

# Karty bezkontaktowe 125 kHz

MARTYNA REINKE

# Plan prezentacji

- ▶ Czym jest karta bezkontaktowa.
- ▶ Standardy kart bezkontaktowych.
- ▶ Zastosowania kart 125 kHz.
- ▶ Możliwości kart.
- ▶ Bezpieczeństwo/kopiowanie.
- ▶ Koszt zakupu.
- ▶ Zalety i wady.

# Czym jest karta bezkontaktowa?

- ▶ Nośnik informacji graficznych oraz danych zapamiętanych w zintegrowanym chipie.
- ▶ Podstawowa cecha: unikalny numer seryjny używany do identyfikacji użytkownika.
- ▶ Odczyt oraz zapis danych wykonywany za pośrednictwem transmisji fal elektromagnetycznych.
- ▶ bezkontaktowa komunikacja dzięki drodze radiowej, z odległości zależnej od mocy czytnika oraz pasma pracy RFID.

# Czym jest technologia RFID?

- ▶ Wykorzystuje fale radiowe do identyfikacji osób i przedmiotów na odległość.
- ▶ Pozwala zaoszczędzić czas i pieniądze.
- ▶ Do przedmiotów przyczepione są specjalne urządzenia: tagi/chipy/znaczniki, zawierające układy elektroniczne z zakodowanymi danymi i antenę odbiorczo-nadawczą.
- ▶ Zapis i odczyt danych odbywa się z pomocą fal radiowych przy użyciu czytnika RFID wraz z anten.



# Standardy RFID

Podział w zależności od częstotliwości działania znaczników i czytnika. Istnieją trzy standardy RFID działające w niskiej, wysokiej lub ultra wysokiej częstotliwości:

- ▶ LF (125kHz) – pasmo niskich częstotliwości (ang. low frequency) zakres: 30 - 300 kHz,
- ▶ HF (13,56MHz) – pasmo wysokich częstotliwości (ang. High frequency) zakres: 3-30 MHz,
- ▶ UHF (860-956 MHz) – pasmo ultra wysokich częstotliwości (ang. Ultra high frequency) zakres: 300 - 3000 MHz.

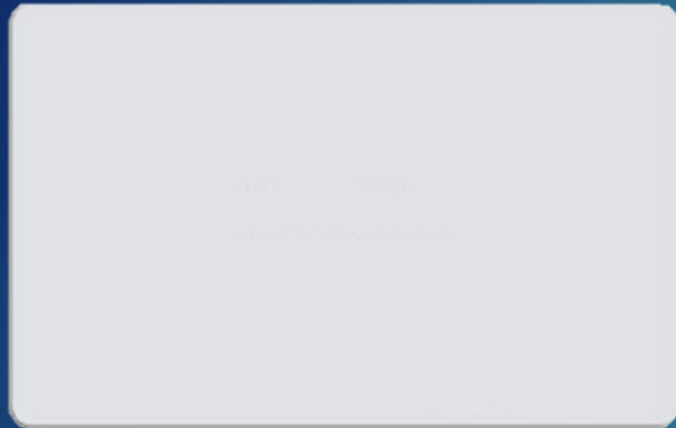
# Standardy kart – częstotliwość 125 kHz

- ▶ Budowa kart zbliżeniowych regulowana jest przez rodzinę standardów :
  - ▶ ISO 14223,
  - ▶ ISO/IEC 18000-2.
- ▶ LF wykorzystywany jest przez dwa standardy RFID używające znaczników pasywnych o małym zasięgu:
  - ▶ Unique,
  - ▶ Hitag.

# Standard Unique

- ▶ Rodzaj karty pasywnej małego zasięgu z możliwością tylko odczytu.
- ▶ Pamięć całkowita: 64 bity (tylko do odczytu).
- ▶ Dane przesyłane są z szybkością 2 kb/s.
- ▶ Unikalny 64 bitowy unikalny numer identyfikacyjny.
- ▶ Karta prosta w obsłudze, trwalsza od innych typów kart (magnetycznych lub chipowych) dzięki komunikacji bezprzewodowej.
- ▶ Przeciętny czas eksploatacji: kilka lat.
- ▶ Współpracuje z czytnikami w odległości od 1 do 10cm.

