



oti DUKPT Demo User Manual

Version 1.1



Notice

This manual and related files contains intellectual property, including but not limited, to trade secrets and know-how, operation procedures and production procedures that belong solely to OTI – On Track Innovations LTD.

Disclosure and/or use and/or production of any part of the above are strictly forbidden, except under a written license from OTI.



Revision History

Version	Description	Date
1.0	First version	2014-01-22
1.1	Editorial changes	2014-01-27

Table of Contents

REVISION HISTORY.....	2
TABLE OF CONTENTS	2
1. Background	3
2. Intended Audience	3
3. Open Reader Connection	3
4. Setup Key-Encryption-Key.....	4
5. IPEK Settings	5
6. Tag Lists.....	7
7. Poll EMV.....	8
8. Firmware Version	9
9. SAM – Factory Settings.....	9
10. Save Output Log	9
11. Clear Log.....	10

1. Background

- **oti Dukpt demo** is a Windows application that demonstrates the use Dukpt based encryption with oti Saturn 6500 payment Reader.
- **Configuration:** The application leads the user through the process of configuring the Reader with the Dukpt-related keys.
- **Transaction:** The application can also instruct the Reader to perform a payment transaction and return the card information encrypted. The application then **decrypts** the data and presents it to the user in both Encrypted and decrypted forms.

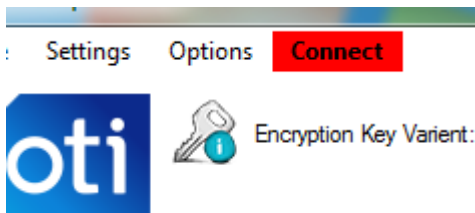
2. Intended Audience

- This manual is intended for terminal integrators wishing working on Saturn 6500 integration.

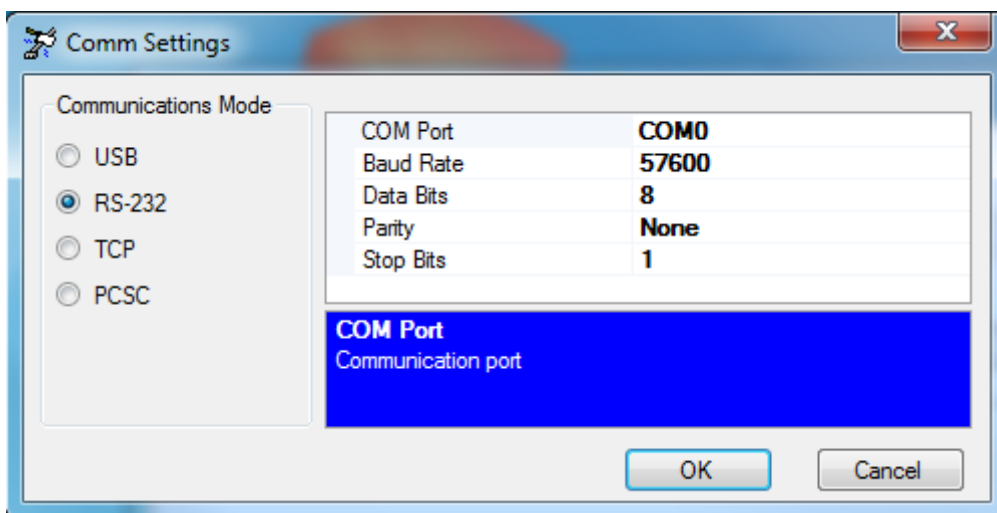
3. Open Reader Connection

While stating, the application will try to connect to the first Reader that responds.

When the application is disconnected from the Reader, the red "**Connect**" button appears in the menu bar.



