LEAF Memory Usage Specification

for MIFARE DESFire® EV2/3

Version 3.1 | September 2020

TABLE OF CONTENTS

1. General Information

This document is intended to provide a complete definition of the data structure for LEAF Memory Usage Specification..

This specification is intended to allow every RFID solution provider to participate in the LEAF program. Its purpose is to give the end-users maximum interoperability, to allow them to manage and own their custom cryptographic keys while giving them the ability to source and program cards from any RFID participating vendor.

Changes made in Version 3.0 + can be found in APPENDIX C.

Technical Highlights

- NXP DESFire EV2 or EV3 can be used for LEAF. Both EV2 and EV3 function identically (they offer no functional differences related to LEAF) and can be used interchangeably with LEAF, and both 4K and 8K memory sizes fit the LEAF memory structure.
- Every LEAF card is configured into the full AES 128-bit encryption mode.
- Every LEAF card is issued in a secure facility to guarantee that the (NXP) transport keys are securely updated and to ensure that every card is authentic and secure.
- The card comes with an advanced access control data structure (ACD), with security features that include digital signatures, unique badge ID/site code sets, and tiered security access privileges
- **Advanced Key management** — The card design allows for the secure applications to be protected by custom keys at issuance or at any time during the lifetime of the product. Additional applications can be added anytime, and without affecting the security of the access control application.
- **LEAF Cc (Custom Crypto)** — The design of the LEAF card also allows for the card to be protected by end-user owned custom keys. LEAF Credentials can be ordered with custom keys. Additionally, the custom keys can be programmed into the card at any time during the life-cycle of the card.
- **Card Security** — The security of LEAF Credentials is guaranteed by unwavering key management provided by the LEAF secure card issuance, and proven distribution and processes. Note that users are encouraged to use their own custom keys (by choosing LEAF Cc) to secure their installation for the maximum level of security.
- **The Open and interoperable functionality** is guaranteed through open and clear specifications, allowing all RFID vendors to create LEAF compatible cards and providing users complete freedom and unlimited ways to use their card

2. Applications Present on a LEAF Card

2.1. Applications on a LEAF Cc card

List of the Application names and associated Application IDs:

- LEAF Cc Access Control Apps: F51CDB and F51CDE. This application is loaded with the Access Control Data (defined in Table 2) and protected by the end-user custom keys
- The Access Control Data for EV1 Compatibility resides in application F532F0 and contains the same access control data defined in Table 4. This application is protected by the end-user custom keys.
- Campus App: F51CDC. The Campus Application includes three files (files 1, 2, and 3). This application is intended for easy and secure use by third-party vendors. This application is pre-loaded (but with no data) This application is protected by the end-user custom keys.
- User Privileges App: F532F1 This Application includes one file (file 1). This application is pre-loaded (but with no data).
- Bio App: 42494F This Application includes two files (file 0 and file 1). Both files are loaded with the ACD ID.
- Additional applications can be added to the card by the end-user, but an authentication with the end-user custom card Master key Kmcc is required.
- Key diversification: All LEAF Cc keys are diversified, except the Bio app keys Kbiow and Kbior, Kc15 and Kc16. These four keys are non-diversified values for LEAF Cc.

Table 1 — The LEAF Card Architecture

Applications	DESFire App IDs	Purpose
Access Control	F51CDB	**LEAF Cc (Custom Crypto) Application for Access Control Data (ACD)** For customers requiring custom keys: This application protects the same ACD using 16 (user-owned) read keys (Kc1 through Kc16) to allow for 16 different independent vendors to read the ACD. The data integrity and authenticity of the ACD is also independently verified by each of the 8 Read Keys. The user can independently and securely provide any one of these 16 keys to the RFID vendor(s) of their choice, guaranteeing full interoperability
	F51CDE	
	F532F0	**EV1 backward compatibility Application** This application is fully compatible with the specification of the 'Generic Access Control Data Model' Application Note AN10957 openly published by NXP. This application is intended for readers requiring DESFire EV1 compatibility. It contains the same access control data as the LEAF ACD.
Campus Application	F51CDC	**The Campus Application** The campus application is designed for the convenience of the user, to securely read and write their various custom applications (such as campus transit, cafeteria, library, purse, etc) independently of the access control data application or other applications. The application includes three files allowing for 64 bytes of data each, which is accessible by a single write key, and three read keys.
Bio Application	42494F	**The Biometrics Application** The Biometrics application is designed to allow Biometrics devices to read/write a biometrics template up to 1KByte in size to the card and to access the card ID in a reader binary format.
User Privileges Application	F532F1	**The User Privileges Application** The User Privileges application is designed to allow the propagation of user access rights to remote devices such as off-line locks, and the logging of user access activities to these remote devices
Other Applications	Any application	**Open Memory** The rest of the card memory is fully accessible to the user for additional applications of their choosing while enjoying the full breadth of the DESFire EV2/3 functionality. The possibilities are limitless.