# Przykłady postaci identyfikatorów Unique



- ▶ Karta zbliżeniowa ISO Unique 125kHz



- ▶ Karta zbliżeniowa Clamshell 125 kHz



- ▶ Tagi zbliżeniowe 125kHz



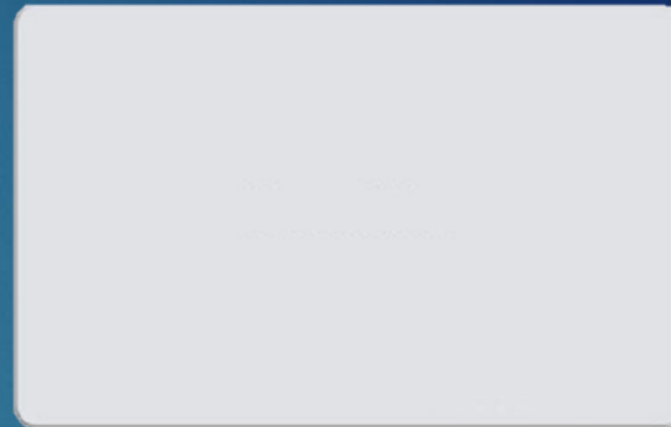
# Standard Hitag

- ▶ Rodzaj karty pasywnej małego zasięgu.
- ▶ Standard bardziej zaawansowany od standardu Unique.
- ▶ Dane przesyłane są z szybkością 4 kb/s.
- ▶ Pozwala na odczyt i zapis, a także zdalne kodowanie.
- ▶ Rozmiar pamięci od 64 bitów do 2048 bitów.
- ▶ Możliwość ochrony hasłem.
- ▶ Łatwa integracja systemów.
- ▶ Wyposażone w systemy antykolizyjne (odczyt wielu kart jednocześnie).

# Przykłady postaci identyfikatorów Hitag



- ▶ HID Tear Shape Hitag1



- ▶ ISO Card Hitag 1



- ▶ RFID Wristband Silicone Tag

# Zastosowania kart 125 kHz

Przykładowe zastosowania:

- ▶ system znakowania i śledzenia zwierząt,
- ▶ system kontroli dostępu,
- ▶ system parkingowych,
- ▶ system opłat drogowych,
- ▶ rejestracja czasu pracy,
- ▶ karty rabatowe,
- ▶ karnety na basen/siłownię
- ▶ karty lojalnościowe (stałego klienta),
- ▶ znakowanie towarów,
- ▶ SKI-pass'y.

# Możliwości kart 125 kHz:

- ▶ prędkość odczytu jest wolniejsza niż w częstotliwościach HF i UHF, ale nie jest podatna na zakłócenia fal radiowych,
- ▶ możliwość odczytu (Unique oraz Hitag) oraz zapisu danych (Hitag),
- ▶ zależnie od typu wykorzystanego układu scalonego, karta ID spełnia dodatkowe funkcje nośnika do wymiany i aktualizacji danych,
- ▶ najczęściej wykorzystywane wewnątrz budynków, jednak sprawdzają się również w zastosowaniach zewnętrznych, o ile nie są narażone na warunki arktyczne,
- ▶ odporne na niesprzyjające czynniki zewnętrzne i mogą być stosowane nawet przy wysokich temperaturach,
- ▶ zdalna identyfikacja niewymagająca dotyku – wszystko odbywa się na odległość,
- ▶ błyskawiczny odczyt z szybkością ponad 100 tagów na 1 sekundę,
- ▶ zasięg do kilkunastu cm.

# Możliwości w porównaniu do kodów kreskowych:

- ▶ identyfikacja wielu elementów jednocześnie,
- ▶ znaczniki RFID są dokładniejsze, lepiej i szybciej odczytywane od kodów kreskowych,
- ▶ znaczniki RFID przechowują więcej informacji niż kody kreskowe,
- ▶ czytniki RFID mogą zarówno odczytywać, jak i zapisywać dane,
- ▶ przytwierdzone do narzędzi i urządzeń, jak formy odlewnicze, matryce, uchwyty, elektronarzędzia i nie ulegają zatarciu czy zniszczeniu,
- ▶ etykiety RFID są w praktyce trwalsze od kodu kreskowego.