Clicking on it will try to automatically detect a Reader. if automatic detection fails - a manual connection form will appear:



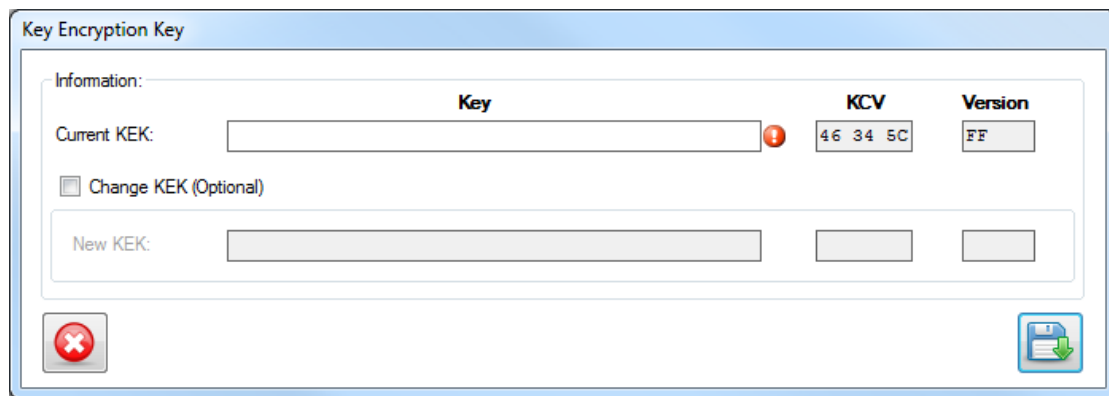
Fill the communication properties manually and click **"OK"**.

Once the application is successfully connected to the Reader, the red **"Connect"** button changes to green **"Disconnect"** button:




4. Setup Key-Encryption-Key

In order to send IPEKs (Pin pad \ Reader), the Key-Encryption-Key (KEK) should be defined first.



The default KEK is: 01 02 03 04 05 07 08 08 07 06 05 04 03 02 01

Default KEK KCV: 46 34 5C

After filling the **"Key"** field – if it matches the KCV read from the Reader – the red error indication () should disappear. If it doesn't – hover the mouse pointer over this blinking icon. The tooltip will help detecting and fixing problems.

Once all errors are solved – click the Save button (right down). it will store the KEK typed for use when sending IPEKs to the Reader.



4.1. Changing KEK

Changing KEK done by checking the **"Change KEK"** option:

☐ Change KEK (Optional)

After checking this option, the new KEK fields are enabled:

☒ Change KEK (Optional)

New KEK:	<input type="text"/>	<input type="text"/>	<input type="text"/>
----------	----------------------	----------------------	----------------------

Fill the new KEK (left field) and KEK version (right field). Once complete, verify that no blinking error marks appears near the input fields. If there are no errors – click the save button. This will send the new KEK to the Reader.

5. IPEK Settings

IPEK Settings form contains information about Reader IPEK and Pin-Pad IPEK.

Reader IPEK is used by the Reader to encrypt clearing data.

