APPLICATION NOTE: LEAF Cc (Custom Crypto version 2.1)
How to read a LEAF card with a RFID Reader interface

May 2018. Released version
FOR PUBLIC DISTRIBUTION

1. General information

This document is intended to provide a definition of the data structure for LEAF 2.1, in order to allow any reader vendor to read the LEAF Cc (Custom crypto) credential

- The NXP DESFire EV2 chip is used for LEAF Cc. Both 4K and 8K memory sizes are used for the LEAF card
- Every LEAF Cc card is configured into the full AES 128-bit encryption mode.
- 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

2. Access Control Application on a LEAF Cc card

- LEAF Cc Access Control App is located in App F51CDB File 2. This application is loaded with the Access Control Data (defined in table 1 below) and 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.**
- LEAF Cc allows for 8 different types of RFID reader devices to indepedently read the ACD„ as this application is protected by 8 read keys and one read/write master key.
- 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 1.

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 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 1: Structure of the ACD (EV2 File 0x02)

3. Keys

Table 2 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 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.

Table 2 : LEAF Key nomenclature and function

4. 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/

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

Table 3: Custom Keys for LEAF Cc

5. 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 end-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. If a vendor can read an EV2 card, they can read the LEAF Cc card!!! For example, the user could ask a vendor to read the Access Control Data Application by sharing Kc7 with one vendor and Kc2 with another vendor. The vendors do not need to collaborate with each other.

Section intentionally left blank

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 4: 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
0x8804deadbeeffeed8804deadbeeffeed800000000000000000000000000000000

All other steps remain the same.