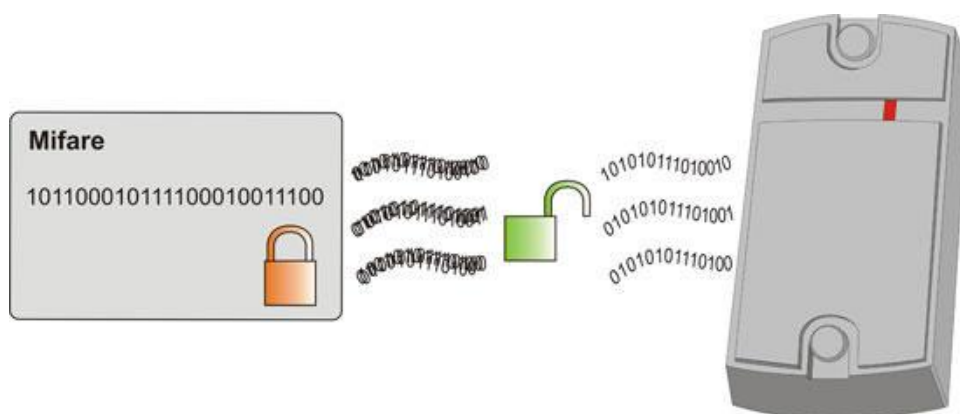
Ogólna zasada działania oraz procedura programowania

1. Zastosowanie technologii IronLogic-Protected

Technologia Protected została zaprojektowana przez IronLogic w celu ochrony przed nieautoryzowanym kopiowaniem i nieautoryzowaną próbą zaprogramowania kluczy w kontrolerach. Ochrona przed kopiowaniem i nieskoordynowaną obsługą polega na wstępnej inicjalizacji czytników oraz identyfikatorów (kluczy Mifare 1K) tym samym tajnym kodem. Karta Obiektu IronLogic jest używana jako bank tajnego kodu i należy przechowywać ją w bezpiecznym miejscu.

Podsumowując wstęp, technologia IL-Protected posiada podwójne zabezpieczenie:

- A.** Zabezpieczenie przed kopiowaniem kluczy do innego klucza.
- B.** Zabezpieczenie przed nieautoryzowaną próbą rejestracji dodatkowych kluczy przez osoby nieupoważnione. W tym przypadku tylko główny administrator (posiadacz Karty Obiektu) odpowiada za rejestrację nowych kluczy.



2. Urządzenia potrzebne do zastosowania technologii IronLogic Protected

2.1 Składniki

- Czytniki: CP-Z2MF / Matrix-II MF-I / Matrix-III MF-I .
- Adapter stacjonarny Z-2 USB MF (przeznaczony do inicjalizacji kluczy)
- Karta obiektu IronLogic 1+2 (karta i 3 breloki z tym samym tajnym kodem)
- Klucze dostępu (Karty / Breloki / Bransolety w technologii Mifare 1K)
- Dowolny kontroler samodzielny lub sieciowy.

2.2 Zasada działania

Głównymi elementami systemu są czytniki CP-Z2M / Matrix-II MF-I / Matrix-III MF-I, które mogą pracować w trybie IronLogic-Protected. W tym trybie czytnik działa tylko z kluczami, którym wcześniej administrator wprowadził tajne hasło. Tajne hasło znajduje się w Karcie Obiektu. W celu uruchomienia trybu IL-Protected konieczne jest przeniesienie tajnego hasła z Karty Obiektu na adapter stacjonarny Z2-USB MF, czytniki oraz na klucze Mifare 1K. Po zapisaniu tajnego hasła czytnik odczyta tylko te klucze, w których zostanie zapisane to samo tajne hasło, czytnik zignoruje wszystkie pozostałe klucze. Bez Karty Obiektu, dodawanie nowych czytników i nowych kluczy dostępu nie będzie możliwe dla wcześniej zaprojektowanego w tej technologii obiektu. Karta z tajnym kluczem nie jest możliwa do skopiowania. Procedura wpisywania tajnego hasła do kluczy dostępu Mifare 1K jest bardzo prosta i nie wymaga żadnego specjalistycznego oprogramowania (potrzebna jest tylko moc USB i odpowiedni firmware dla Z2-USB MF). Zайдź Z2-USB MF na stronie <https://hatpol.pl> i przejdź do zakładki „do pobrania” aby ściągnąć paczkę aktualizacji firmware dla funkcji Protected.

