VTAP

Application Note - Read secured data from DESFire cards and tags

Firmware from v2.2.5.0

VTAP50 and VTAP100

Revised July 2024 v1.61

DOT ORIGIN

If you need help to set up or use your VTAP reader, beyond what is contained in this Application Note, then please contact our support team.

Email: **vtap-support@dotorigin.com**

Download the latest documentation and firmware from **https://vtapnfc.com**

Telephone UK and Europe: +44 (0) 1428 685861

Telephone North America and Latin America: +1 (562) 262-9642

If you have any feedback on setting up or using your VTAP reader or this documentation, then please contact our support team. The product is constantly being reviewed and improved and we value feedback about your experience.

Dot Origin Ltd
Unit 7, Coopers Place Business Park, Combe Lane, Wormley
Godalming GU8 5SZ United Kingdom
+44 (0) 1428 685861

Contents

1 Read secured data from DESFire cards or tags

MIFARE DESFire cards may contain a number of applications, identified by an application ID. Each application may contain a number of data files and a number of cryptographic keys, for use with either the AES or 3DES ciphers. Each file is identified with a file ID and may be individually protected, requiring authentication with one of the application keys, for read or write access and for communications security.

To read data from a DESFire card, the `config.txt` file for your VTAP reader must specify the application ID and file ID, where the required data is stored. The VTAP reader supports a number of formats and options to read, decode or output the secure data. To read any protected data you also need to load the appropriate key into one of the VTAP reader's app key slots, and specify in the `config.txt` file the crypto algorithm, the key number (within the card's application) and the corresponding VTAP app key slot, where that key has been loaded.

After looking at reading data from individually secured files on DESFire cards in this section, this Application Note will look at how to **Read data when key diversification is used**, which adds an extra layer to the decoding process.

1.1 VTAP reader configuration to read your secure DESFire cards

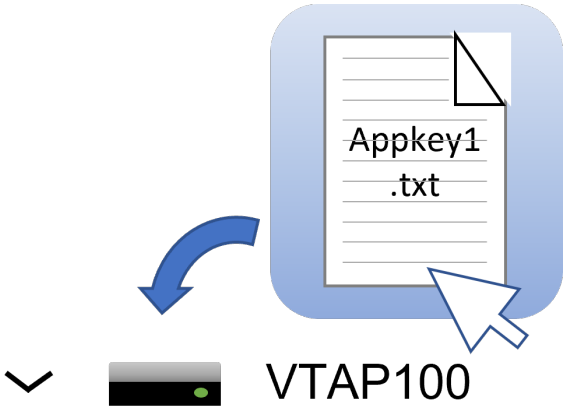
Step 1: Upload necessary DESFire application key(s) to your VTAP reader.

This follows the same approach as when you first uploaded mobile pass key files.

1. Save each of the DESFire application keys you need to use in a file, with the name `appkey#.txt`, where # is replaced with a number from 1 to 9. Each text file should just contain one DESFire application key with 32 hex digits, for example, `key=bd6a15d1039e7527edfd01f37a220f3e`

   Note: You cannot use more than 9 application key files.

2. Load your keys by copying these files onto your VTAP reader. Just connect your VTAP reader to a PC via USB, so it appears as a mass storage device on the PC file system (unless disabled or locked), then you can drag and drop the files.



3. Power cycle the VTAP reader. (Disconnect or eject the drive from the PC then reconnect it.) When you reboot the VTAP reader your key will have been stored in hardware, and will no longer be listed as a file on the device.

Step 2: Add extra lines to the config.txt file to describe the Application ID, appkey and format to use

1. Open the file `config.txt` in a text editor (such as Windows Notepad).
2. Add lines to the file `config.txt`, using your own Application ID, File ID and Key Number. If there is already a line reading `NFCType4=U`, instructing the VTAP reader to read only the UID of DESFire cards, you will need to overwrite that line with the new content.

> **Note:** The VTAP reader expects the `DESFireAppID` to be a 24 bit number formatted as 6 hex digits with the most significant byte first. However, some vendors and software treat the Application ID value as a byte sequence with the least significant byte first, which is the byte order used in communications with the card. If the VTAP reader fails to read your DESFire card application, try reversing the order of the `DESFireAppID` bytes. For example, if `DESFireAppID=F56400` try `DESFireAppID=0064F5`.

Two examples follow, the first where the DESFire data is securely held and requires keys, and the second without cryptography or a DESFire format.