3. Data Structure

The card is structured to allow for multiple applications to independently reside on the card and to allow for additional applications to be added freely to the card at any time.

The access control data spans over several applications. LEAF Cc also allows for 16 different types of RFID reader devices from any vendor, as these applications are protected by 16 read keys and one read/write master key.

The card is also programmed with a legacy DESFire EV1 application for backward compatibility (featuring full compatibility with the NXP application note AN10957)

The LEAF compatibility is genuinely open as it is not restricted to LEAF vendors. Because this specification is openly published, any RFID vendor may supply end-users with compatible DESFire EV2/3 cards protected by their custom keys.

3.1. Access control Data (ACD) Applications

- 16 end-user read keys and one read/write key allow different types of RFID devices to access the ACD without the need for vendors to share a key.

The data is structured as such:

- LEAF Cc Application
    - Access Control App 1: F51CDB File 2
    - Access Control App 2: F51CDE File 2
- These Applications are configured as such:
    - Encryption AES (communication fully enciphered)
    - Read Access Rights via 8 keys (K1 .. K8)
    - Application master key K0: Read/Write Access
    - The Data is contained in File 2 of all four Access control Applications and is defined in Table 2 below.

Table 2 — Structure of the ACD (EV2/3 File 0x02)

Field Name	Field Type	Length (Bytes)	Value range and/or (example)
Version – Major	**Binary**	**1**	**0x03**
Version – Minor	Binary	1	0x00
Customer / Site Code	BCD	5	0 … 9,999,999,999
Credential ID	BCD	8	0 … 9,999,999,999,999,999
Access Data Format	Binary	1	0 .. 255
Access Data Bit Length	Binary	1	1 .. 128 (for example 0x1A for 26-bit output)
Access Reader Data	Binary	16	Right justified array of bitstream data. Example (hexadecimal): 00 00 00 00 00 00 00 00 00 00 00 00 03 55 00 FF Corresponding Wiegand bitstream output for Access Data Bit Length 26-bit: 11 0101 0101 0000 0000 1111 1111
Externally Printed Number	BCD	8	0 .. 9,999,999,999,999,999
Order Data	BCD	5	0 .. 9,999,999,999 10 digits: - Vendor ID 4 most significant digit - Least significant 6-digits: up to the vendor
Reissue code	BCD	1	0
Reserved Future Use	Binary	9	0
Secure Issuance Digital Signature	Binary	8	System 8-byte CMAC signature (using key Ksi)
Reader Digital Signatures	Binary	80 (8x10)	02 01 + 8-byte CMAC signature based on K1 and file data 02 02 + 8-byte CMAC signature based on K2 and file data 02 03 + 8-byte CMAC signature based on K3 and file data 02 04 + 8-byte CMAC signature based on K4 and file data 02 05 + 8-byte CMAC signature based on K5 and file data 02 06 + 8-byte CMAC signature based on K6 and file data 02 07 + 8-byte CMAC signature based on K7 and file data 02 08 + 8-byte CMAC signature based on K8 and file data

3.2. DESFire EV1 Compatibility Application

The Access Control Data for EV1 Compatibility reside in application F532F0. It is fully defined in the specification GENERIC ACCESS CONTROL DATA MODEL (Application Note AN10957.pdf) published by NXP. See Table 7 for key nomenclature.

