

VTAP

Application Note - Using OSDP

Firmware from v2.2.5.0

VTAP50 and VTAP100

Revised September 2024 v1.2

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.

Copyright 2024 Dot Origin Ltd. All rights reserved.

No part of this Application Note may be published or reproduced without the written permission of Dot Origin Ltd except for personal use. This Application Note relates to correct use of the VTAP reader only. No liability can be accepted under any circumstances relating to the operation of the user's own PC, network or infrastructure.

Dot Origin Ltd

Unit 7, Coopers Place Business Park, Combe Lane, Wormley

Godalming GU8 5SZ United Kingdom

+44 (0) 1428 685861

Contents

1 Using OSDP	1
1.1 Initialisation	1
1.2 Secure mode only	2
1.3 File transfer mechanism	2
1.4 OSDP custom Commands	2
1.5 VTAP commands permitted in OSDP mode	3
1.6 RS-485 issues	3
2 Send pass payload using OSDP over an RS-485 interface	4
3 Load an OSDP application key	6
4 About Application Notes	7

1 Using OSDP

OSDP is the Open Supervised Device Protocol, which defines a method for secure communication between an Access Control Unit (ACU) and all its Peripheral Devices (PDs), such as the VTAP reader. In this protocol the ACU is always primary and the PDs are subordinate devices.

The VTAP reader Command Interfaces are set up as human interfaces. Using the secure OSDP protocol on interfaces provides an ideal machine interface with the necessary CRCs and integrity checks.

There are four OSDP profiles - Basic, Secure, Smartcard and Biometric. VTAP readers support only the first two of these:

- Basic - which provides a direct Wiegand alternative, to send credentials and control simple LED or buzzer feedback. Credentials are passed in ASCII or raw (Wiegand) format, as a binary number comprised of a bit count and bit stream.
- Secure - which uses an AES 128bit key stored in one of the VTAP reader encryption key slots. Secure includes all the features of Basic with the addition of a secure communications channel.
- Smartcard (not supported by VTAP) - is intended to allow secure information to be sent between ACU and smartcard without action from the intervening reader. This creates a set up similar to a VPN, intended to support security challenges, for example when using US PIV cards.
- Biometric (not supported by VTAP) - extends the smartcard functionality to the secure transmission of fingerprint and other templates between ACU and biometric device without action from the intervening reader.

1.1 Initialisation

Normally, an initial request for data from a PD will be made by the ACU. It will retrieve basic information, such as the device number, IEEE vendor number and its capabilities. If a secure channel is required, the shared key can either be preloaded into one of the 9 app key slots on the VTAP reader or, if supported by the ACU, it can be generated and set by the ACU on first use. The key is needed to set up a secure channel. When the OSDP key slot in the VTAP reader is empty, it is in "initialisation mode" and the default Secure Channel Base Key (SCBK-D) will be used. Any new Secure Channel Base Key (SCBK) set by the ACU (using the `osdp_KEYSET` command) will always overwrite the one being used to support OSDP at that point. The ACU can change this key as often as it likes.

It is an assumption in the OSDP standard that this initialisation will happen on a short cable connection, where the ACU and PD can both be seen and trusted at the time an initial key is shared.

1.2 Secure mode only

To ensure that secure communications remain secure whenever you use OSDP, it is possible to use settings on the VTAP reader (see `Serial2OSDPSecureOnly` below) to require that only the Secure profile is used, after initialisation. If this is not done, it is possible that the implementation of OSDP on the ACU would allow its PDs to fall back to using the Basic profile if Secure credentials failed.

1.3 File transfer mechanism

OSDP can be used to send firmware updates or transfer other files (config.txt, encryption keys, keyboard maps etc) securely. This relies on VTAP reader files having assigned numerical IDs to identify the purpose of the data, used in place of filenames.

These file numbers are specified by the `FtType` parameter within the `osdp_FILETRANSFER` command. The numbers 2 to 127 are reserved in the OSDP specification v2.2 for future use. The VTAP OSDP implementation therefore uses the range of numbers reserved for private use 128 to 255.

VTAP filename	FtType in <code>osdp_FILETRANSFER</code>	VTAP filename	FtType in <code>osdp_FILETRANSFER</code>
CONFIG.TXT	128	APPKEY1.TXT	141
VTAPWARE.DAT	129	APPKEY2.TXT	142
PRIVATE1.PEM	130	APPKEY3.TXT	143
PRIVATE2.PEM	131	APPKEY4.TXT	144
PRIVATE3.PEM	132	APPKEY5.TXT	145
PRIVATE4.PEM	133	APPKEY6.TXT	146
PRIVATE5.PEM	134	APPKEY7.TXT	147
PRIVATE6.PEM	135	APPKEY8.TXT	148
		APPKEY9.TXT	149

1.4 OSDP custom Commands

OSDP permits the definition of a set of custom commands. The custom commands allow for control of many VTAP reader features that are not anticipated in the current version of OSDP. So custom commands are defined for the VTAP reader to permit a subset of its normal serial commands, for example to change to card emulation mode and set card emulation data.

Although LED on/off, timed LEDs and black, red, green, amber, blue, magenta, cyan, and white colours are supported by the VTAP reader, it does not currently support the full extent of `osdp_LED` control (for example switching between different on/off colours). Anything more complex than a simple beep and/or red LED, for example using any other RGB colour, will rely on use of a VTAP custom command.

The `osdp_BUZ` command is well supported by the VTAP reader, as it corresponds closely to the existing VTAP beep command.