3. Urządzenia IronLogic wspierające technologię chronioną IronLogic

Czytnik CP-Z2MF podtynkowy

Czytnik CP-Z2MF natynkowy

Czytnik Matrix-II MF-I

Czytnik Matrix-III MF-I

Adapter stacjonarny Z-2 USB MF

Karta Obiektu IronLogic 1 + 2

Karty / breloki / Bransolety w technologii Mifare 1K

4. Procedura programowania

Zapisywanie / usuwania tajnego hasła do / z Adapter stacjonarny Z2-USB MF:

Adapter Z-2 USB MF musi mieć wgrane specjalne oprogramowanie układowe (firmware). Firmware może zainstalować administrator systemu, lub podczas zamówienia produktów można poprosić serwis o przygotowanie adaptera z odpowiednim firmware. Po udanej aktualizacji Z2-USB MF dioda będzie migać na czerwono już po włączeniu zasilania.

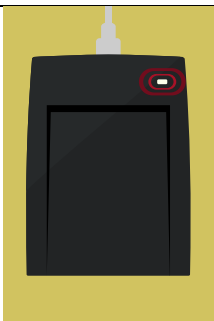
4.1 Wprowadzanie adaptera Z2-USB MF w stan rejestracji tajnego hasła

* Warunkiem wprowadzenia stanu rejestracji tajnego hasła w Z2-USB MF jest aktualizacja jego oprogramowania wewnętrznego.

Procedura:

- Zbliż Kartę Obiektu do Z-2 USB MF, dioda LED przestanie migać i zacznie świecić światłem ciągłym na czerwono, oznacza to że zapisanie tajnego hasła z Karty Obiektu do Z-2 USB MF zakończyło się pomyślnie.

Z-2 USB MF będzie przechowywać tajne hasło w swojej pamięci wewnętrznej tak długo, jak będzie zasilany lub do ponownego zbliżenia Karty Obiektu. Gdy tylko zasilanie USB zostanie odłączone od Z-2 USB MF, tajne hasło zostanie usunięte.

Stan Normalny (dioda mruga na czerwono)	Zbliżanie Karty Obiektu (dioda mruga na czerwono)	Stan rejestracji gotowy (dioda świeci na zielono)	Usuwanie Karty obiektu (dioda świeci na zielono)	Stan gotowy do zapisu tajnego hasła w kluczach dostępu Mifare 1K.(dioda świeci na czerwono)	Pomarańczowy kolor diody LED wskazuje, że zbliżona karta nie jest Kartą Obiektu.
					

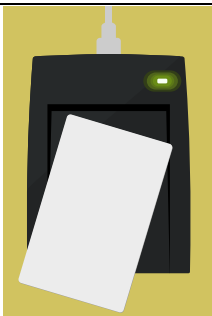
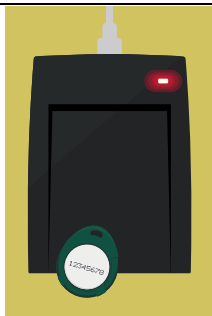
4.2 Przenoszenie (zapisywanie) tajnego hasła do kluczy dostępu Mifare 1K

* Warunkiem tworzenia kluczy dostępu jest przeniesienie (zapisanie) tajnego hasła z Karty Obiektu do Z2 USB MF.

Procedura:

Umieść klucz dostępu z chipem Mifare 1K na adapterze Z-2 USB MF. Czerwona dioda LED na adapterze

zgaśnie, a następnie zielony kolor zaświeci się wskazując, że tajne hasło zostało zapisane do klucza dostępu. Jeśli dioda LED będzie stale świecić na żółto oznaczać to, że zbliżona karta nie jest „pusta” kartą Mifare 1K i prawdopodobnie już wcześniej została zainicjowana przy użyciu innej Karty Obiektu.

