astra telematics

Application Note: Driver ID using RFID/NFC Cards

Scope
All devices

Overview
Our vehicle tracking devices can be used with an external card reader to read a variety of RFID/NFC cards for driver ID purposes. This application note contains useful information about using our CR001 card reader with all our devices.

Related Documents
The following documents are recommended reading to accompany this document:

- AT110, AT200, AT210 and AT240 User Guides
- AT110, AT200, AT210 and AT240 Installation Guides
- Astra Communications Protocols K, M & V

The User Guides can be obtained from:

http://www.gps-telematics.co.uk/downloads.htm

The Protocol Description document is available on request by emailing support@gps-telematics.co.uk

Reader & Card Requirements
- CR001 Card Reader
- CB001 Power / Ignition Cable
- CB243, CB113, CB213 or CB203 'plug & play' device cable (to match device)
- Card Compatibility:
    - ISO1443A: Mifare Classic 1k and 4k (incl. EV1), Mini, DESFire EV1, PlusS&X, Pro X, SmartMX, Ultralight, Ultralight EV1, Ultralight C, NTAG2xx
    - SLE44R35, SLE66Rxx (my-d move), LEGIC Advant, PayPass
    - ISO14443B: Calypso, CEPAS, Moneo, PicoPass, SRI512, SRT512, SRI4K, SRIX4K
    - ISO18092 / NFC: NFC Forum Tag Type 1-4
    - Sony FeliCa

CR001 Card Reader Installation
It is recommended that the card reader is powered from an ignition switched power source to avoid battery drain issues whilst the vehicle is parked. Current consumption is approx.. 50mA @ 12V DC.

The CR001 card reader is fitted with 2 connectors, one for RS232 connection to the Astra telematics device and a 2nd for connection to an ignition switched power source.

The RS232 connector (2 way) will mate with the corresponding connector on the device plug & play cable (CB243, CB113, CB213 or CB203)

The power connector (4 way) will mate with our CB001 power cable for termination directly to the vehicle power source (ignition switched), using the RED and BLACK wires.

Device Configuration

Command to configure driver ID source, authorisation, reporting and timeouts.

```
$DRIC,<driver_id_source>,<reminder>,<confirm>,<report_all>,<immobilise>,
<validity_timeout_secs>,<auth_timeout_secs>,<imob_output_state>,
<server_authorisation>,<allow_manual_imob_override>,<reminder_timeout_sec>
```

<driver_id_source>
Our devices support various modes of driver ID. To use RFID/NFC card reader mode with our CR001, set the device driver ID source to 2. Default device configuration is zero (driver ID disabled).

<reminder>
This option can be used to enabled an audible or visible reminder, to help ensure that the driver does not forget to present the ID card for each journey. If the reminder option is enabled, the output assigned to reminder is switched ON whenever the vehicle ignition is turned on, until an ID card is presented. This can be used with our BZ001 external buzzer option. Default device configuration is *reminder* disabled.

<confirm>
This device output can be used to indicate to the driver when an ID card has been read successfully. The output assigned to *confirm* is turned on momentarily. By default, the confirm output is used to drive the LED indicator built into the IB001 ID card Probe. Default device configuration is *confirm* disabled.

<report_all>
Enable this option if you wish the device to create an event / report in response to each and every ID card read by the device. Default device configuration is *report_all* disabled

<immobilise>
Enable this option if you wish the driver ID to be linked to the device immobiliser output and controller automatically based on driver ID. Default device configuration is *immobilise* disabled

<validity_timeout_secs>
Driver ID data will be attached to all journey START and STOP reports until validity expires. If set to zero, the ID card data will become invalid at the next STOP report. Default device configuration is 7200 seconds.

<auth_timeout_secs>
For use when *immobilise* option is enabled. After presenting the ID card, the driver has *auth_timeout_secs* to start the vehicle. The default device configuration is 30 seconds.

<imob_output_state>
The state of the digital output when immobilisation is active.
0 = output OFF for immobilisation. 1 = output ON for immobilisation. Default is 0.

