APPLICATION NOTE: LEAF Si (Secure issuance) 2.1

APPLICATION DEFINITION FOR USE ON THE DESFIRE EV2 PLATFORM

April 2018. Released version
FOR PUBLIC DISTRIBUTION

1. General information

This document is intended to provide a complete definition of the data structure for LEAF 2.1. Here are the technical highlights:

- The NXP DESFire EV2 chip is used for LEAF. Both 4K and 8K memory sizes are used for the LEAF card
- 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 Si (Secure issuance):** Desfire EV2 based LEAF cards may be issued by a certified LEAF vendor for out-of-the-box interoperability, convenience, and high security without the need for additional key management by the user. These cards are referred to as “LEAF Si”.
- **LEAF Cc (Custom Crypto):** The design of the LEAF card also allows for the card to be protected by end-user owned custom keys. The LEAF cards can be ordered with custom keys. Additionally, the custom keys can be programmed into the card at anytime during the life-cycle of the card.
- **Card Security:** The security of LEAF cards 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

This specification is intended to allow every RFID solution provider to participate in the LEAF program. It’s 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.

2. Applications present on a LEAF cards

2.1. Applications on a LEAF Si card

List of the Application names and associated Application IDs (see table 1):

- The LEAF Si Application Access Control Data (defined in Table 2) resides in these three applications:
  - Access Control App 1: F51CD8
  - Access Control App 2: F51CD9
  - Access Control App 3: F51CDA
- LEAF Cc Access Control App: F51CDB. This application is pre-loaded (but with no keys and no data) and is available for the end-user to upgrade their cards to custom keys
- The Access Control Data for EV1 Compatibility App F532F0. This application is pre-loaded (but with no keys and no data) and is available for the end-user to upgrade their cards to 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 keys and no data) and is available for the end-user to upgrade their cards to custom keys
- **Additional applications can be freely added to the card (with no authentication required)**

2.2. Applications on a LEAF Cc card

List of the Application names and associated Application IDs:

- The LEAF Si Applications are not present
- LEAF Cc Access Control App: F51CDB. 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 reside 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.
- **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.**

Table 1 (below) describes the architecture of the LEAF card

Applications	Desfire App IDs	Purpose
Access Control	F51CD8	**LEAF Si Applications for Access Control Data (ACD)** These 3 applications allow for 24 different LEAF Si participating RFID vendors to independently read the ACD, through 24 independent Read Keys Kv1 though Kv24. The data integrity and authenticity of the ACD is also independently verified by each of the 24 Read Keys. (Note: These applications are not present in Leaf Cc cards)
	F51CD9	
	F51CDA	
	F51CDB	**LEAF Cc (Custom Crypto) Application for Access Control Data (ACD)** For customers requiring custom keys: This application protects the same ACD using 8 (user-owned) read keys (Kc1 through Kc8) to allow for 8 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 8 keys to the RFID vendor(s) of their choice, guaranteeing full interoperability
	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.
Other Applications	**Any application**	**The 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 functionality. The possibilities are limitless.

Table 1: the LEAF Card Architecture

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 Si allows up to 24 different types of RFID reader devices from certified LEAF vendors to independently and securely read the same card. LEAF Cc allows for 8 different types of RFID reader devices from any vendors, as this application is protected by 8 read keys and one read/write master key.

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

The program is not restricted to LEAF vendors. Because this specification is openly published, any RFID vendor may supply end-users with LEAF-compatible Desfire EV2 cards protected by their custom keys

3.1. ACD (Access control Data) Applications

- In the case of LEAF Si cards, the ACD structure is written to the three LEAF Si applications, allowing for a secure read by many different RFID devices (such as wall readers, locks, printers, USB readers, etc…) where each RFID device can read the ACD and verify the ACD’s authenticity independently of other RFID device vendors, with a specific key assigned to it.
- In the case of LEAF Cc cards the ACD is only written to the LEAF Cc application (The LEAF Si applications are not installed). 8 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 Si Applications
  - Access Control App 1: F51CD8 File 2
  - Access Control App 2: F51CD9 File 2
  - Access Control App 3: F51CDA File 2
- LEAF Cc Application
  - Access Control App 1: F51CDB 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.

