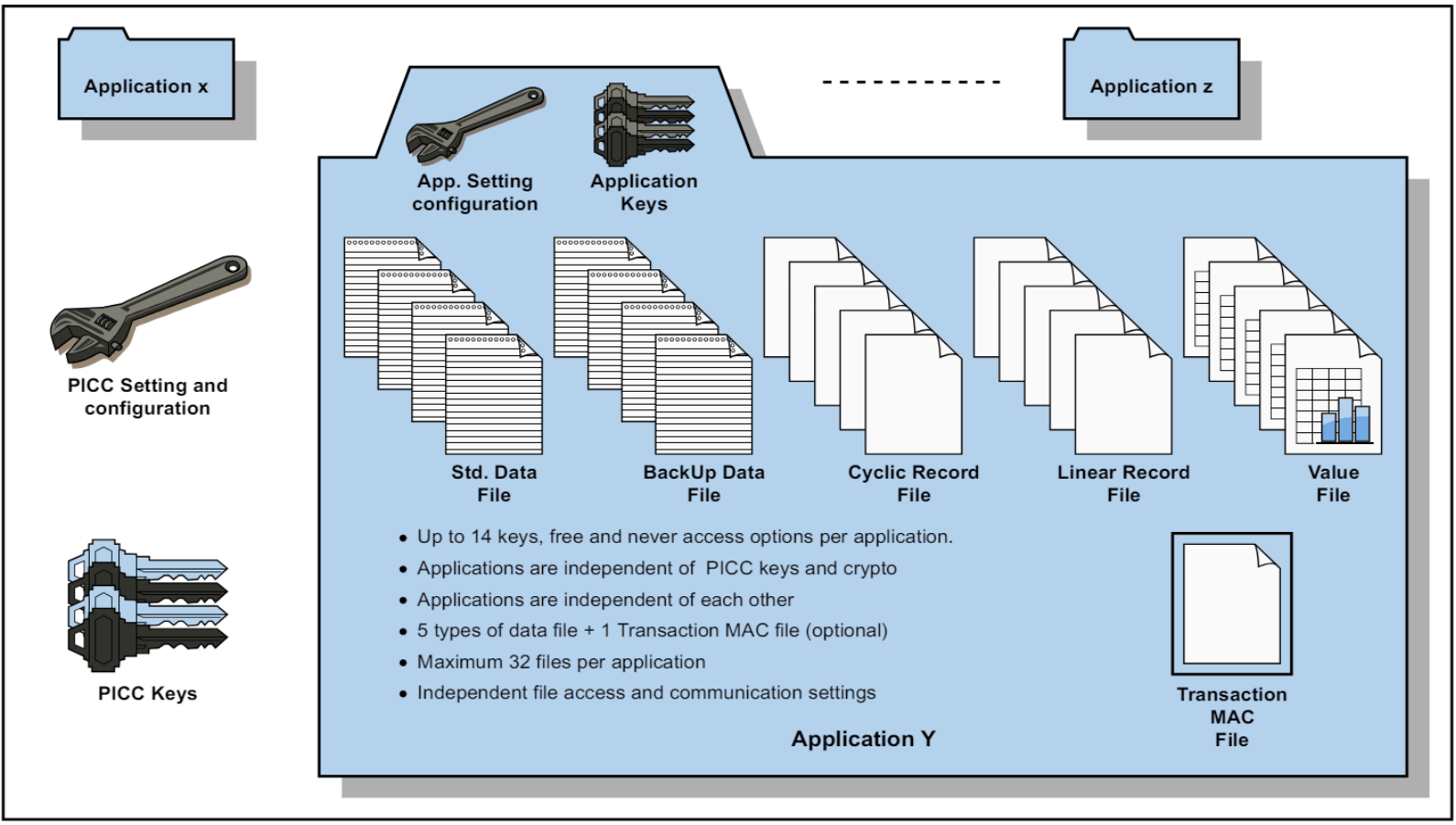
# DESFire

## 1. Organizacja aplikacji

### 1.1 Graficzna organizacja aplikacji




### 1.2 Ogólna struktura

Karta może przechowywać wiele aplikacji, każda jest niezależna od innych - sąsiednie aplikacje nie mają dostępu do plików (Application Z oraz Application X nie mają dostępu do plików Application Y) - organizacja pamięci jest elastyczna i może być dynamicznie konfigurowana w celu spełnienia dowolnych wymagań aplikacji.

