Opis protokołu komunikacyjnego z czytnikiem administracyjnym Mifare

www.infratronik.com

Rewizja 01, 2005-09-01

Lista dostępnych rozkazów w wersji v1.02

Objaśnienie

Wszystkie symbole występujące w opisie :A1..,B1..D1.. oznaczają dane w postaci dwubajtowych ciągów znaków liczb hexadecymalnych
liczby 0xA1 należy wysyłać w postaci A1 jak również należy pomijać przy transmisji znak space

przykładowo zapis : **$ 0x14 B1 B2 *** gdzie B1=0xA1 B2=00 reprezentowany będzie następująco w postaci stringu: ' **$14A100*** '

Odczyt wersji oprogramowania:

Rozkaz ten służy do odczytania dwubajtowego numeru wersji oprogramowania czytnika

Rozkaz wysyłany do czytnika $ 0x14 *
Dane odebrane z czytnika $ 0x14 B1 B2 * <- PICC

gdzie: B1 i B2 numer wersji

Odczyt statusu czytnika

Rozkaz wysyłany do czytnika $ 0x01 *
Dane odebrane z czytnika $ 0x01 B1 B2 B3 B4 *

gdzie:

B1 stat_mifare - status transmisji
B2 statusPcd - status czytnika
B3 sak-bajt odesłany przez kartę po dokonaniu selekcji

Odczyt numeru seryjnego czytnika.

Każdy czytnik posiada unikalny numer seryjny którego nie można zmienić
Rozkaz wysyłany do czytnika $ 0x02 *
Dane odebrane z czytnika $ 0x02 B1 B2 B3 B4 *

gdzie:
B1,B2,B3,B4 czterobajtowy numer seryjny

Odczyt typu karty

Rozkaz wysyłany do czytnika $ 0x04 *
Dane odebrane z czytnika
$ 0x04 B1 B2 * lub Status w przypadku braku karty

gdzie:
B1,B2 typ karty 0400-mifare 1k
4400-mifareultralight
1000 mifarlight

Odczyt UID karty

Cztynik zwraca 4 bajty identyfikatora + crc karty lub status w przypadku niepowodzenia

Rozkaz wysyłany do czytnika $ 0x03 *
Dane odebrane z czytnika :
$ 0x03 B1 B2 B3 B4 B5 * lub Status w przypadku braku karty

gdzie:
B1,B2,B3,B4 - kod karty
B5 - suma kontrolna batów B1..B4 (B1 xor B2 xor B3 xor B4 = B5)

Odczyt bloku karty

Czytnik zwraca odczytany blok karty
Rozkaz wysyłany do czytnika $ 0x05 A1 *
Dane odebrane z czytnika $ 0x05 B1 B2 B3 D1..D16 * lub
$ 0x05 B1 B2 B3 B4 * w przypadku nie odczytania bloku
gdzie:
a1 – numer blok

B1- numer bloku który był ostatnio poddawany autentykacji
B2- numer bloku odczytywanego
B3- ilość odebranych bajtów
B4- błąd odesłany przez kartę w przypadku niepowodzenia
D1..D16 - dane z odczytywanego bloku

Zapis bloku karty 16 bajtów

Cztynik zapisuje do bloku pamięci przesłane dane
Warunkiem powodzenia jest wcześniejsza autentykacja sektora w którym znajduje się blok

Rozkaz wysyłany do czytnika $ 0x06 A1 D1..D16 *
Dane odebrane z czytnika Status

A1 numer bloku – jest to adres bezwzględny (00..3F) numeru bloku w pamięci karty
D1..D16 - dane do zapisu

Zapis bloku karty 4 bajty - przeznaczony dla kart ultralight

Czytnik zapisuje do bloku pamięci przesłane dane

Rozkaz wysyłany do czytnika $ 0x07 A1 D1..D4 *
Dane odebrane z czytnika Status

A1 numer bloku - jest to adres bezwzględny numeru bloku w pamięci karty
D1..D4 - dane do zapisu

Autentykacja

Przed wykonaniem autentykacji należy dokonać selekcji karty

Rozkaz wysyłany do czytnika $ 0x0A A1 A2 *
Dane odebrane z czytnika Status

A1- numer dowolnego bloku w sektorze poddawanego autentykacji numer ten jest adresem bezwzględnym liczonym począwszy od zerowego bloku karty