DESFire EV1 Compatibility Application ID, Files, and details

- Fully compliant with specification AN10957.pdf
- Application ID F532F0
- File 1: Free read access. Change via K0.
- File 2: Secure read (fully encrypted with MAC signature) via K1. Change via K0
- Three Keys per application. All keys are AES 128-bit keys.
- Key nomenclature (per AN10957.pdf):
    - APPMK is the "APPlication Master Key" (Read/Write K0)
    - APPVK is the "APPlication Verification Key" (Read-only key K1)
    - OCPSK is the "Originality Cloning Protection System Key"
- Additional notes:
    - Files also called objects in Application Note AN10957.pdf. File 0x01 called Card Identifier Object. File 2 called PACS Data.
    - Both files are Standard data files. They are structured per Tables 3 and 4 below

Table 4 — Structure of File 0x01 of the application F532F0 — The Access Control Data for EV1 Compatibility

Field Name	Field Type	Length (Bytes)	Value range and/or example
Manufacturer	ASCIIZ	16	Example: 'SMARTRAC USA 0100'
Mutual Authentication Mode	Binary	2	0xCA02 (ISO7816-4 auth, AES128)
Communication Encryption	Binary	1	0x02 (fully enciphered)
Customer ID	BCD	4	Example 0x12 34 56 78
Key Version	BCD	1	0
Digital Signature	Binary	8	CMAC signature based on the diversified OCPSK Key, UID, File data (See Appendix B and Application Note AN10957.pdf)

Table 5 — Structure of File 0x02 of the application F532F0 — The Access Control Data for EV1 Compatibility

Field Name	Field Type	Length (Bytes)	Value range and/or example
Version – Major	Binary	1	0x00
Version – Minor	Binary	1	0x04
Customer / Site Code	BCD	5	0 … 9,999,999,999
Credential ID	BCD	8	0 … 9,999,999,999,999,999
Reissue Code	BCD	1	0
PIN Code	BCD	4	0
Customer Specific Data	Binary	20	**Default Data Format (Maximum 64 bits of access data)** Bytes 0 thru 9: 0x1001 + 8 bytes of Wiegand data with sentinel Bytes 10 & 11: Define the Wiegand format (i.e. 0x1A01 for 26-1) Example (hexadecimal) 10 01 00 00 00 00 07 55 00 FF 1A 01 00 00 00 00 00 00 00 00 1A = 26 bits 01 = Wiegand 26 bit format 01 Corresponding Wiegand bit stream output = 11 0101 0101 0000 0000 1111 1111 (sentinel bit omitted)
			Custom Data Format (Maximum 144 bits) Byte 0:Indicates the number of bits of the Access control bitstream Byte 1: Format reference byte (Defines parity etc…) Bytes 2 .. 19: Right justified array of bitstream data Example (hexadecimal) 1A 01 00 00 00 00 00 00 00 00 00 00 00 00 00 03 55 00 FF 1A = 26 bits 01 = Wiegand 26 bit format 01 Corresponding Wiegand bitstream output = 11 0101 0101 0000 0000 1111 1111
Digital Signature	Binary	8	CMAC signature based on the diversified OCPSK Key, UID, File data ((See Appendix B and Application Note AN10957.pdf)

3.3. Campus Applications

Each file is protected by one read key. All three campus files are protected by a common write key. The 3 files 1, 2, and 3 are all 64-byte deep.

3.4. Biometrics Application

The Biometrics Application is structured as such:

- Biometrics Application
  - Application ID 42494F
  - File 0: Standard Data File, length 1024 bytes
  - File 1: Standard Data File, length 96 bytes
  - K1: Read Only for both files
  - Application master key K2: Read/Write/Change Access Rights

Table 6 — Structure of File 0 and file 1 of the application 42494F — The Biometrics Application

File	Field Name	Field Type	Length (Bytes)	Value range and/or example
File 0	User ID Tag (0x32)	TLV	27	Example: 0x32 0x18 0x00 “123456\0 .. \0”
	Optional TLVs holding Biometric data and other identifiers.	Multiple TLVs	997	Optional TLVs
File 1	User ID	Binary	96	Raw User ID in hexadecimal, least significant byte first

3.5. User Privileges Application

The User Privileges Application is structured as such:

- Application ID F532F1 (File 1 Standard Data File, length of 768 bytes)
- Application master key K1: Read/Write/Change Access Rights

4. Keys

Table 7 — Describes the LEAF key nomenclature and the functions assigned to each key.

