**For more information please contact support@innovative-technology.co.uk**

## eSSP Software Development for Host Applications

Smiley Secure Protocol - SSP is a secure interface specifically designed by Innovative Technology to address problems experienced by cash handling systems. eSSP (encrypted SSP) adds an encryption layer using an AES (Advanced Encryption Standard) algorithm which uses a 128-bit key for an advanced level of security.

Innovative Technology have various software developer kits to assist when implementing eSSP into kiosks, change machines, amusement or gaming applications. These comprehensive Software Development Kits have been created for the complete, current ITL product range to ensure that integration is as rapid and straightforward as possible, even with limited programming experience.

Our current SDK range includes:

C# .Net (ITLLib.dll library version 1.0.0.3)
- Bank Note Validator v1.3
- NV11 v1.3
- Smart Payout v1.8
- Smart Hopper v1.8
- Bank Note Validator and Smart Hopper v1.3
- NV11 and Smart Hopper v1.3
- Smart Payout and Smart Hopper v1.4


C++ (ITLSSPProc.dll library version 1.2.7)
- Bank Note Validator v1.0
- NV11 v1.0
- Smart Payout v1.0
- Smart Hopper v1.0

Multiple unit SDKs will be available for C++ in the near future.

All these SDKs include libraries containing methods to handle ports, negotiate encryption keys, construct packets and encrypt commands sent to the validator (encrypted or plain).

The SDKs contain full example source code showing the recommended way to interface with Innovative Technology products. These examples are tailored specifically for our individual product ranges to eliminate confusion and include demonstrations of interfacing with multiple units in one application.

All Windows Software Development Kits are provided as a Visual Studio 2010 project ensuring they are as current as possible, however if an earlier version is required please contact us. Linux C++ libraries and example source code are also available.

To accompany the Software Development Kits full documentation is available. This documentation describes the process of implementing your software to communicate with ITL products and provides a description of how to use the libraries provided in the Software Development Kits.

**For more information or specific requests, please contact your local support office or email: support@innovative-technology.co.uk**

**Newly released datasets – June 2012**

| Country | Code | Reason | Validator |
|---|---|---|---|
| Australia | AUD02 | New dataset | BV20 |
| China | CNY02/03/04 | Improved acceptance | NV10 / USB |
| Russia | All applicable | 500 and 5000 Ruble notes added | NV9 / USB<br>NV10 / USB |
| Russia | RUB02/03 | 5000 Ruble note added | NV200 |
| Russia | All applicable | 2010 issue 500 Ruble note added | BV20 / BV50 / BV100 |
| USA - Euro | U0007/8 | New datasets | NV10 / USB |

## Banknote validator protocols explained

The banknote validator communicates with its host machine via a protocol that determines how the validator and the host machine transfer information. The host machine generally controls the validator by enabling it to accept banknotes and then interpret signals from the validator, allowing the host machine to determine the value of the note being read. Listed below are various available protocols that vary in terms of complexity, security and implementation. Innovative Technology's own protocol SSP (Smiley Secure Protocol) is a group 3, recommended protocol with increased security.

### *Group 1 Protocols*

***1. Parallel.***

This is a basic 4 wire interface system where each note is recognised as a signal on an individual wire. There are four corresponding inhibit / enable lines on the validator so that individual note denominations can be selected. This interface provides a signal which is 100ms active low with the vend line dependant on the note that has been accepted. The host machine requires a pull up resistor, as all validator outputs are open collector. There is also an option to include an escrow control line from the host machine to the validator.

***2. Binary.***

Allowing up to 15 individual channels to be programmed into the validator the output signals are provided as a binary number representation on up to 4 output pins. It is only possible to Inhibit / enable a maximum of 4 individual channels. This interface also provides signals which are 100ms active low with the vend lines dependant on the note which has been accepted. The host machine requires a pull up resistor as all validator outputs are open collector. This interface also has the option to include an Escrow control line from the host machine to the validator.

***3. Pulse.***

This interface system allows up to 15 individual channels to be programmed into the validator. The output signals are provided as a discreet number of pulses on a single pin. It is only possible to inhibit/enable a maximum of 4 individual channels. This interface also provides signals which are 100ms active low, where each denomination can be set to send a specific number of pulses. The host machine requires a pull up resistor as all validator outputs are open collector. This interface also has the option to include an Escrow control line from the host machine to the validator.

## Group 2 Protocols

### 4. Serial Input / Output (SIO).

This interface has an increased level of control and protection as compared to those in Group 1. This protocol is based on a single byte command and response system. The host machine issues its command to the validator which then responds with its own message. This system does not incorporate error checking or encryption. The speed of the communications can be selected as 300 baud or 9600 baud.

## Group 3 Protocols

### 5. SSP (Smiley Secure Protocol).

This interface represents a high level of security for banknote validators, incorporating error checking and is Innovative Technology's own secure protocol. The validator communicates with the host machine by responding to a Poll command, the validator then sends a packet (a number of bytes) of data to the host machine. This packet of data contains a checksum which is sent from validator to host with the host machine then calculating its own checksum from the packet of data, which must agree with the transmitted checksum. The data also includes the validator serial number information to remove the risk of swapping out the validator for a different device. This serial protocol gives improved security from manual interference, compared with the group 1 protocols. There are sample VB code examples available from ITL as well as a full user manual on the implementation of SSP.

### 6. ccTalk.

This interface is also a secure communications protocol and is widely used in gaming machines. Data is further protected by including a 6 bit encryption key protecting data transferred between host and validator from external interference. The ccTalk protocol is one of the special interfaces programmed on ITL validators. Full details of the ccTalk protocol can be found at www.cctalk.org. The details of the encryption coding can be obtained on signing an NDA with ITL.

### 7. MDB.

This interface protocol is used predominantly on vending machines. This protocol allows multiple devices on the same bus eg. banknote validator, coin acceptor and coin hopper, controlled by the system on the host machine. The MDB protocol requires a special hardware adaptor to be included between the validator and the host machine. There are many interpretations of the MDB protocol and it is necessary to check with ITL that the MDB protocol which has been implemented on the note validator is actually compatible with the MDB controller board in the machine.

### 8. Other Protocols

Contact support@innovative-technology.co.uk for details or implementation of any other specific machine protocols.