1.5 VTAP commands permitted in OSDP mode

VTAP command interfaces can potentially be used for all of the usual VTAP serial commands, even when that the same interface has been assigned to OSDP mode. These potentially allow a host system not using OSDP to communicate with a VTAP over a communication channel that has been set to use OSDP. OSDP requests and standard VTAP (human readable) commands can co-exist on the same port.

For security reasons, when in secure only mode, only two of those VTAP serial commands are permitted: `?osdp` will determine whether OSDP is active on an interface and `?b` will find out whether secure only mode has been selected.

Although OSDP is often implemented over an RS-485 interface, the same protocol can be used over any VTAP reader serial interface.

1.6 RS-485 issues

RS-485 interfaces give rise to a number of potential issues. RS-485 relies on screened twisted pairs of cables, for which **a common ground is essential**. If modern equipment is used, including slew-rate limited transceivers, operating at low voltage and high impedance, there is no need for terminating resistors, which can limit the number of PDs that can be daisy-chained.

2 Send pass payload using OSDP over an RS-485 interface

The OSDP interface allows mobile NFC pass card and tag payloads to be passed straight to an access controller, like data from any other access control card reader. To enable an OSDP interface you will need to make changes to the `config.txt` file.

Note: You can use OSDP on any serial interface. Here it is assumed you are using OSDP over a Serial2 RS-485 interface, as this is the most common scenario, creating an RS-485 OSDP connection between a reader and door controller. To use OSDP on a different interface just substitute `Serial2...` in the examples for `Serial...` or `COMPort...`

1. First ensure that the Serial2 interface is enabled as an RS-485 interface.

Example: Changes to `config.txt` to enable the Serial2 RS-485 interface

```
Serial2RS485=1
Serial2Settings=9600,n,8,1 ; this is the default - but must match
                           ; required interface speed
Serial2Source=A1
```

Here `Serial2RS485=1` sets the Serial2 interface to behave as an RS-485 interface. `Serial2Source=A1` is the default setting to ensure that interface will send data from all passes and cards/tags that can be read. And `Serial2Settings=9600,n,8,1` ensures that the interface speed used by the VTAP reader matches that expected on the RS-485 interface.

2. Then add settings to allow the Serial2 interface to follow OSDP.

Example: Changes to `config.txt` needed to use OSDP on the Serial2 interface

```
; Essential settings
Serial2OSDP=1
Serial2OSDPAddress=0

; Settings for secure channel mode
Serial2OSDPKeySlot=3
Serial2OSDPSecureOnly=0 ; use =1 if you need to enforce secure channel

; Other options
Serial2OSDPFormat=Wiegand ; use =Wiegand or =ASCII credential format
```

These settings in `config.txt`, are specific to control the transfer of data using OSDP:

- `Serial2OSDP` enables or disables use of OSDP on the Serial2 interface.
 - `Serial2OSDPAddress` gives the VTAP reader a numerical address 0 to 126, as a peripheral device under OSDP.
 - `Serial2OSDPKeySlot` points to any one of the 9 available application key slots, loaded by providing a file such as `appkey3.txt`, as the one to be used to hold the OSDP Secure Channel Base Key.
 - `Serial2OSDPFormat` can either be set to ASCII or Wiegand (raw), where the output will be a binary number comprised of a bit count and bit stream. In Wiegand format the other `Wiegand...` settings will determine how that data is formatted, for example setting the bit length and format for pass and tag data. (See the VTAP Commands Reference Guide or VTAP Application Notes on Access Control for more detail.)
 - `Serial2OSDPSecureOnly` can be used to require that only the Secure profile is used, after initialisation. If this is not done, it is possible that the implementation of OSDP on the controller would allow its PDs to fall back to using the Basic profile if Secure credentials failed.
3. After making the necessary changes to your `config.txt` file and saving it, you can connect the VTAP100 to your access controller. (Consult the VTAP100-PAC-485 Installation Guide for wiring information.) You can leave other USB or serial connections in place at the same time, if you want to test the configuration before disconnecting.

Passes will then be read by VTAP100 with data passed direct to your access controller using OSDP.

Refer to the VTAP Serial Integration Guide for more about the Serial2 RS-485 interface.

3 Load an OSDP application key

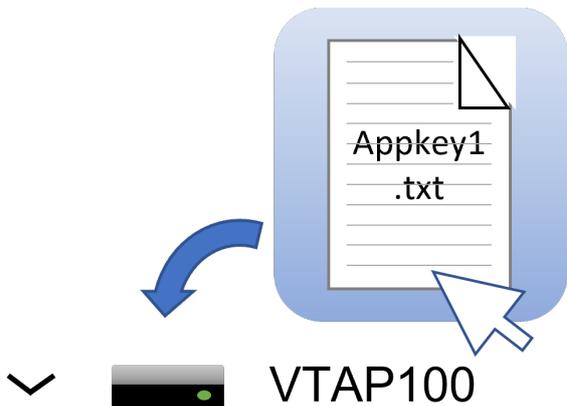
In order to operate in secure mode you may need to load your OSDP key into your VTAP reader, using one of the 9 available application key slots.

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

1. Save the application key 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 application key with 32 hex digits, for example, `key=bd6a15d1039e7527edfd01f37a220f3e`

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

2. Load your key by copying the file 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.

When this is done remember to edit the `config.txt` file, using the setting `Serial2OSDPKeySlot` to point to the key you uploaded by its slot number. For example, if you uploaded a file called `appkey3.txt`, that file is in slot 3, so use `Serial2OSDPKeySlot=3`.

4 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.