Application	LEAF Key name	Key usage	Application ID and DESFire EV2/3 Key Assignment/name	Access rights
Card level	Km	Card Master Key	PICC master key	Card Master
LEAF Cc	Ksicc	Custom System CMAC signature key	Ksicc is used to compute and verify the Secure Issuance Digital Signature of the ACD	Not Applicable. This key is known by the card issuer and used to verify the card's authenticity of the issuance
	Kc1 through Kc8	Custom Access Control Application Read Keys	8 Read-only Keys for app F51CDB (K1 through K8)	A total of 16 (2x8) custom (end-user owned) read-only keys.
	Kc9 through Kc16		8 Read-only Keys for app F51CDE (K1 through K8)	Kc1-Kc14 are diversified Kc15 and Kc16 are non-diversified
EV1 backward compatibility Access Control Data (App ID F532F0)	APPMK	EV1 Application (Write) Key	K0	1 Read/write key. Allows to change the file contents and the application keys
	APPVK	EV1 Application Read Key	K1	One read-only key
	OCPSK	EV1 Originality Cloning Protection System Key	OCPSK	EV1 backward compatibility Application CMAC signature computation key
Campus Application (App ID F51CDC)	Kcw	Campus Application A Read/Write Key	K0	1 Read/write key. Allows to change the files contents and the three read keys
	Kcr1, Kcr2, Kcr3	Campus Application Read Keys	K1 (read-only key for file 1) K2 (read-only key for file 2) K3 (read-only key for file 3)	Three read-only keys (one key per file)
Biometrics App (App ID 42494F)	Kbiow	Read/Write/Change Access Rights	K2	non-diversified for LEAF Cc only
	Kbior	Read only	K1	non-diversified for LEAF Cc only
User Privileges App (App ID F532F1)	Kupw	Read/Write/Change Access Rights	K1	A single key for all read/write operations

5. Key Diversification

Key diversification for all diversified keys are 16-byte AES keys and are diversified for each card using the card UID. The key diversification is defined in Application Note (per Application Note AN10957.pdf) section 4.5. Additionally, a key diversification tool can be used by developers to verify the computation of the key diversification (and the intermediary steps). This tool can be found at https://leaf-ip.firebaseapp.com/

Exception: The Bio App keys (Kbiow and Kbior) and the access app keys Kc15 and Kc16 are not diversified on LEAF Cc cards to allow for compatibility with products with no key diversification capabilities..

6. Custom Cryptographic Keys

LEAF Credentials are secured by the end-user custom keys (listed in Table 8).

Table 8 — Custom Keys to be specified for LEAF Cc

Custom Crypto Keys (Cc)	Key Function
Kmcc	Km Card Master Key
Kawcc	LEAF Cc Access Control Application Master Key
Ksicc	Leaf Cc System CMAC Signature Key
Kc1 through Kc16	The 16 LEAF Cc(Custom Crypto) read keys of the Custom Access control application
APPVKcc	EV1 backward compatibility Application Read Key
OCPSKcc	EV1 backward compatibility Originality Cloning Protection System Key
Kcw	Master Read/Write Key for the Campus Application
Kcr1 Kcr2 Kcr3	The three Campus read keys for each of the three Campus Application files
Kbior Kbiow	Non-diversified read and write keys to access and manage the Biometrics Application
Kupw	read/write key for the user privileges Application

7. Reader Compatibility and Requirements

7.1. LEAF Cc Reader Compatibility

Every DESFire compatible reader or RFID device can also securely read the LEAF card when encoded with custom keys (Cc) . The user can decide which reader vendor may read their card, by sharing the appropriate key information. No affiliation with the LEAF program is necessary. For example, the user could ask any vendor to read the Access Control Data Application (F51CDB) by sharing Kc7 with them.