Każda aplikacja ma swój folder, który jest kontenerem plików danych, gdzie może znajdować się 5 typów plików do przechowywania danych oraz 1 typ pliku do przechowywania MAC transakcji.
Karty Mifare DESFire EV3 są zgodne między innymi z normami: ISO/IEC 14443-A, ISO/IEC 7816-4.

## 1.3 Poziom PICC (Proximity Integrated Circuit Card)

Na poziomie PICC (zarządzanie całą kartą) właściciel, który ma dostęp do kluczy głównych (PICC Keys), ma możliwość przeprowadzania operacji takich jak

- tworzenie nowych aplikacji,
- usuwanie istniejących aplikacji,
- modyfikowanie struktury aplikacji,
- zmiana ustawień globalnych (między innymi ustawień bezpieczeństwa).

W celu odczytania plików aplikacji właściciel musi być w posiadaniu klucza aplikacji.

## 1.4 Poziom aplikacji

Składa się z:

a) Application Keys: każda aplikacja może mieć do 14 kluczy, które kontrolują dostęp do plików i funkcji wewnątrz aplikacji. Klucze te są niezależne od kluczy na poziomie PICC,

b) App. Setting Configuration: ustawienia konfiguracyjne aplikacji obejmują zarządzanie dostępem i konfiguracją plików w ramach danej aplikacji.

## 1.5 Rodzaje plików w aplikacji

W ramach aplikacji może istnieć do 32 plików, które są zarządzane niezależnie od innych aplikacji na karcie. Pliki te mogą mieć różne typy, w zależności od potrzeb aplikacji:

a) Std. Data File (Standardowy plik danych): przechowuje standardowe dane,

b) BackUp Data File (Plik kopii zapasowej): przechowuje dane, które mogą być przywracane w razie potrzeby,

c) Cyclic Record File (Cykliczny plik rejestru): przechowuje dane w sposób cykliczny, co jest przydatne np. do zapisu logów,

d) Linear Record File (Liniowy plik rejestru): przechowuje dane w sposób liniowy, bez nadpisywania,

e) Value File (Plik wartościowy): przechowuje wartości, które mogą być zwiększane lub zmniejszane, co jest przydatne w aplikacjach takich jak e-portfele.

f) Transaction MAC File (Plik MAC transakcji): opcjonalny plik używany do zabezpieczania transakcji poprzez kody MAC.

### 1.6 Dodatkowe funkcje

a) Każda aplikacja może mieć do 14 kluczy z różnymi poziomami dostępu,

b) Aplikacje są niezależne od kluczy i mechanizmów kryptograficznych na poziomie PICC,

c) Każda aplikacja jest niezależna od innych aplikacji na karcie,

d) Każdy plik w ramach aplikacji ma swoje własne ustawienia dostępu i komunikacji.

## 2. Klucze domyślne

a) Klucz główny (Master Key): pozwala na zarządzanie kartą jako całością:

- klucz główny posiada pełne uprawnienia do zarządzania kartą jako całością. Daje on dostęp do wszystkich danych i funkcji na karcie,
- kluczowy dla ochrony danych przechowywanych na karcie,
- umożliwia podział możliwych operacji na poszczególnych użytkowników,
- należy regularnie zmieniać klucz w celach bezpieczeństwa,
- umożliwia zarządzanie wieloma aplikacjami na jednej karcie.

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

3. Polecenia i odpowiedzi

3.1 Komendy uwierzytelniania - służą do potwierdzania tożsamości i autoryzacji dostępu poprzez weryfikację kluczy uwierzytelniających

- Authenticate
- AuthenticateISO
- AuthenticateAES
- AuthenticateEV2First
- AuthenticateEV2NonFirst

  Przykładowe odpowiedzi dla wymienionych komend:
  - sukces: 0x00
  - błąd:
    - 0x9D (Niepowodzenie z powodu braku uprawnień)
    - 0x0E (Błąd wewnętrzny)
    - 0x1A (Błąd klucza)