# Bezpieczeństwo/kopiowanie

- ▶ Systemy RFID narażone są na różnego rodzaju ataki, których celem może być
  - ▶ uzyskanie nieautoryzowanego dostępu do informacji zapisanych w znacznikach,
  - ▶ wprowadzenie w błąd operatorów lub użytkowników systemu przez wprowadzenie do niego fałszywych danych,
  - ▶ uniemożliwienie spełniania funkcji przez identyfikator.

W drugim i trzecim przypadku numer identyfikacyjny pozostaje niezmienny, przez co czytnik rozpoznaje go prawidłowo i przesłane przez niego informacje traktuje jako wiarygodne.

# Bezpieczeństwo/kopiowanie

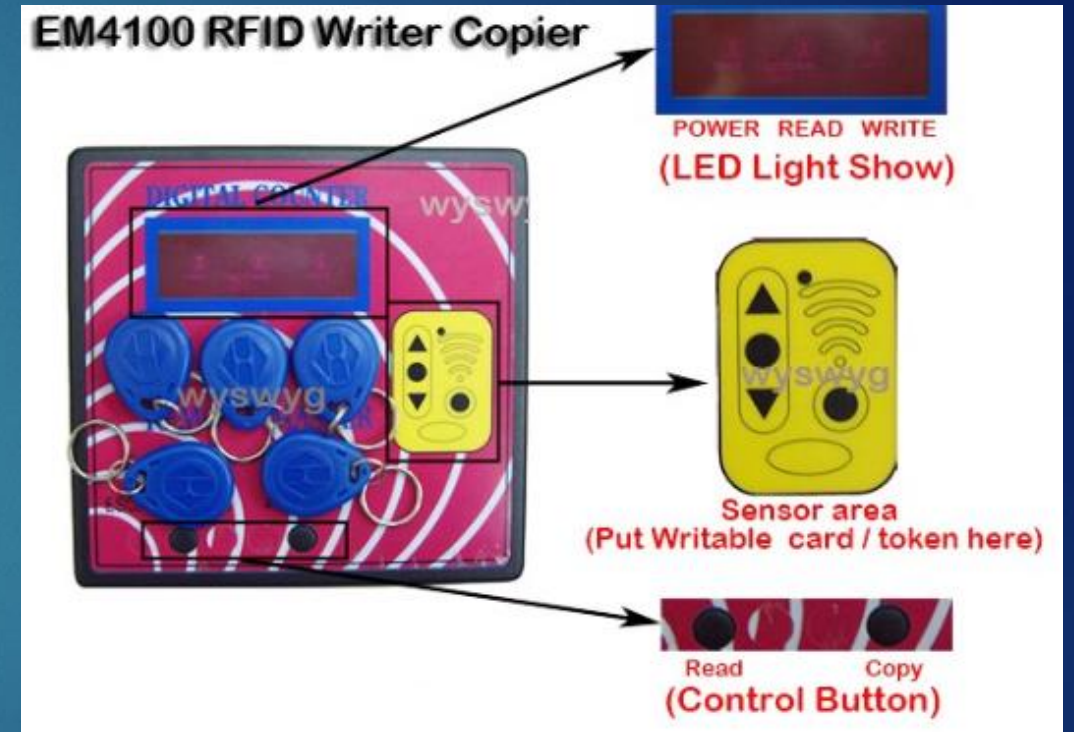
- ▶ Innym rozwiązaniem jest odczyt numeru ID tagu, a następnie użycie go do podszycia się pod ten znacznik z wykorzystaniem urządzenia potrafiącego symulować jego działanie.
- ▶ Dostęp do danych mogą również próbować uzyskać czytniki spoza systemu.
- ▶ Atakujący może wydać komendę znaczniki.
- ▶ Inne sposoby to: podsłuchanie lub zakłócanie transmisji między znacznikiem a czytnikiem.

# Bezpieczeństwo/kopiowanie

Do skopiowania karty tak na prawdę potrzebne są dwie rzeczy:

- ▶ czysta karta,
- ▶ czytnik z możliwością programowania.

W celu skopiowania karty, należy położyć ją na żółtym sensorze. Następnie należy wcisnąć przycisk „Read”. W tym momencie następuje odczytanie numeru karty oraz zapisanie jej w pamięci czytnika. Następnym krokiem jest umieszczenie czystej karty w obrębie sensora. Naciskając przycisk „Copy” przesyłamy wcześniej zapisane dane karty do nowego taga. Jest to jeden z najprostszyc sposobów na kopiowanie kart UNIQUE.



