Gemalto DESFire
Datasheet

Contents

1. GEMALTO MIFARE DESFIRE

1.1 Overview

Transport operators are now facing increasingly sophisticated demands. Their infrastructures need to fit the requirements of multi-application usage in a secure environment. The microprocessor-based smart card is an ideal solution for increasing data storage, enhancing security and flexibility. The Mifare DESFire cards can handle far more complex applications than traditional memory cards.

The Gemalto DESFire is a new Mifare generation product with improved security and a maximum interoperability.

1.1.1 Security

Mutual challenge and response authentication, data ciphering, and message authentication protect the whole system from the fraud. These checks are guaranteed thanks to its embedded 3-DES encryption engine. Furthermore, each Gemalto Mifare DESFire has a unique hard-written serial number which guaranties that each card can be individually selected.

1.1.2 Interoperability

The Gemalto DESFire card offers maximum interoperability ensured by the compliance with four levels ISO 14443-A standard both in the readers (called Proximity Coupling Device or PCD) and in the cards (called Proximity Integrated Circuits Cards or PICCs). While memory chips can support most functions of ISO 14443, only a microprocessor can fully support all four parts, including Part 3, which refers to anti-collision measures required when more than one card is in the field; and Part 4, which specifies the protocols for high-level security required for secure transactions. Companies who are looking to guarantee interoperability should require full compliance of ISO 14443 Parts 1-4.

1.1.3 High throughput

The card and reader start to transmit data as soon as the card enter the reader RF antenna field, thus enabling the card holder to carry out transactions quickly and conveniently, through an intentional action.

The RF communication interface transfers data between the Gemalto Mifare DESFire card and reader at a baud rate up to 424kbits/s. This high data transfer rate enables ticketing transactions to be handled in 0,1 to 0,5 second. Therefore, transactions can be carried out without cardholders having to stop in front of the reader or remove the Gemalto Mifare card from their wallets.

2. GEMALTO MIFARE DESFIRE FEATURES

2.1 Compatibility with norms

ISO 14443-1/2/3	Defines a proximity card used for identification that used the credit card form factor (ISO 7810-ID-1)	✓ Yes compliant
ISO 14443-4	High level protocol (T=CL)	✓ Yes compliant
ISO 9798-2	Security techniques – Entity authentication mechanism	✓ Yes compliant
ISO 7810	Format for identification card (ID-1)	✓ Yes compliant
ISO 7813	Additional characteristics of ID-1 plastic banking cards (thickness for example)	✓ Yes compliant
ISO 7816	ID-1 identification with an embedded chip and contact surfaces	✓ Yes compliant
ISO 10373	Protocol test methods for proximity cards	✓ Yes compliant

2.2 Electrical

Chip	NXP
Non Volatile Memory	4 Kbytes
Basic Functionality	Contactless card operated remotely from a dedicated reader using RF transmission
Operating frequency	13,56 MHz
Communication speed	106, 212 or 424 Kbit/s
Operating range	Up to 10 cm (depending on the reader and the antenna design)

2.3 Durability

Mechanical stress	250 bending cycles on each side, 500 torsion cycles on each side as specified in ISO10373 without loosing functionality and aesthetic aspects.

2.4 Security

- Mutual three pass authentication

Prior to data transmission, a mutual three-pass authentication can be done employing either DES or 3DES.
Data transmission can be done on 3 levels of security :

- Plain data transfer,
- Plain data transfer with DES/3DES cryptographic checksum (MAC),
- Fully encrypted data transfer

- Any data transferred from card to reader or vice-versa is encrypted on RF-channel with replay attack protection.
- The authenticity of the data on application level is guaranteed with a 4 bytes MAC.
- Access to user data is granted on application level. For each application up to 14 different keys (16 bytes each) can be assigned to control access to data stored in the card, preventing from fraudulent access.
- There are 4 different Access Rights stored for each file with each application :
  - Read Access
  - Write Access
  - Read & Write Access
  - Change Access Rights
- Anti-collision
- Anti-cloning

Each chip has a unique card serial number (7 bytes) to ensure the uniqueness of each device.

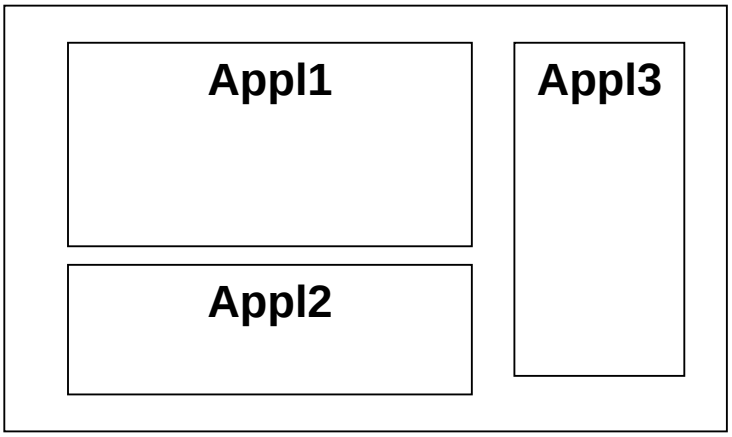
3. MEMORY ORGANIZATION & ACCESS

The DESFire contains 4Kbytes of Non Volatile memory. This memory is organized using a flexible system. The card can hold up to 28 applications, each application can have up to 16 files and up to 14 (3)DES keys. So it allows having different types of application with different levels of security.

Each application and/or file can be created, at card pre-personalization (card production), at personalization stage or in the field.

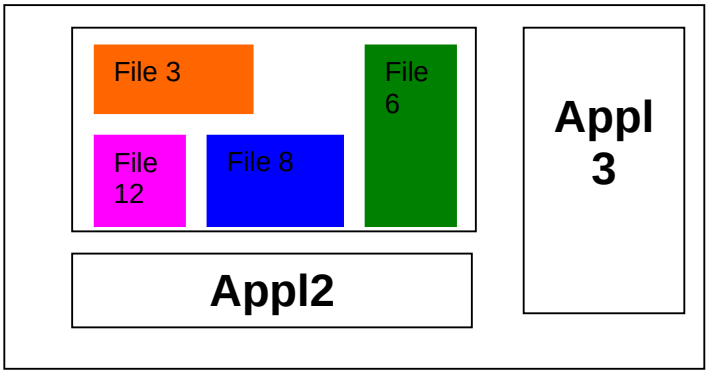
3.1 Applications

The card can contain up to 28 applications. For example a card can have 3 applications: one for transport (Appl1), one for access control (Appl2) and the last for e-purse (Appl3).



3.2 Files

The DESFire can contain up to 16 files per application.



There are 5 different types of files:

- Standard data files
- Backup data files
- Value files with backup
- Linear record files with backup
- Cyclic record files with backup