3.2 Komendy zarządzania pamięcią i konfiguracji - służą do kontrolowania alokacji, ustawień oraz zarządzania pamięcią

- FreeMem
- Format
- SetConfiguration
- GetVersion
- GetCardUID

  Przykładowe odpowiedzi dla wymienionych komend:
  - sukces: 0x00
  - błąd:
    - 0x6E (Nieobsługiwane polecenie)
    - 0x0E (Błąd wewnętrzny)
    - 0x1F (Błąd odczytu UID)

3.3 Komendy zarządzania kluczami - umożliwiają zarządzanie kluczami uwierzytelniającymi oraz manipulowanie nimi

- ChangeKey
- ChangeKeyEV2
- InitializeKeySet
- FinalizeKeySet
- RollKeySet
- GetKeySettings

- ChangeKeySettings
- GetKeyVersion

  Przykładowe odpowiedzi dla wymienionych komend:
  - sukces: 0x00
  - błąd:
    - 0x9D (Niepowodzenie z powodu braku uprawnień)
    - 0x0E (Błąd wewnętrzny)
    - 0x1F (Błąd odczytu wersji klucza)

### 3.4 Komendy zarządzania aplikacjami - umożliwiają tworzenie, usuwanie, wybieranie i zarządzanie aplikacjami

- CreateApplication
- DeleteApplication
- CreateDelegatedApplication
- SelectApplication
- GetApplicationIDs
- GetDFNames
- GetDelegatedInfo

  Przykładowe odpowiedzi dla wymienionych komend:
  - sukces: 0x00
  - błąd:
    - 0x9D (Niepowodzenie z powodu braku uprawnień)
    - 0x0E (Błąd wewnętrzny)
    - 0x1F (Błąd odczytu danych)

### 3.5 Komendy zarządzania plikami - umożliwiają tworzenie, usuwanie, odczyt, zapis i modyfikację plików

- CreateStdDataFile
- CreateBackupDataFile
- CreateValueFile
- CreateLinearRecordFile
- CreateCyclicRecordFile
- CreateTransactionMACFile
- DeleteFile
- GetFileIDs
- GetISOFileIDs
- GetFileSettings
- ChangeFileSettings

Przykładowe odpowiedzi dla wymienionych komend:

- sukces: 0x00
- błąd:
  - 0x9D (Niepowodzenie z powodu braku uprawnień)
  - 0x0E (Błąd wewnętrzny)
  - 0x1F (Błąd odczytu danych)

## 3.6 Komendy zarządzania danymi - umożliwiają operacje odczytu, zapisu, manipulacji oraz aktualizacji danych

- ReadData
- WriteData
- GetValue
- Credit
- Debit
- LimitedCredit
- ReadRecords
- WriteRecord
- UpdateRecord
- ClearRecordFile

Przykładowe odpowiedzi dla wymienionych komend:

- sukces: 0x00
- błąd:
  - 0x9D (Niepowodzenie z powodu braku uprawnień)
  - 0x0E (Błąd wewnętrzny)
  - 0x1F (Błąd odczytu danych)

## 3.7 Komendy zarządzania transakcjami - umożliwiają kontrolę nad operacjami transakcyjnymi, w tym zatwierdzanie lub anulowanie wcześniejszych operacji zapisu

- CommitTransaction
- AbortTransaction
- CommitReaderID

Przykładowe odpowiedzi dla wymienionych komend:

- sukces: 0x00
- błąd:
  - 0x9D (Niepowodzenie z powodu braku uprawnień)
  - 0x0E (Błąd wewnętrzny)
  - 0x10 (Błąd zakończenia transakcji)

3.8 Komendy standardu ISO\IEC 7816-4 - umożliwiają interakcje zgodnie z wymienionym protokołem (wybór pliku, odczyt danych binarnych, aktualizację danych binarnych itd.)