Field Name	Field Type	Length (Bytes)	Value range and/or (example)
Version – Major	**Binary**	**1**	**0x02**
Version – Minor	Binary	1	0x01
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 bit stream data. Example (hexadecimal): 00 00 00 00 00 00 00 00 00 00 00 00 03 55 00 FF Corresponding Wiegand bit stream 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

Table 2: Structure of the ACD (EV2 File 0x02)

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 5 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
    -

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 3: 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
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	Byte 0:Indicates the number of bits of the legacy Access control bit stream (i.e. Wiegand) Byte 1: Format reference byte Bytes 2 .. 19: Right justified array of bit stream data Example (hexadecimal) 1A 01 00 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 bit stream 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)

Table 4: Structure of File 0x02 of the application F532F0 The Access Control Data for EV1 Compatibility

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.

4. Keys

Table 5 below describes the LEAF key nomenclature and the functions assigned to each key.

Application	LEAF Key name	Key usage	Application ID and Desfire EV2 Key Assignment/name	Access rights
Card level	Km	Card Master Key	PICC master key	Card Master
LEAF Si	Kmw	Access Control Application Master Key	K0 for the four ACD applications F51CD8, F51CD9, F51CDA, F51CDB.	The Read/write key. Allows to change the contents of the files and change all the application keys
	Ksi	System CMAC signature key	Ksi 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
	Kv1 through Kv8	Vendor Keys 1 through 24. Access Control Application Read Keys (24 keys total)	8 Read-only Keys for app F51CD8 (K1 thru K8)	A total of 24 (3x8) read-only keys. They are used by the various RFID readers and devices to read the Access control application data and verify its authenticity (by computing the CMAC)
	Kv9 through Kv16		8 Read-only Keys for app F51CD9 (K1 through K8)	
	Kv17 through Kv24		8 Read-only Keys for app F51CDA (K1 through K8)	
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 8 custom (end-user owned) read-only keys.
EV1 backward compatibility Access Control Data (App ID F532F0)	APPMK	EV1 Application (Write) Key	K0	1 Read/write key. Allows to change the files 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)

Table 5 : LEAF Key nomenclature and function

5. Key Diversification

All 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/

6. How to Order LEAF cards

STEP 1: Define the card format information

- Chip size (Desfire EV2 4K or Desfire EV2 8K)
- External Printed Number and Credential ID
- Customer/Site Code
- Wiegand format (Pick your format from the LEAF published Wiegand Formats Application note.pdf)

STEP 2: Choose LEAF Si or LEAF Cc

LEAF Si: These cards are securely issued with LEAF Si applications and keys (No keys need to be provided to the vendor)

Or

LEAF Cc: The cards are secured by the end-user custom keys (listed in table 6 below)

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 Kc2 Kc3 Kc4 Kc5 Kc6 Kc7 Kc8	The 8 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

Table 6: Custom Keys to be specified for LEAF Cc

7. LEAF Key Management

7.1. Securing the LEAF Keys

This section is mostly relevant to participating LEAF card issuers. All the keys are provided by the LEAF program to the participating secure card issuance vendors, using a hardware security module or HSM. Table 7 (below) includes the HSM Key reference for the purpose of card programming during the secure issuance. The HSM guarantees that the secure card issuance vendors do not have access to the non-diversified LEAF Si key values. Table 7 also lists a set of test keys, which can be conveniently and freely shared by and between vendors for the purpose of product testing. Additional test keys are listed in Appendix A, for vendors to test a set of LEAF Cc keys.

Application	LEAF Key name	HSM Key Ref	Test Key value
Card level	Km	02 D0	00010101 01010101 01010101 01010101
LEAF ACD (Access Control Data) App IDs F51CD8, F51CD9, F51CDA, F51CDB	Kmw	02 A0	22010101 01010101 01010101 01010101
	Ksi	02 A1	33010101 01010101 01010101 01010101
	Kv1 Kv2 Kv3 Kv4 Kv5 Kv6 Kv7 Kv8	02 01 02 02 02 03 02 04 02 05 02 06 02 07 02 08	D8010101 01010101 01010101 01010101 D8020101 01010101 01010101 01010101 D8030101 01010101 01010101 01010101 D8040101 01010101 01010101 01010101 D8050101 01010101 01010101 01010101 D8060101 01010101 01010101 01010101 D8070101 01010101 01010101 01010101 D8080101 01010101 01010101 01010101
	Kv9 Kv10 Kv11 Kv12 Kv13 Kv14 Kv15 Kv16	02 09 02 0A 02 0B 02 0C 02 0D 02 OE 02 0F 02 10	D9010101 01010101 01010101 01010101 D9020101 01010101 01010101 01010101 D9030101 01010101 01010101 01010101 D9040101 01010101 01010101 01010101 D9050101 01010101 01010101 01010101 D9060101 01010101 01010101 01010101 D9070101 01010101 01010101 01010101 D9080101 01010101 01010101 01010101
	Kv17 Kv18 Kv19 Kv20 Kv21 Kv22 Kv23 Kv24	02 11 02 12 02 13 02 14 02 15 02 16 02 17 02 18	DA010101 01010101 01010101 01010101 DA020101 01010101 01010101 01010101 DA030101 01010101 01010101 01010101 DA040101 01010101 01010101 01010101 DA050101 01010101 01010101 01010101 DA060101 01010101 01010101 01010101 DA070101 01010101 01010101 01010101 DA080101 01010101 01010101 01010101