- ▶ Czytnik z możliwością kopiowania kart koszt ok 50 dolarów



# Bezpieczeństwo/kopiowanie

- ▶ Aby zapobiec atakom/kopiowaniu, konieczne jest wzajemne uwierzytelnienie znacznika i czytnika. Ten drugi rozpoznaje pierwszy na podstawie jego numeru ID.
- ▶ Czytnik może przesyłać pewną, losowo wybraną liczbę, którą znacznik, korzystając z takiego samego klucza szyfrującego, co nadawca, musi odesłać zakodowaną.
- ▶ Najpopularniejszą metodą jest zabezpieczenie dostępu do tagu hasłem.
- ▶ Najpowszechniejszą metodą zabezpieczenia przed podsłuchaniem transmisji jest szyfrowanie informacji. Najskuteczniejszym sposobem na uniknięcie tego jest jednak po prostu niezapisywanie w znaczniku żadnych ważnych informacji oprócz jego numeru identyfikującego.

# Koszty zakupu identyfikatora:

- ▶ karta zbliżeniowa ISO Unique 125kHz 1-2 zł,
- ▶ tagi zbliżeniowe 125kHz 1-4 zł,
- ▶ transponder zbliżeniowy Unique 125KHz 6-9 zł,
- ▶ ISO Card Hitag 1 9-10 zł,
- ▶ HID Tear Shape Hitag1 9-10 zł,
- ▶ RFID Wristband Silicone Tag 18-20 zł,

# Koszty zakupu czytnika



- ▶ Czytnik kart Unique – USB  
30 - 70 zł



- ▶ Netronix PAC-Dux  
155 - 190 zł

# Zalety

- ▶ System prosty w obsłudze oraz skuteczny.
- ▶ Karty i breloki mają obudowy zabezpieczające ochronę wewnętrznych układów elektronicznych przed cieczami i uszkodzeniami mechanicznymi.
- ▶ Przewaga technologii RFID nad systemami kodów kreskowych – kontakt wizyjny karty i czytnika nie jest wymagany, dzięki czemu nie zawsze jest konieczność wyjmowania identyfikatora z plecaka/torebki.
- ▶ Do dyspozycji programowalne tagi.
- ▶ Wybrane czytniki zbliżeniowe umożliwiają przetwarzanie danych, np. obliczenie czasu spędzonego przez pracownika w miejscu pracy.

# Wady

- ▶ Ze względu na liczbę wyprodukowanych na świecie kart, możliwe jest dublowanie się indywidualnych numerów kart.
- ▶ Brak zabezpieczenia/szyfrowania danych zapisanych w pamięci tagów, co umożliwia osobom postronnym nieautoryzowane skopiowanie karty.
- ▶ W przypadku zbliżenia dwóch kart Unique do czytnika żadna z nich nie zostanie odczytana, (wzajemne zakłócanie), w przypadku standardu HITAG (z systemem antykolizyjnym) odczyt danych z kilku kart jednocześnie).

# Bibliografia

- ▶ <https://www.rfidpolska.pl/technologie-rfid-co-to-jest/>
- ▶ <http://www.mcp.poznan.pl/wp-content/uploads/2018/01/Karty-dalekiego-zasiegu.pdf>
- ▶ <https://www.rfidpolska.pl/standardy-rfid/>
- ▶ <http://www.cs.pl/produkty/karty-zblizeniowe-125khz/>
- ▶ <https://automatykab2b.pl/temat-miesiaca/49858-rfid-i-znakowanie-czesc-1-kompendium-rfid/strona/5>
- ▶ <http://rfid-lab.pl/opis-standardu-hitag>
- ▶ <https://www.zabezpieczenia.com.pl/kontrola-dost%C4%99pu/wszystko-na-jednej-karcie>
- ▶ <https://www.rfidpolska.pl/technologie-rfid-co-to-jest/>
- ▶ [https://sklep.delta.poznan.pl/unique-125khz-standard-technologiei-rfid\\_11\\_aid901.html](https://sklep.delta.poznan.pl/unique-125khz-standard-technologiei-rfid_11_aid901.html)
- ▶ <https://allegro.pl/>
- ▶ <https://www.tme.eu/>
- ▶ <http://rfid-lab.pl/standard-unique-%E2%80%93-om%C3%B3wienie-i-zastosowania>

Dziękuję za uwagę!