- ISOSelectFile
- ISOReadBinary
- ISOUpdateBinary
- ISOReadRecord
- ISOAppendRecord
- ISOGetChallenge
- ISOExternalAuthenticate
- ISOInternalAuthenticate

  Przykładowe odpowiedzi dla wymienionych komend:
  - sukces: 0x00
  - błąd:
    - 0x9D (Niepowodzenie z powodu braku uprawnień)
    - 0x0E (Błąd wewnętrzny)
    - 0x1F (Błąd wyboru pliku ISO)

3.9 Komendy kart wirtualnych - umożliwiają manipulację danymi poprzez symulację operacji kart wirtualnych

- ISOSelect
- ISOExternalAuthenticate

  Przykładowe odpowiedzi dla wymienionych komend:
  - sukces: 0x00
  - błąd:
    - 0x9D (Niepowodzenie z powodu braku uprawnień)
    - 0x0E (Błąd wewnętrzny)
    - 0x1F (Błąd wyboru pliku ISO)

3.10 Komendy kontroli zbliżeniowej - umożliwiają wykonywanie operacji związanych z dokładnym pomiarowaniem odległości w celu kontroli zbliżeniowej

- PreparePC
- ProximityCheck
- VerifyPC

Przykładowe odpowiedzi dla wymienionych komend:

- sukces: 0x00
- błąd:
  - 0x9D (Niepowodzenie z powodu braku uprawnień)
  - 0x0E (Błąd wewnętrzny)
  - 0x10 (Błąd przygotowania do kontroli zbliżeniowej)

### 3.11 Komendy kontroli oryginalności - umożliwiają sprawdzenie autentyczności danych lub urządzeń

- Read_Sig
  - sukces: 0x00 (Pomyślne odczytanie sygnatury)
  - błąd:
    - 0x9D (Niepowodzenie z powodu braku uprawnień)
    - 0x0E (Błąd wewnętrzny)
    - 0x1F (Błąd odczytu sygnatury)

## 4. 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): przesyłanie danych między kartą a czytnikiem, dane są zabezpieczane przez dołączenie kryptograficznej sumy kontrolnej - obliczanej na podstawie danych oraz klucza kryptograficznego, co zapewnia bezpieczeństwo i niezmienność przesyłanych informacji,

c) szyfrowany transfer danych (zabezpieczony przez CRC przed szyfrowaniem): dane wraz z sumą kontrolną są szyfrowane wybraną metodą kryptograficzną, co zwiększa integralność i niezmienność przesyłanych informacji.

## 5. Zgodność z Mifare Classic (pełne)

Karty Mifare Classic jest szeroką stosowaną rodziną kart bezstykowych, które są znane ze swojej prostoty i niezawodności, jednak porównując je z kartami Mifare DESFire EV3 można wyróżnić najważniejsze rozbieżności:

- mniejszy poziom bezpieczeństwa (starsze algorytmy kryptograficzne, brak zaawansowanych mechanizmów zabezpieczeń),

- mniejsza pamięć,
- węższy zakres funkcji i możliwości,
- tylko jednokierunkowa komunikacji,
- mniejsza kompatybilność wsteczna.

Aby uzyskać pełną zgodność kart Mifare Classic i Mifare DESFire EV3 należy:

a) skorzystać z funkcji emulacji w Mifare DESFire EV3 - konfiguracja karty w celu imitacji struktury pamięci i kluczy używanych przez Mifare Classic:

   - utworzenie aplikacji z identyfikatorem aplikacji odpowiadającym Mifare Classic,

   - odwzorowanie sektorów Mifare Classic na plik w DESFire.

b) skorzystać z tego samego zestawu kluczy i metod autoryzacji w obu systemach:

   - konfiguracja Mifare DESFire EV3 przy użyciu tych samych kluczy co Mifare Classic,

   - konfiguracja, żeby DESFIRE korzystał z kluczy w odpowiednich emulowanych sektorach,

   - użycie jednolitego trybu szyfrowania DES, 3DES lub AES.

c) korzystać z odpowiednich czytników:

   - z wbudowaną możliwością obsługiwania obu typów kart,

   - zaktualizować posiadane czytniki jeśli to możliwe.

d) sklonować dane:

   - skorzystać z narzędzia bądź odpowiednio przygotowanego skryptu, który odczyta dane z kart Mifare Classic i zapisać je w odpowiedniej strukturze na DESFire.

## 6. Bibliografia


MIFARE DESFire EV3
MIFARE
MIFARE DESFire
Differences Between MIFARE Classic And MIFARE DESFire Cards?
NXP® MIFARE® DESFire® EV3