DESFire

Autor: Jacek Ziętek

Plan prezentacji

1. Wprowadzenie.
2. Organizacja aplikacji.
3. Klucze domyślne.
4. Polecenia i odpowiedzi.
5. Secure communication.
6. Różnice między Mifare Classic a Mifare DESFIRE.
7. Zgodność z Mifare Classic.

Wprowadzenie

Desfire:

- rodzina kart inteligentnych,
- opracowana przez NXP Semiconductors,
- obsługa wielu aplikacji na jednej karcie,
- bezpieczne przechowywanie i przetwarzanie danych,
- systemy kontroli dostępu, płatności bezstykowych itd,
- powszechne stosowanie.

DESFire EV1:

- podstawowe mechanizmy bezpieczeństwa,
- ograniczona pojemność pamięci,
- wsparcie dla wielu aplikacji.

DESFire EV2:

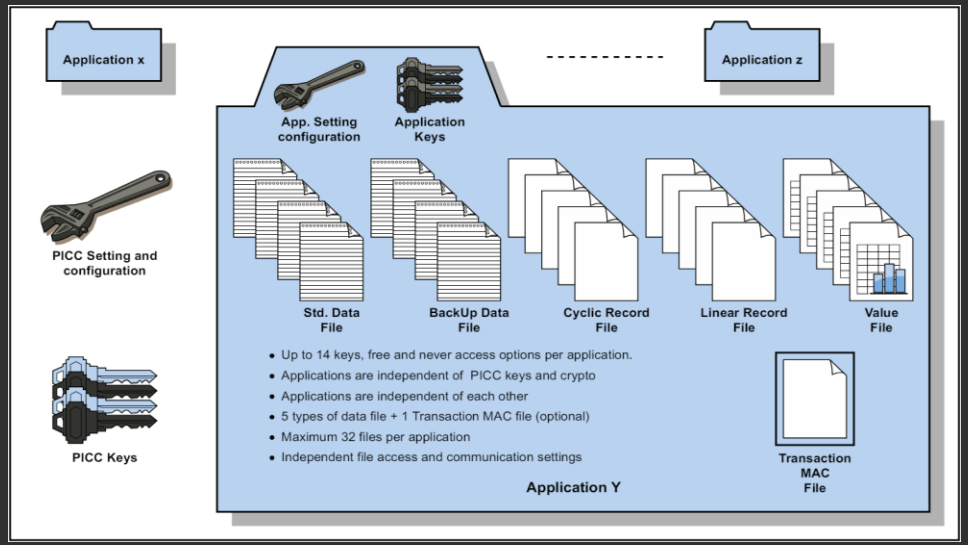
- dynamiczna zmiana klucza,
- więcej kluczy dla każdej aplikacji,
- zwiększona pojemność pamięci.

DESFire EV3:

- ulepszone algorytmy szyfrowania,
- poprawiona obsługa transmisji danych,
- wyższy poziom bezpieczeństwa i wydajności.

Organizacja aplikacji

- aplikacje niezależne od siebie nawzajem (X i Z - brak dostępu do plików Y),
- aplikacja to kontener plików (5 typów plików do składowania danych i 1 typ do MAC transakcji),
- rodzaje plików:
  - Std. Data File - standardowe dane,
  - BackUp Data File - dane przywracane w miarę potrzeby,
  - Cyclic Record File - cykliczne dane (np logi),
  - Linear Record File - liniowe dane,
  - Value File - wartości zwiększane\zmniejszane (np e-portfel),
  - Transaction MAC File - zabezpieczanie transakcji poprzez kody MAC,
- poziom PICC,
- poziom aplikacji.



Poziom PICC

- zarządzanie całą kartą,
- PICC Keys - klucze umożliwiające przeprowadzanie takich operacji jak:
  - tworzenie nowych aplikacji,
  - usuwanie istniejących aplikacji,
  - modyfikowanie struktury aplikacji,
  - zmiana ustawień globalnych (między innymi ustawień bezpieczeństwa).

- posiadanie klucza PICC nie jest równoznaczne z możliwością odczytywania plików aplikacji.

Poziom aplikacji

- Application Keys:
  - każda aplikacja do 14 kluczy,
  - kontrola dostępu do plików i funkcji wewnątrz aplikacji,
  - niezależne od kluczy PICC.

- App. Setting Configuration:
  - zarządzanie dostępem w ramach aplikacji,
  - konfiguracja plików w ramach aplikacji.

Klucze domyślne

- Klucz główny (Master Key): pozwala na zarządzanie kartą jako całością:
  - daje pełne uprawnienia,
  - umożliwia podział możliwych operacji na poszczególnych użytkowników,
  - umożliwia zarządzanie wieloma aplikacjami,
  - regularna zmiana klucza w celach bezpieczeństwa,

- Klucze aplikacji: każda aplikacja może korzystać z różnych kluczy kryptograficznych (do 14).