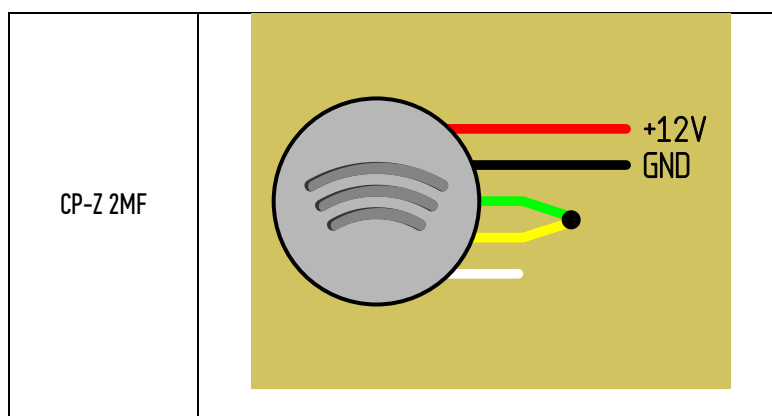
Wprowadzanie adaptera w stan zapisu za pomocą Karty Obiektu.	Adapter gotowy do zapisu tajnego hasła na kluczach dostępu Mifare 1K.	Zbliż klucz Mifare 1K, w celu wprowadzenia tajnego hasła.	Dioda Led zgaśnie na 2sek	Dioda LED zaświeci się na zielono jeśli klucz będzie prawidłowo powiązany tajnych hasłem	Żółty kolor diody LED oznacza, że z jakiegoś powodu tego klucza nie można zainicjować!
					

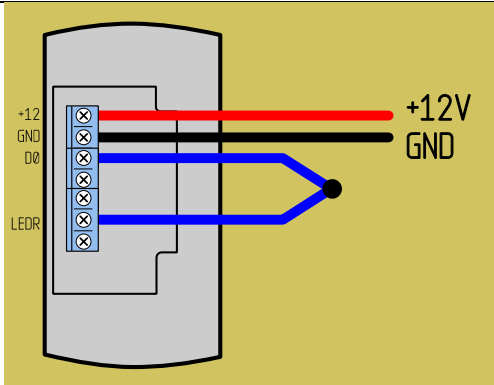
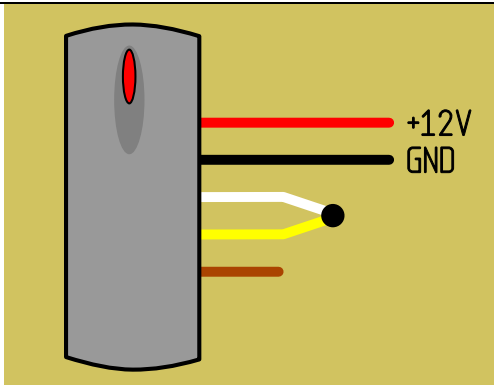
4.3 Przenoszenie (zapisywanie) tajnego hasła do czytnika

Zapisywanie tajnego hasła do czytnika odbywa się za pomocą Karty Obiektu, tej samej która wcześniej służyła nam do wprowadzenia hasła w adapterze Z2-USB MF.

Aby włączyć tryb Protected i zapisać tajne hasło do czytnika, należy wykonać następujące operacje:

- wyłączyć zasilanie czytnika (+12V oraz -12V DC) – połącz zaciski DATA-0 i zewnętrzne sterowanie diodą LED
- włącz zasilanie czytnika, dioda LED zaświeci się na czerwono - zbliż Kartę Obiektu do czytnika - dioda LED mignie 2 razy, a następnie zaświeci się ciągłym światłem (czytnik wpisuje tajne hasło do pamięci) - jeśli czytnik znajduje się już w trybie "Protected" i zostanie podjęta druga próba ustawienia tego trybu dla czytnika, dioda LED miga kilkakrotnie - wyłącz zasilanie czytnika – rozepnij zaciski DATA-0 i zewnętrzne sterowanie LED – teraz można podłączyć czytnik do kontrolera zgodnie z preferencjami.