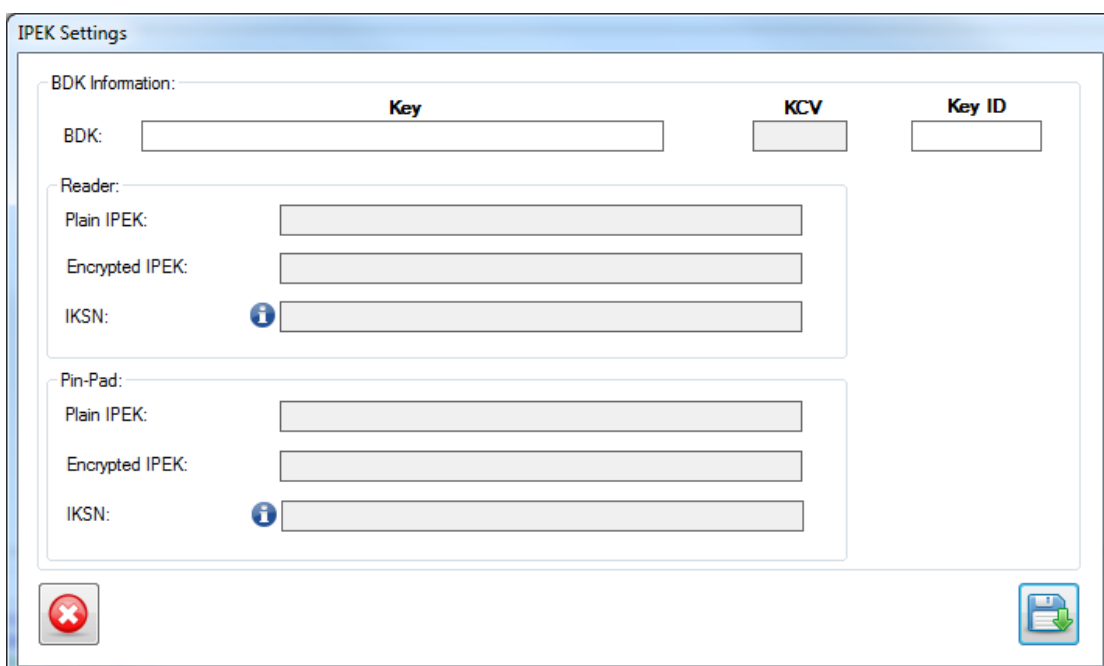
Pin Pad IPEK is used by the Reader to decrypt Offline-PIN: if the card requests Offline-PIN – then the Reader expects that Offline-PIN to be encrypted by the PIN-Pad's IPEK using Dukpt.

This information contains 3 parts for each IPEK key:

1. Plain IPEK: The IPEK auto-generated from BDK.
2. Encrypted IPEK: The Plain IPEK encrypted with KEK.
3. IKS: Additional required information for DUKPT encryption.



Fill those fields:



- Key: 16 hex-bytes. Don't use weak keys.
- Key ID: 21 bits. Total 4 bytes. Maximum value: 07 FF FF FF





After filling the "**Key**" field and the "**Key ID**" field, the application will generate the other fields.

Note that auto-generated information may be different from the information on Reader \ pin-pad. In this case, the application will present a warning icon near the "**Plain IPEK**" fields. For Example:

Reader:	
Plain IPEK:	42 59 C0 07 94 D3 C0 86 05 2A F7 06 3E 40 E1 EF 
Encrypted IPEK:	C4 94 55 69 85 F9 4A BE 70 37 FB 8C D9 63 82 7D
IKSN:	 FF FF FF FF FF FF FF E0 00 00

Pin-Pad:	
Plain IPEK:	D6 48 2B FA 0B 51 4F 23 5C AC 93 7F 6E BE 36 D4 
Encrypted IPEK:	0E 45 4F 4B 42 5F 29 CA D8 95 6C FC 17 51 DE 3C
IKSN:	 FF FF FF E0 20 40 60 80 00 00

After IKSN parameter was generated, the application shows a summary of how this value was calculated. The description is shown in a tooltip. Move the mouse pointer above the information icon ():

IKSN:	 FF FF FF FF FF FF FF E0 00 00
Pin-Pad:	<div> "07-FF-FF-FF" - Key Id. "FF-FF-FF-FF" - Reader Serial Number "00-00-00" - Encryption Counter </div>
Plain IPEK:	

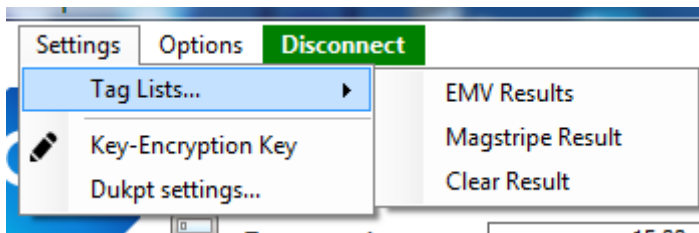
Click on the save button to send the new IPEKs to the Reader:



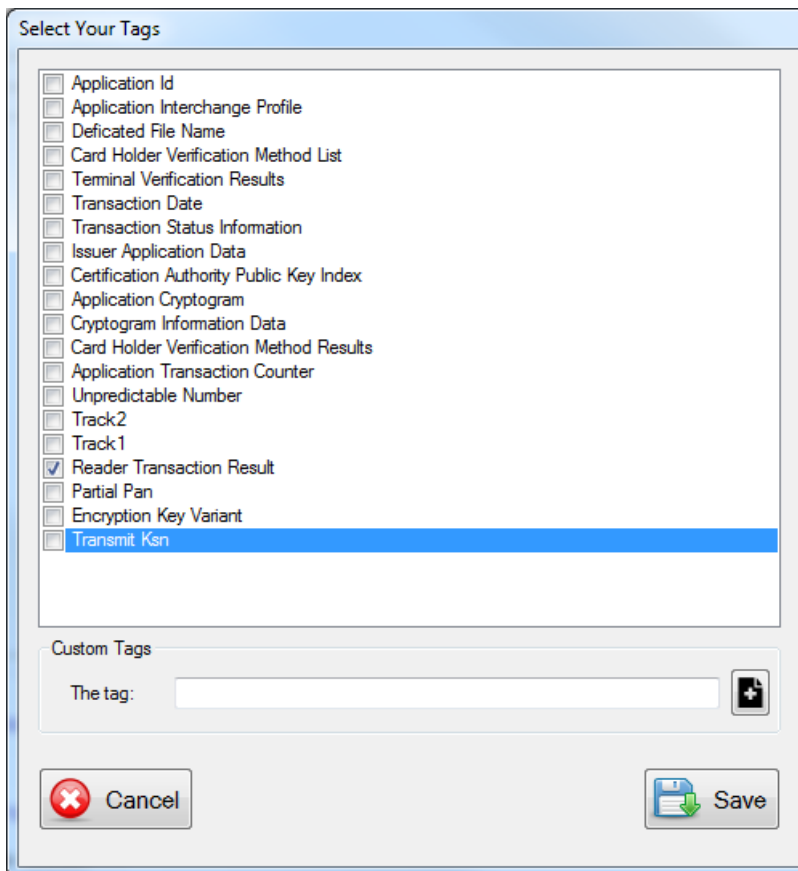
6. Tag Lists

On "Poll EMV" command – the Reader returns various data objects. The user can control which data objects are returned by setting the Reader's Tag lists. 3 Kinds of Tag lists available:

1. EMV Result – data objects to return after an EMV transaction.
2. Magstripe Result – data objects to return after an Magstripe transaction.
3. Plain Result – data objects that won't be encrypted with DUKPT.



In order to edit those tag lists, select one of those results-lists (EMV, MagStripe or Clear) from the Settings -> Tag Lists sub menu:



Check the required tags and click the Save button.

Note: The tag "Reader Key Variant" of the "Plain Result Tag List" is mandatory.

7. Poll EMV

Once the application is synchronized with the Reader (i.e. has the same keys), the **"Poll EMV"** button becomes enabled. Clicking it tells the Reader to perform a payment transaction.

Fill the transaction amount number:

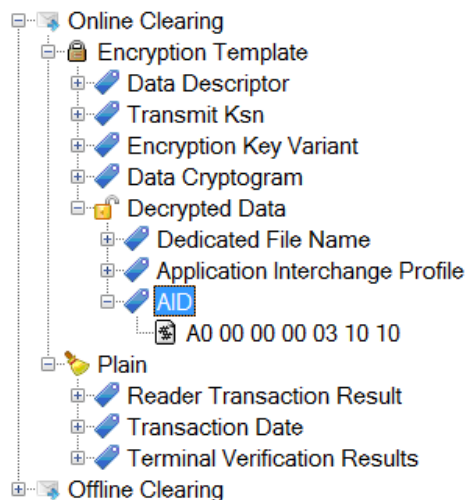


Transaction Amount:

Click the **"Poll EMV"** button:



After clicking this button – the Reader will wait for a payment card. Place a card on the Reader. The Reader will beep and then the application will display a tree view in the middle of the screen. This tree should look similar to this one:



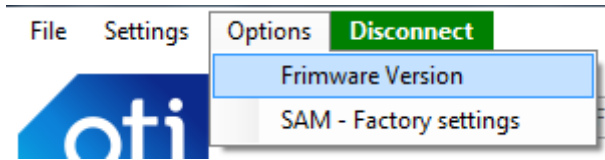
The root element type depends on the **"Reader Transaction Type"** object. In this example, There are two clearing elements: Online and Offline.

For each clearing message from the Reader – the application will display an **"Encryption Template"** node that contains encrypted data and key metadata. Inside this node the application also displays the decryption of the encrypted message.

The **"Plain"** node contains tags that were transmitted from the Reader in clear text.

8. Firmware Version

This command prints the current firmware version into the log.

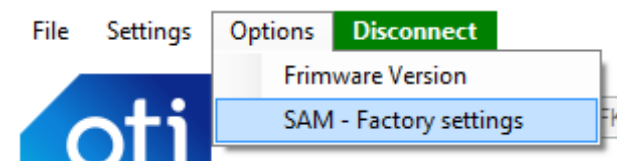


The application displays the result in the log windows (bottom of the screen):

```
Log
23/01/2014 15:48:57: Getting firmware version...
23/01/2014 15:48:57: >> 02 0A 00 3D DF 4E 01 01 A4 03
23/01/2014 15:48:57: << 02 21 00 3D FF 01 18 DF 4E 15 41 52 4D 20 50 4D 54 20 30 34 30 35 30 36 20
30 6E 2E 2E 2E 00 3C 03
23/01/2014 15:48:57: Firmware version: ARM PMT 040506 On...
```

9. SAM – Factory Settings

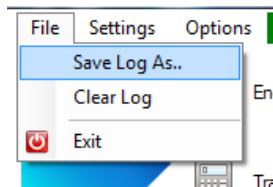
Reset SAM settings and delete IPEKs.



After clicking the button, wait a few seconds until the Reader finishes reloading.

10. Save Output Log

Saving the application output log by clicking the "Save Log As..." button (under the "File" menu).

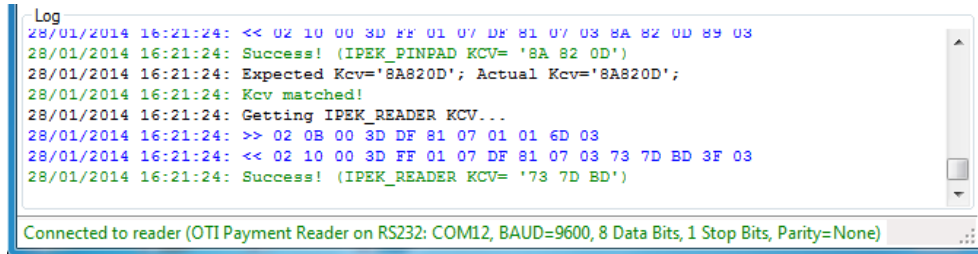


After clicking the button, a save file dialog will pop-up. Select your save location and click the "Save" button.

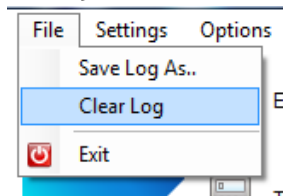
The output file format is "RTF" (Rich Text File). You can open and edit this file with "Microsoft WordPad", "Microsoft Word" or any other RTF compatible application.

11. Clear Log

This application outputs all its log messages into the "Log" area in the bottom of the main form.



It's possible to clear this area by clicking the "**Clear Log**" button (under the "**File**" menu).



After clicking the clear button, the "Log" area will be cleared.