A2- A2.0=0 Klucz A
A2.0=1 Klucz B

A2.1=0 Klucz pochodzi z pamięci EEprom
A2.1=1 Klucz pochodzi z pamięci ram (musi być uprzednio załadowany)

Uaktywnienie karty

Po wykonaniu tej instrukcji możliwe stają się dalsze operacje na danej karcie (w przypadku kart Mifare 1K i Mifare 4K w pierwszej kolejności autentykacja)
W celu aktywacji karty konieczne jest wcześniejsze poznanie UID karty

Rozkaz wysyłany do czytnika $ 0x13 *
Dane odebrane z czytnika Status

Zapis nowego klucza do pamięci RAM czytnika

Uwaga -rozkaz ten nie określa rodzaju klucz A / B gdyż informacja ta przekazywana jest na poziomie rozkazu autentykacji

Rozkaz wysyłany do czytnika $ 0x0C A1 A2 A3 A4 A5 A6 *
Dane odebrane z czytnika Status

A1..A6- nowy klucz

Ustawienie trybu pracy czytnika

Rozkaz wysyłany do czytnika $ 0x12 A1 *
Dane odebrane z czytnika Status

A1.0=0 Automatyczne odpytywanie włączone

A1.0=1 Automatyczne odpytywanie wyłączone

A1.1=0 Led 2 zgaszony
A1.1=1 Led 2 zapalony

Po podłączeniu zasilania bity A1.0 i A1.1 są ustawione na 0

Podczas włączonego automatycznego odpytywania czytnik odczytuje typ karty , numer seryjny i sektor 0 karty za pomoczą hasła zawartego w RAM i autentykacji kluczem B po pierwszym odczycie sprawdza czy karta jest przyłożona do czytnika i odczytuje już tylko typ karty.

Przykłady:

Odczyt sektora 0 karty MIfare1K

Aby odczytać sektor należ wysłać do czytnika następujące rozkazy, należy pamiętać aby zachować odstępy czasowe pomiędzy kolejnymi rozkazami – co najmniej 150 ms lub odczytać odpowiedź zwrotną od czytnika.

1. $1201* - wyłączenie autoodpytywania (operacja jednorazowa) rozkaz jest zapamiętywany do chwili zaniku zasilania.
2. $0C A1..A6 * Zapis klucza do czytnika (A1..A6 klucz) – jest to operacja wykonywana jednorazowo – jeśli pozostałe sektory posiadają te same klucze wówczas nie trzeba ponownie zapisywać klucza do pamięci RAM. Po odłączeniu zasilania klucz jest tracony. Standardowy klucz dla sektora 0 będącego zgodnym ze standardem MAD jest następujący ‘A0A1A2A3A4A5’.

3. $04* - odczyt typu karty
4. $03* - odczyt UID karty
5. $13* - selekcja karty
6. $0A0002 *- autenyukacja karty
7. $0500* -odczyt 16 bajtów bloku 0 sektora 0
8. $0501* -odczyt 16 bajtów bloku 1 sektora 0
9. $0502* -odczyt 16 bajtów bloku 2 sektora 0
10. $0503* -odczyt 16 bajtów bloku 3 sektora 0

Odczyt sektora 2 karty MIfare1K kluczem A ‘010203040506’

1. $1201* - wyłączenie autoodpytywania
2. $0C010203040506* - zapis klucza do RAM
3. $04* - odczyt typu karty
4. $03* - odczyt UID karty
5. $13* - selekcja karty
6. $0A0802 * - autenyukacja karty
7. $0508* - odczyt 16 bajtów bloku 0 sektora 2
8. $0509* - odczyt 16 bajtów bloku 1 sektora 2
9. $050A* - odczyt 16 bajtów bloku 2 sektora 2
10. $050B* - odczyt 16 bajtów bloku 3 sektora 2

Zapis bloku 0 sektora 1 kluczem A ‘010203040506’ karty MIfare1K

11. $1201* - wyłączenie autoodpytywania
12. $0C010203040506* - zapis klucza do RAM
13. $04* - odczyt typu karty
14. $03* - odczyt UID karty
15. $13* - selekcja karty
16. $0A0402 * - autenyukacja karty
17. $06040011223344556677889 9AABBCCDDEEFF * zapis bloku 0 sektora 1
18. $0504* - odczyt 16 bajtów bloku 0 sektora 1 (dla sprawdzenia poprawności zapisu)