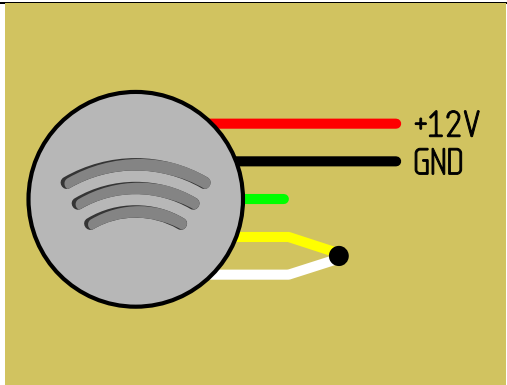
Matrix-II MF-I	
Matrix-III MF-I	

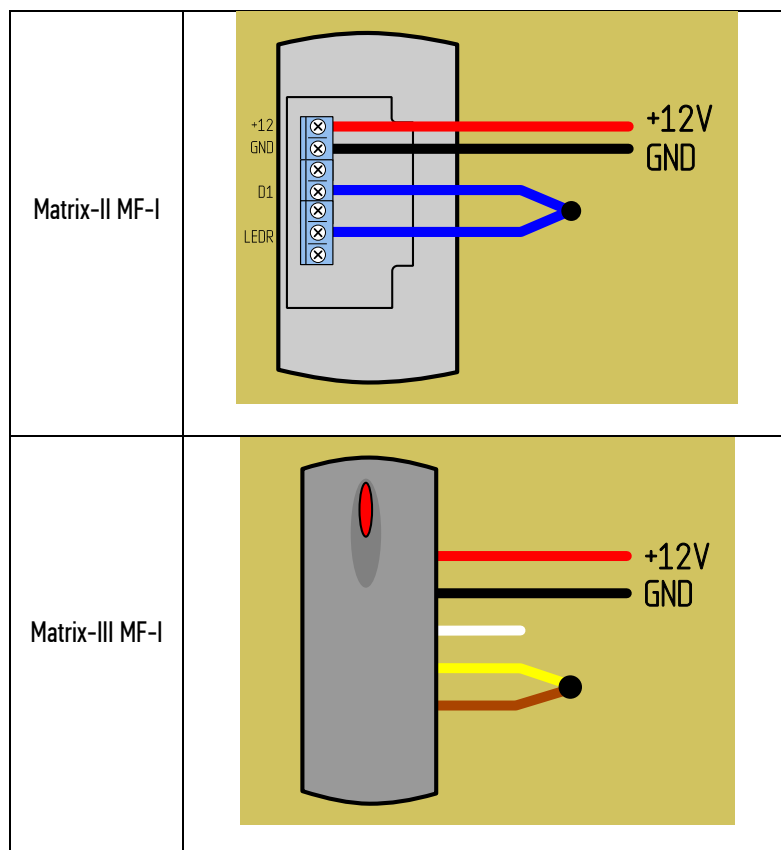
4.4 Usuwanie tajnego hasła z czytników IronLogic

Usuwanie tajnego hasła z czytnika odbywa się za pomocą Karty Obiektu (tej samej, która służyła wcześniej do uruchomienia trybu Protected).

Aby usunąć tajne hasło z czytnika, wykonaj następujące czynności:

- wyłącz zasilanie - odłącz przewody od kontrolera (jeśli takie podłączenie istnieje) - połącz zaciski DATA-1 i zewnętrzne sterowanie diodą LED - włącz zasilanie czytnika – zbliż Kartę Obiektu do czytnika - dioda LED zamruga 2 razy, a następnie zaświeci się ciągłym światłem (czytnik kasuje tajny kod wyłączając tryb Protected) - jeśli czytnik jest już w trybie "Otwartym" i podjęta zostanie druga próba ustawienia tego trybu dla czytnika, dioda LED miga kilkakrotnie - wyłącz zasilania – rozepnij zacisk DATA-1 od zewnętrzne sterowanie diodą LED – teraz można podłączyć czytnik do kontrolera zgodnie z preferencjami.

CP-Z 2MF	
----------	--



Do czytników IronLogic, które obsługują technologię IL Protected można dodać do 10 różnych Kart Obiektu.. Pozwala to na zastosowanie tej technologii na obiektach o dużej liczbie przejścia.

5. Często zadawane pytania

Pytanie: W kopercie Karta Obiektu znajdują się 1 x karta oraz 2 x brelok. Dlaczego?

Odpowiedź: 2 x brelok i 1 x karta to identyczne kopie (duplikaty kluczy). W przypadku utraty 1 klucza możesz wykorzystać zapasowe nośniki z tajnym hasłem.

Pytanie: Czy do jednej karty Mifare 1K można zapisać dwa tajne hasła z dwóch osobnych zestawów Karty Obiektu?

Odpowiedź: Nie, to niemożliwe. Klucz dostępu można zapisać za pomocą tajnego hasła tylko raz w danym kluczu.

Pytanie: Czy do jednego czytnika można zapisać więcej tajnych haseł przy użyciu różnych Kart Obiektu?

Odpowiedź: Tak, można. Aby to zrobić, musisz mieć kolejną Kartę Obiektu, z której tajne hasło zostało zapisane w czytniku naściennym. Ponadto nowa wersja oprogramowania układowego czytnika pozwala zapisać do 10 sztuk różnych Kart Obiektu w jednym czytniku. Zapewni to dodatkową funkcjonalność w celu zabezpieczenia dużych obiektów z różnymi prawami dostępu dla użytkowników.