APPENDIX A: User Test Keys

A set of test keys for LEAF Cc is suggested below. These keys may be used for any necessary testing between vendors and users

Table 9 — LEAF Cc Test keys

Custom Crypto Keys (Cc)	Test Key Value
Kmcc	A0010101 01010101 01010101 01010101
Kawcc	A1010101 01010101 01010101 01010101
Ksicc	A2010101 01010101 01010101 01010101
Kc1 Kc2 Kc3 Kc4 Kc5 Kc6 Kc7 Kc8 Kc9 Kc10 Kc11 Kc12 Kc13 Kc14 Kc15 (non-diversified!) Kc16 (non-diversified!)	DB010101 01010101 01010101 01010101 DB020101 01010101 01010101 01010101 DB030101 01010101 01010101 01010101 DB040101 01010101 01010101 01010101 DB050101 01010101 01010101 01010101 DB060101 01010101 01010101 01010101 DB070101 01010101 01010101 01010101 DB080101 01010101 01010101 01010101 DE010101 01010101 01010101 01010101 DE020101 01010101 01010101 01010101 DE030101 01010101 01010101 01010101 DE040101 01010101 01010101 01010101 DE050101 01010101 01010101 01010101 DE060101 01010101 01010101 01010101 DE070101 01010101 01010101 01010101 DE080101 01010101 01010101 01010101
APPVKcc	E1010101 01010101 01010101 01010101
OCPSKcc	E1020101 01010101 01010101 01010101
Kcw	C2000101 01010101 01010101 01010101
Kcr1	C2010101 01010101 01010101 01010101
Kcr2	C2020101 01010101 01010101 01010101
Kcr3	C2030101 01010101 01010101 01010101
Kbiow (non-diversified!)	B1000101 01010101 01010101 01010101
Kbior (non-diversified!)	B2010101 01010101 01010101 01010101
Kupw	F1010101 01010101 01010101 01010101

APPENDIX B: Modified CMAC Generation

The CMAC signature discussed throughout this document references the AN10957.pdf application note. In this application note, section 5 titled Digital Signature / Originality Check, describes the generation of the digital signature using a CMAC calculation. This LEAF application follows this method with one exception. The diversification described in Step 2:

Step 2 : Create Div Input Div Constant 1 + UID + Padding
0x0104deadbeeffeed800000000000000000000000000000000000000000000000

has been changed to:

Step 2 : Create Div Input Div Constant 0x88 + UID + 0x88 + UID + Padding
0x8804deadbeeffeed8804deadbeeffeed800000000000000000000000000000000

All other steps remain the same.

APPENDIX C: Changes in Version 3.1

Table 10 — Changes in version up to 3.1

Change ID	In Version	Description
301	3.0	Removal of one ACD application in LEAF Si 16 read keys Kv1 through Kv16 (down from 24)
302	3.0	Added one ACD application in LEAF Cc to match the LEAF Si app structure and number of keys: 16 read keys Kv1 through Kv16 (up from 8)
303	3.0	Added file 1 as the high-security issuer file for LEAF Si in-app F51CD8
304	3.0	Additional applications can no longer be added to LEAF Si cards. In order to add applications to the card, the card must be upgraded to LEAF Cc first.
305	3.0	Modified Customer-specific data field in the EV1 compatibility app to include the use of a sentinel bit. This data field can still support the format described in Leaf specification version 2.1 to handle bitstreams larger than 64 bits (Maximum = 144 bits)
306	3.0	Added application 42494F and file 0 for Biometrics applications.
307	3.0	All LEAF Si keys are diversified All LEAF Cc keys are diversified, except the Bio app keys Kbiow and Kbior, and the Access App keys Kc15 and Kc16. These four keys are non-diversified values for LEAF Cc
308	3.0	Added application F532F1 and file 1 for the "User Privileges" Application
309	3.0	Added EV3 because it is released to general availability and offers complete compatibility.
310	3.1	Removed LEAF Si references
311	3.1	Clarified Kc15 and Kc16
312	3.1	Renamed LEAF Credential Ordering information to Custom Cryptographic Keys

Note: Changes do not affect backward compatibility.