Polecenia i odpowiedzi

Komendy:

a) uwierzytelniania (potwierdzanie tożsamości),
b) zarządzania pamięcią i konfiguracji (kontrolowanie alokacji, ustawień i zarządzanie pamięcią),
c) zarządzania kluczami (zarządzanie i manipulacja kluczami),
d) zarządzania aplikacjami,
e) zarządzania plikami,
f) zarządzania danymi,
g) zarządzania transakcjami,

Przykładowe komendy i odpowiedzi błędu:

a) Authenticate - 0x1A (Błąd klucza),
b) FreeMem - 0x0E (Błąd wewnętrzny),
c) ChangeKey - 0x9D (Brak uprawnień),
d) GetApplicationIDs - 0x1F (Bład odczytu danych),
e) DeleteFile - 0x9D (Brak uprawnień),
f) WriteData - 0x1F (Błąd odczytu danych),
g) CommitTransaction - 0x10 (Bład zakończenia transakcji)

Polecenia i odpowiedzi

Komendy:

h) standardu ISO\IEC 7816-4 (interakcje zgodnie z wymienionym protokołem),
i) kart wirtualnych (manipulacja danymi poprzez symulację operacji kart wirtualnych),
j) kontroli zbliżeniowej (operacje związane z pomiarowaniem odległości w celu kontroli zbliżeniowej),
k) kontroli oryginalności (sprawdzenie autentyczności danych lub urządzeń).

Przykładowe komendy i odpowiedzi błędu:

h) ISOReadRecord - 0x0E (Błąd wewnętrzny),
i) ISOSelect - 0x1F (Błąd wyboru pliku ISO),
j) ProximityCheck - 0x10 (Błąd przygotowania do kontroli zbliżeniowej),
k) Read_Sig - 0x1F (Błąd odczytu sygnatury).

Secure communication

Typy bezpiecznej komunikacji:

a) zwykły transfer danych - możliwy tylko w trybie kompatybilności wstecznej z MF3ICD40 i EV2 secure messaging,
b) zwykły transfer danych z kryptograficzną sumą kontrolną MAC - zabezpieczenie danych poprzez dołączenie sumy kontrolnej,
c) szyfrowany transfer danych (zabezpieczony przez CRC przed szyfrowaniem) - zabezpieczenie danych poprzez dołączenie sumy kontrolnej i szyfrowanie.

Różnice między Mifare Classic a Mifare DESFIRE.

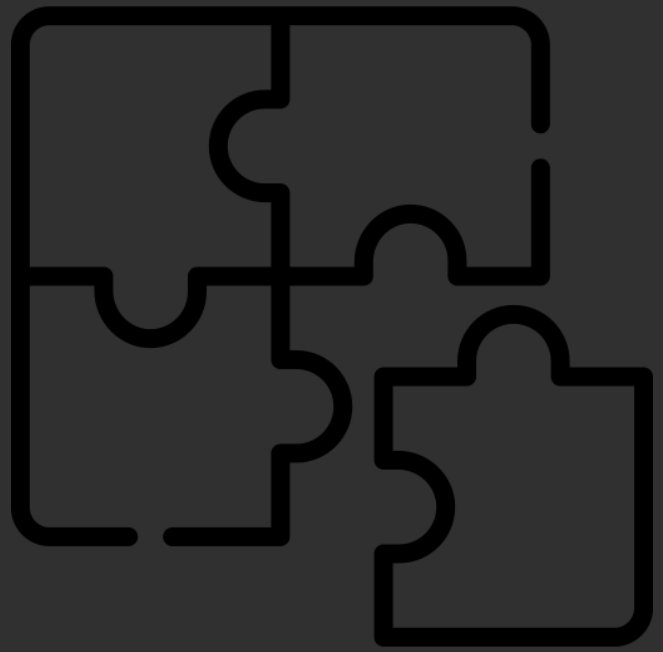
Najważniejsze różnice Mifare Classic względem Mifare DESFire:

- mniejszy poziom bezpieczeństwa (starsze algorytmy kryptograficzne,
- brak zaawansowanych mechanizmów zabezpieczeń),
- mniejsza pamięć,
- węższy zakres funkcji i możliwości,
- tylko jednokierunkowa komunikacji,
- mniejsza kompatybilność wsteczna.

Zgodność z Mifare Classic (pełne)

Pełna zgodność:

- Emulacja na DESFire EV3:
  - utworzenie aplikacji z identyfikatorem Mifare Classic,
  - odwzorowanie sektorów Mifare Classic na plik w DESFire.
- Zestaw kluczy i autoryzacja:
  - konfiguracja DESFire EV3 z kluczami Mifare Classic,
  - użycie tych samych kluczy w emulowanych sektorach,
  - wybranie jednolitego trybu szyfrowania: DES, 3DES lub AES.
- Czytniki:
  - używanie czytników obsługujących oba typy kart,
  - aktualizacja posiadanych czytników, jeśli to możliwe.
- Klonowanie danych:
  - użycie narzędzia lub skryptu do odczytu danych z Mifare Classic i zapisania ich na DESFire.



Dziękuję za uwagę