ELEKTRONICZNE KARTY IDENTYFIKACYJNE
Laboratorium 1
Komunikacja z układem zbliżeniowym MIFARE®Standard (1kB)

Uwaga: W roli programu narzędziowego do komunikacji z układem ***MIFARE®Standard*** wykorzystać program:
./omnikey/samples/contactlessdemovc/release/ContactlessDemoVC.exe.

Wybór opcji programu:
Connected Reader: OMNIKEY CardMan 5x21 -CL 0
Transmission Option: Secured

Sekwencja operacji: ***Request, Anticollision, Select*** jest wykonywana przez program automatycznie po umieszczeniu karty w polu oddziaływania czytnika.
Dalsza komunikacja z układem wymaga wyboru sektora (wybór pośredni przez wskazanie bezwzględnego numeru bloku od ***0*** do ***63***, tzn. wskazanie bloku o numerze od ***0*** do ***3*** równoznaczne jest z rozpooczęciem komunikacji z sektorem ***0***, itd.).
Po każdej zmianie sektora należy przeprowadzić najpierw pomyślnie wzajemne uwierzytelnianie. W trakcie ćwiczenia wykorzystywać ***wyłącznie*** uwierzytelnianie za pomocą ***klucza A*** (***opcje programu:*** ***Authentication Mode: Mode A; Access Option: 6-byte key***).

Ważne: Nie modyfikować za pomocą operacji WRITE bloku z kluczami i bitami kontroli dostępu, nawet, gdy aktualna konfiguracja sektora na to pozwala !!!
Nie modyfikować zawartosci bloków o numerach 3, 7, 11, 15, 19, 23, 27, itd.. !!!

Dokumentacja:
Mifare_1KB_Func_Spec.pdf - specyfikacja układu MF1 IC S50
M001830.pdf - specyfikacja konwencji MAD (MIFARE Application Directory)
mad_overview.pdf – lista przyznanych identyfikatorów MAD (z 1.12.2007)

Uwaga:
W trakcie realizacji kolejnych punktów scenariusza sporządzać na bieżąco sprawozdanie z wykonywanych działań, min. rejestrując polecenia wysyłane przez czytnik do karty oraz zawartość odczytywanych bloków pamięci nieulotnej.

1. **Komunikacja z Elektroniczną Legitymacją Studencką.** Odczytać zawartość sektora numer ***0*** swojej elektronicznej legitymacji studenckiej (***klucz uwierzytalniajacy A = 'A0A1A2A3A4A5' hex***).

   - Zinterpretować zawartość bloku ***0***;
   - Zinterpretować zawartość bloków ***1*** i ***2***; struktura danych w tych blokach zgodna jest ze specyfikacją ***MAD1***; odczytać i zinterpretować zawartość bajta ***Info-byte***; oraz pozostałych bajtów w blokach ***1*** i ***2***; korzystając z informacji o sektorze zarządzanym przez wydawcę karty (***Card Publisher Sector - CPS***) znaleźć na liście przyznanych identyfikatorów informację o tym wydawcy;
   - Zinterpretować zawartość bloku ***3*** (w następującej kolejności: bajt ogólnego przeznaczenia – ***General Purpose Byte*** – ***GPB*** - o specyfikacji zgodnej z ***MAD1***, bity warunków dostępu, klucze uwierzytelniające ***A*** i ***B***).

2. **Odczyt i interpretacja konfiguracji „dziewiczego" układu Mifare®Standard.** Odczytać zawartość sektora numer ***1*** „dziewiczego" układu dostarczonego przez prowadzącego zajęcia (***klucze uwierzytalniajace A i B = 'FFFFFFFFFFFF' hex***).

   - Zinterpretować zawartość bloku ***3*** (w następującej kolejności: bajt ogólnego przeznaczenia – ***General Purpose Byte*** – ***GPB*** - o specyfikacji zgodnej z ***MAD1***, bity warunków dostępu, klucze uwierzytelniające ***A*** i ***B***). Uwaga: bloki danych o numerach ***4***, ***5*** i ***6*** powinny być wypełnione bajtami o wartości ***0x00***.

3. **Odczyt (*READ*) i zapis (*WRITE*) danych w blokach o numerach *4, 5* i *6* sektora o numerze 1.** Sprawdzić działanie operacji odczytu i zapisu danych we wskazanych blokach sektora. Po dokonaniu zapisu usunąć kartę z pola oddziaływania czytnika, a następnie ponownie uwierzytelnić sie kluczem ***A*** i dokonać odczytu zmodyfikowanych bloków. Na zakończenie tej części ćwiczenia wypełnić zmodyfikowane bloki danych (***4***, ***5*** i ***6***) bajtami o wartości ***0x00.***

4. **Inicjacja bloku o numerze *4* sektora o numerze 1 jako „elektronicznej portmonetki" (*Value block*) i sprawdzenie działania operacji „uzupełniania" (*INCREMENT*) i „wydawania" (*DECREMENT*) „walorów finansowych" .** Zainicjować (zgodnie ze specyfikacją układu scalonego) blok o numerze ***4*** do działania w trybie i formacie „elektronicznej portmonetki" (***wskazówka:*** ***jako wartość „adresu" do kontroli integralności operacji wybrać adres 0x10***). W celu inicjacji wydać polecenie zapisu (***WRITE***). Zaobserwować działanie operacji ***INCREMENT*** i ***DECREMENT*** (po wywołaniu każdej z nich dokonać odczytu zawartości bloku za pomocą operacji ***READ***). Na zakończenie tej części ćwiczenia wypełnić zmodyfikowany blok danych (***4***) bajtami o wartości ***0x00.***