Example: Settings in `config.txt` to read secured data from DESFire cards or tags

```
!VTAPconfig

NFCType4=D          ; Read NFC Type4 cards as DESFire
DESFireAppID=F56400 ; 24 bit value (6 hex digits)
DESFireFileID=1     ; File ID within application (decimal 1 to 255)
DESFireCrypto=3     ; 0 = None; 1 = 3DES; 3 = AES (default)
DESFireKeyNum=1     ; Application key number used for authentication
DESFireKeySlot=1    ; Application key slot number on VTAP
                    ; here use appkey 1
DESFireFormat=1     ; How to interpret the data
                    ; =0 no format
                    ; (set DESFireReadLength and TagReadFormat)
                    ; =1 KEY-ID format (26 bit facility code
                    ; and number, H10301 compatible)
```

If `DESFireCrypto=0` (no cryptography) or `DESFireKeySlot=0` (no key), there will be no authentication or file communications encryption. This will allow unrestricted, plain text file access to some application data, only if this is permitted by the DESFire card configuration.

When `DESFireFormat=0`, you can further control the output by using the settings:

- `TagReadFormat` - to output the payload in either hex (=h, default), ASCII (=a) or decimal (=d).
  - If ASCII is set, each byte is an ASCII character.
  - When decimal is set, the VTAP reader will interpret binary data as a 64 bit decimal value and output ASCII decimal digits. In this case `TagReadLength` should not exceed 4 bytes.
  - For hexadecimal, the VTAP reader will convert binary data to ASCII hex digits with 2 digits per byte.
- `TagWiegandBits` - to set the number of bits output over the Wiegand interface (=1 to 255), where the default is 0, or for automatic detection of bits available use =0 value.

Example: Settings in `config.txt` to read data from DESFire cards or tags without cryptography or DESFire format

```
!VTAPconfig

NFCType4=D
DESFireAppID=2308A1
DESFireFileID=48
DESFireCrypto=0     ; No cryptography
DESFireFormat=0     ; No format, so must set DESFireReadLength and
                    ; TagReadFormat
DESFireReadLength=8 ; Number of bytes to read if DESFireFormat=0
TagReadFormat=a     ; Output payload in ASCII format, with each byte
                    ; interpreted as an ASCII character
TagWiegandBits=64   ; Set the Wiegand output bit length to 64
```

3. Save the amended `config.txt` file and these changes will take effect immediately.

1.2 Read multiple applications or files in the same DESFire card

You may need to read and output values from multiple applications or files within the same DESFire card, where all the applications may have different security requirements.

The VTAP readers can read up to 6 applications within the same DESFire card, access them separately (according to their corresponding security requirements), and output the values, concatenated with a defined separator.

To use this feature, `DESFire...` settings become `DESFire#...` settings, where # is a number from 1 to 6. The number shows which settings form a group for reading each of 1 to 6 values from separate files and or applications on a DESFire card or tag. If you use multiple `DESFire#...` settings the values read will be output together, spaced by the `DESFireSeparator` string. The lowest numbered DESFire read will be first in the output string, then continuing in ascending numeric order.

Note: If a number is not used in `DESFire...` settings, then the VTAP reader would treat those settings as `DESFire1...` For example `DESFireCrypto` or `DESFireFileID` would be considered as `DESFire1Crypto` and `DESFire1FileID`.

Example: Settings in `config.txt` to read multiple applications or files from DESFire cards or tags

```
!VTAPconfig

NFCType4=D

DESFire1AppID=A253C6
DESFire1FileID=0
DESFire1Crypto=3     ; AES (default)
DESFire1KeyNum=1
DESFire1KeySlot=2    ; use appkey 2
DESFire1Format=0
DESFire1ReadLength=12

DESFire2AppID=D90200
DESFire2FileID=1
DESFire2Crypto=0     ; no authentication required
DESFire2Format=0
DESFire2ReadLength=13
```

The output from this DESFire card read will be the two defined application reads, concatenated and with a default comma separator between them:
303038393939353739343937,4D4F4C30303531353930323137

Use `DESFireSeparator` (defaults to ",") to set a separator character(s) between the outputs of all the DESFire applications. Up to 16 characters can be used and URL encoding is also supported.

Example: Settings in `config.txt` to set a custom separator between outputs from multiple DESFire applications, output as ASCII format data

```
!VTAPconfig

NFCType4=D

DESFire3AppID=83A205
DESFire3FileID=1
DESFire3Crypto=0     ; no authentication required
DESFire3Format=0
DESFire3ReadLength=13

DESFire5AppID=C200A1
DESFire5FileID=1
DESFire5Crypto=3     ; AES (default)
DESFire1KeyNum=1
DESFire1KeySlot=1    ; use appkey 1
DESFire5Format=0
DESFire5ReadLength=12

DESFireSeparator=|

TagReadFormat=a
```

The output from this DESFire card read will then be the two defined application reads, concatenated and with a custom | separator between them, presented as ASCII: 086280451106|AOM0844175535

Without the `TagReadFormat` setting the output would be: 414F4D3038343431373535333 5|303836323830343531313036

When using the Wiegand interface, multiple reads are not supported. In this case, only the lowest numbered `DESFire#...` settings will be used, which might not be `DESFire1...`. If only `DESFire3...` and `DESFire4...` settings are defined in `config.txt`, the `DESFire3...` settings would then be used for output over Wiegand.

