Smartcard Tap & Ride

DESfire card configuration

Version: 03

Date: 2019-10-24

CONFIDENTIAL

Revision History

Author	Version	Date	Details of Change
Nick Sutherland	01	2019-09-10	Draft
Nick Sutherland	02	2019-10-03	Feedback from Universal Smartcards and detailed changes to file formats
Nick Sutherland	03	2019-10-24	Added SAM definition
Luis Vivas	04	2019-11-13	Added key 5 to SAM table

Copyright

Table of Contents

Section 1 Introduction

1.1 Purpose

This document describes the structure of Masabi Justride Tap and Ride Desfire smartcards for partners who will manufacture these cards. It provides details of the applications, files and access key behaviour for each element of the card

1.2 Reference Documents

NXP document: AN10922 Symmetric key diversifications Rev. 2.2 — 2 July 2019

Masabi document: Detailed design of DESFire ABT tokens

Section 2 Format Definitions

2.1 Justride DESfire EV1/2 card format definition

GENERAL NOTES

UID to be visible without presenting any key.

If possible UIDs should be non consecutive.

ICN to be printed on the card (later we may ask for this to be as a 1D barcode as well as text)

ICN assignment should be specified as agreed with the Agency.

Keys for a test batch of 5 cards will be provided via secure email, production keys will be different and may be supplied using a SAM.

Each card has 1 app with 6 files and 14 keys all diversified using the UID and AppID and the specified Diversification Master Key according to AN10922.

Text files 0 to 3 will contain the same data on each card but this data will be different between cards. A CSV file will be provided with a row for each card. The data in the CSV file will be provided as text and can be written to the card without modification.

Text files 4 and 5 will initially be empty. These will be written by devices in the field and will be cyclic record files with 8 entries each probably 64B or less per record.

CARD MASTER AID

No apps can be created or deleted and no public listing is possible

Application ID (hex)	: 0x0
Number of Keys	: 1
Key Type	: AES
Allow master key change	: YES
Free directory list without master key	: NO
Free create/delete without master key	: NO
Configuration changeable	: NO

Keys (fixed)

KeyID.PICCMasterKey	: Diversified according to AN10922 using card UID

Justride Tap and Ride AID

Application ID (hex)	: Different by card scheme and defined by Masabi. Example: 0x525452
Number of Keys	: 14
Key Type	: AES
Authentication with changed key necessary	: YES
Allow master key change	: YES
Free directory list without master key	: YES
Free create/delete without master key	: NO
Configuration changeable with master key	: NO

Keys (fixed)

Key 0 is the App master key, Key 1 can change the values of keys 1 to 13

KeyID.AppMasterKey 0	: Diversified according to AN10922 using card UID and AppID
KeyID.AppKey 1	: Diversified according to AN10922 using card UID and AppID
KeyID.AppKey 2	: Diversified according to AN10922 using card UID and AppID
KeyID.AppKey 3	: Diversified according to AN10922 using card UID and AppID

KeyID.AppKey 4	: Diversified according to AN10922 using card UID and AppID
KeyID.AppKey 5	: Diversified according to AN10922 using card UID and AppID
KeyID.AppKey 6	: Diversified according to AN10922 using card UID and AppID
KeyID.AppKey 7	: Diversified according to AN10922 using card UID and AppID
KeyID.AppKey 8	: Diversified according to AN10922 using card UID and AppID
KeyID.AppKey 9	: Diversified according to AN10922 using card UID and AppID
KeyID.AppKey 10	: Diversified according to AN10922 using card UID and AppID
KeyID.AppKey 11	: Diversified according to AN10922 using card UID and AppID
KeyID.AppKey 12	: Diversified according to AN10922 using card UID and AppID
KeyID.AppKey 13	: Diversified according to AN10922 using card UID and AppID

Data File

File ID (hex)	: 0
Full AES Enciphering	: YES
Read Access Key No. (hex)	: 2
Write Access Key No. (hex)	: N/A
Read/Write Access Key No. (hex)	: N/A
Change Access Rights Key No. (hex)	: N/A
File Size (dec)	: 128 bytes
Data storage	: TEXT

File ID (hex)	: 1
Full AES Enciphering	: YES
Read Access Key No. (hex)	: 3
Write Access Key No. (hex)	: N/A
Read/Write Access Key No. (hex)	: N/A
Change Access Rights Key No. (hex)	: N/A
File Size (dec)	: 128 bytes
Data storage	: TEXT

File ID (hex)	: 2
Full AES Enciphering	: YES
Read Access Key No. (hex)	: 4
Write Access Key No. (hex)	: N/A
Read/Write Access Key No. (hex)	: N/A
Change Access Rights Key No. (hex)	: N/A
File Size (dec)	: 128 bytes
Data storage	: TEXT

File ID (hex)	: 3
Full AES Enciphering	: YES
Read Access Key No. (hex)	: 5
Write Access Key No. (hex)	: N/A
Read/Write Access Key No. (hex)	: N/A
Change Access Rights Key No. (hex)	: N/A
File Size (dec)	: 128 bytes
Data storage	: TEXT

File ID (hex)	: 4
Full AES Enciphering	: YES
Read Access Key No. (hex)	: 6
Write Access Key No. (hex)	: 7
Read/Write Access Key No. (hex)	: N/A
Change Access Rights Key No. (hex)	: N/A
File Size (dec)	: 512 bytes (not written during manufacture only later in the field)
Data storage	: BINARY

File ID (hex)	: 5
Full AES Enciphering	: YES
Read Access Key No. (hex)	: 8

Write Access Key No. (hex)	: 9
Read/Write Access Key No. (hex)	: N/A
Change Access Rights Key No. (hex)	: N/A
File Size (dec)	: 512 bytes (not written during manufacture only later in the field)
Data storage	: BINARY