<server_authorisation>
This option allows the acceptance of each driver ID to be controlled from the client server for vehicle immobilisation purposes. The commands required for this feature are described in the Authorised Driver Implementation section below.

<manual_imob_override>
Allows manual over-ride of the device immobilizer output using $IMOB or $SDIG commands. Default is 0 (not allowed).

<reminder_timeout_sec>
timeout on reminder buzzer in seconds. Default is zero, for an indefinite timeout.

Note that if the card reader has been connected as recommended then the ignition must be switched on first before a card can be read. The card reader will be ready to read cards as soon as it is powered up.

All supported cards hold an identification number between 4 and 7 bytes length. When a card has been read this data is reported with each journey START and STOP report (see appropriate protocol description document, available on request from Astra Telematics).

Assignment of Device Digital Outputs

Use the CDOP command to assign specific digital outputs of the device to a given application.

$CDOP,<output-number>,<application>

<Application>	Description
0	Not assigned
1	Immobiliser
2	Reminder (driver ID)
3	Confirm (driver ID)
4	Driver Behaviour - yellow
5	Driver Behaviour - orange
6	Driver Behaviour - red

Examples:

$CDOP,3,1	use digital output 3 for immobilisation.
$CDOP,2,3	use digital output 2 for confirm.
$CDOP,1	Will display the application assigned to digital output 1
$CDOP	Will display the available options for all applications

Note: applications can be assigned to only one digital output. If an application has been assigned to a digital output and then later assigned to a different one, the previous assignment will be set to zero (not assigned).

Authorised Driver Implementation

The device will store a list of up to 50 approved cards and up to 50 declined cards.

Each time a 'new' card is read (i.e. not currently in the approved list), the device will query the host server for approval to accept the new card. This process should take approximately 10 seconds. Cards approved by the host will be added to the approved list and when presented again in the future they will be immediately authorised by the device.

Cards that are declined will not be added to the approved list and will not allow the vehicle to be started. These are stored in a declined list. Declined cards send a query to the host so that if they are changed to approved in future they will be added to the approved list. Cards previously approved can be removed from the approved list by the host.

If there are no communications with the host server, approved cards will allow the vehicle to be started and declined cards will not allow the vehicle to be started. Unknown cards will

be temporarily allowed to start the vehicle and approval will be requested as soon as communications resume. If declined at that point, the vehicle will be immobilised.

If the approved list becomes full and a new card is presented and authorised, the oldest card will be removed from the list to make room for the new one. The oldest card is based on the last time that the cards were presented, so regularly used cards should never be removed from the approved list.

The device can re-request authorisation from the server of all cards in the approved list periodically.

Command Descriptions

In the command descriptions the <family-code> and <serial-number> are formatted as follows:

Argument	Format
<family-code>	Card first ID byte, fixed length, 2 hexadecimal digits (leading zeros), e.g. 01. For a 4 byte ID this will always be 00.
<serial-number>	Card ID bytes 2 to 7, fixed length, 12 hexadecimal digits (leading zeros), e.g. 0000125408C9. For a 4 byte ID the first digits will always be 0000.

The following table describes the commands. The first command is from device to host whilst the rest are from host to device.

Command	Description
$DRID,<model>,CHECK,<imei>,<family-code>,<serial-number>	Device requests card authorisation from host
$DRID,APPROVE,<family-code>,<serial-number>	Host approval of card
$DRID,DECLINE,<family-code>,<serial-number>	Host declines card (unknown)
$DRID,ADD,<family-code>,<serial-number>	Host request to add card to approved list
$DRID,REMOVE,<family-code>,<serial-number>	Host request to remove card from approved list
$DRID,CLEAR	Host request to delete approved and declined list
$DRID,CLEAR,WHITE	Host request to delete approved list
$DRID,CLEAR,BLACK	Host request to delete declined list
$DRID,BLOCK,<family-code>,<serial-number>	Host request to add card to declined list
$DRID,VERIFY,<hours>	Host request to set the device whitelist verification period (0-65535). 0 disables the request

For example:

$DRID,AT110,CHECK,351777042187300,01,0000125408C9