2 Read data when key diversification is used

In the last section a single app key was used together with the card UID, application and file identifiers to select and decode the secured data in a particular file.

Some cards or passes can be set up so that each one carries a different key, although all are derived from the same master key. This is a feature of DESFire EV1 and EV2 cards, MIFARE2Go passes, Apple Wallet Access passes and others. One form of 'key diversification' scheme to support this is NXP AN10922. Your VTAP reader can decode data from cards or passes which have unique keys, set up in accordance with NXP AN10922 ("Symmetric Key Diversifications" Application Note v2.2 from NXP B.V. 2 July 2019).

If the card or pass UID is also hidden, you will need to provide an additional Privacy key, and Privacy key number, to authenticate in order to read the real UID. This is used together with System Identifier information (up to 16 bytes of data, saved as if it was another key) and the master key, to derive the card's unique read key. This is in addition to the usual settings needed to decode secured data in an encrypted application, described in the previous section **Read secured data from DESFire cards and tags**.

2.1 Extra configuration to support key diversification

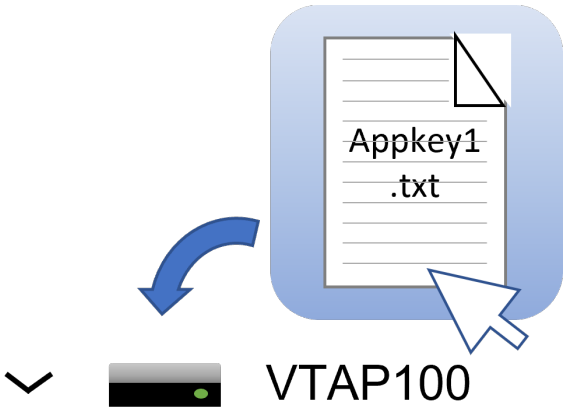
Step 1: Upload Privacy key(s) and System Identifier key(s) to your VTAP reader.

This follows the same approach as when you first uploaded mobile pass key files.

1. Save each of the keys you need to use in a file, with the name `appkey#.txt`, where # is replaced with a number from 1 to 9. Every file needs a unique name. Each text file should just contain one key with 32 hex digits, for example, `key=bd6a15d1039e7527edfd01f37a220f3e`

   Note: You cannot use more than 9 application key files.

2. Load your keys by copying these files onto your VTAP reader. Just connect your VTAP reader to a PC via USB, so it appears as a mass storage device on the PC file system (unless disabled or locked), then you can drag and drop the files.



3. Power cycle the VTAP reader. (Disconnect or eject the drive from the PC then reconnect it.) When you reboot the VTAP reader your key will have been stored in hardware, and will no longer be listed as a file on the device.

Step 2: Add extra lines to the config.txt file to describe the Privacy key and System Identifier key to use

1. Open the file `config.txt` in a text editor (such as Windows Notepad).
2. Add lines to the file `config.txt`, using your own key slots and key number.

Example: Settings in `config.txt` to read secured data from passes cards or tags using NXP AN10922 key diversification

```
!VTAPconfig

NFCType4=D
DESFireCrypto=3             ; Crypto algorithm is AES (default)

DESFireKeyDiversification=1; Use AN10922 key diversification

DESFireAppID=123456         ; The DESFire application ID
DESFireFileID=0             ; The DESFire data file ID within the
                            ;  application
DESFireKeyNum=2             ; Authenticate with key 02 ID within the
                            ;  DESFire application to access the data
                            ;  file
DESFireKeySlot=2            ; The master read key for accessing the data
                            ;  file is in VTAP appkey slot 2

DESFirePrivacyKeyNum=1      ; Authenticate with key 01 ID within the
                            ;  DESFire application to access the card's
                            ;  real UID
DESFirePrivacyKeySlot=1     ; The privacy key for accessing the UID is
                            ;  in VTAP appkey slot 1
DESFireSysIDKeySlot=3       ; The system ID for key diversification is
                            ;  stored in VTAP appkey slot 3
DESFireSysIDLength=6        ; The system ID length is 6 characters
                            ;  (optional - if omitted the length of data
                            ;  stored in the SysID appkey slot is used)
DESFireReadLength=5         ; Read 5 bytes of data from the data file
```

3. Save the amended `config.txt` file and these changes will take effect immediately.

3 About Application Notes

Application Notes address topics of interest to small groups of customers, or topics around the use of a VTAP reader with third-party systems.

The main documents available to support your use of the VTAP50 and VTAP100 are the Installation Guide for your VTAP reader model and the VTAP Configuration Guide. You will find the latest versions of these, and other useful information at **https://vtapnfc.com**.

If you need further help do contact us by email to **vtap-support@dotorigin.com**, or by phone +44 (0) 1428 685861 from Europe and Asia, or +1 (562) 262-9642 from Northern and Latin America.