Table 7 : Test Keys and HSM Key references

7.2. Deployment of LEAF cards

Tables 8a and 8b below show how the keys are used for the various applications, for both LEAF Si and LEAF Cc cards. The keys provided by the HSM are highlighted in RED, and the end-user owned Cc keys are highlighted in BLUE

Application	LEAF Key name	Key usage	DESFIRE Key	HSM Key Ref For LEAF Si
Card level	Km	Card Master Key	Card Master Key	02 D0
LEAF Si Access Control Data App IDs F51CD8, F51CD9, F51CDA	Kmw	Access Control Application Master Key	K0 for all four applications	02 A0
	Ksi	System CMAC signature key	Ksi	02 A1
	Kv1 through Kv8	Read keys for App ID F51CD8	K1 through K8	02 01 through 02 08
	Kv9 Through Kv16	Read keys for App ID F51CD9	K1 through K8	02 09 through 02 10
	Kv17 Through Kv24	Read keys for App ID F51CDA	K1 through K8	02 11 through 02 18
LEAF Cc Access Control Data App ID F51CDB	Kawcc	Application (read/write) Key	K0	ZEROS
	Ksicc	System CMAC Signature Key	Ksicc	ZEROS
	Kc1 through Kc8	Read Keys	K1 through K8	ZEROS
EV1 backward compatibility Access Control Data (App ID F532F0)	APPMK	EV1 backward compatibility Application (Write) Key	K0	ZEROS
	APPVK	EV1 backward compatibility Application Read Key	K1	ZEROS
	OCPSK	EV1 backward compatibility Originality Cloning Protection System Key	OCPSK	ZEROS
Campus Application (App ID F51CDC)	Kcw	Master Campus Application Read/Write Key	K0	ZEROS
	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)	ZEROS

Table 8a: Application Assignment of LEAF Si keys

Application	Key usage	DESFIRE Key	LEAF Cc end-user owned keys
Card level	Card Master Key	Card Master Key	Kmcc
LEAF Cc Access Control Data App ID F51CDB	Application (read/write) Key	K0	Kawcc
	Read Keys	K1 through K8	Kc1 through Kc8
EV1 backward compatibility Access Control Data (App ID F532F0)	EV1 backward compatibility Application (Write) Key	K0	Kawcc
	EV1 backward compatibility Application Read Key	K1	APPVKcc
	EV1 backward compatibility Originality Cloning Protection System Key	OCPSK	OCPSKcc
Campus Application (App ID F51CDC)	Master Campus Application Read/Write Key	K0	Kcw
	Campus Application Read Keys	K1 (read-only key for file 1) K2 (read-only key for file 2)	Kcr1, Kcr2, Kcr3

		K3 (read-only key for file 3)	

Table 8b: Application Assignment of LEAF Cc keys.

7.3. Reader compatibility and requirements

7.3.1. LEAF Si Reader Compatibility

Every Desfire compatible reader or RFID device can securely read the LEAF Si card. The LEAF program provides one of the 24 read-keys to the vendor to allow it's reader to securely read the Access Control Data (ACD). Each reader that reads the ACD is also required to verify it's authenticity by computing their assigned CMAC.

7.3.2. 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 these vendors. 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

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	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
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

Table 10: LEAF Cc Test keys

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 IP 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
0x8804deadbeeffeed8804deadbeeffeed80000000000000000000000000000000

All other steps remain the same.