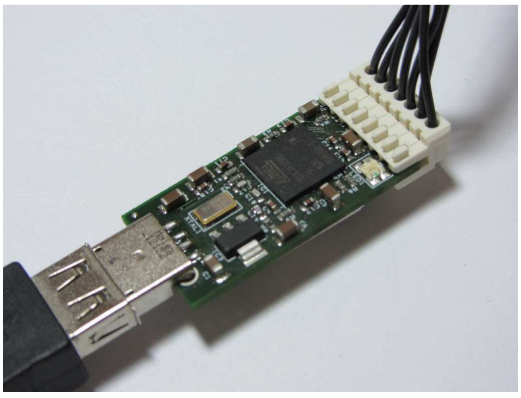
Crypto Stick Storage



Manual

Prototype

Crypto Stick Storage

Version 0.2

Document history

Version	Date	Description	Author
0.1	25.07.13	Initial start	R. Böddeker
0.2	09.05.14	Start the documentation of new interface	R. Böddeker

Content

Intro

This document is on the way to get the user manual for the Crypto Stick Storage. It's on the way …

Benefits

- 100% Open Source software and hardware; open interfaces for easy integration
- Hardware-encrypted 32 GB mass storage (AES-256). Read/write speed of up to 6 MB/s.
- Hidden volumes and plausible deniability
- One Time Passwords allow secure two-factor-authentication with Google, Dropbox, Tumblr, Amazon Web Service and many more websites compatible to Google Authenticator.
- Secure key store for data and email encryption (e.g. GnuPG, OpenPGP, S/MIME), user authentication (e.g. SSH), document signing etc. based on the high-secure OpenPGP Card.
- Works with Windows, Linux, MacOS X
- Firmware updates can be applied easily

Important information's for a quick start

The administration program (CryptoStickGUI.exe) to access the Crypto Stick Storage is on the unencrypted volume of the Crypto Stick Storage. You find it in the subdirectory of your OS.

The default PINs of the OpenPGP card are unchanged.

The user PIN is	123456
The admin PIN is	12345678

Please change the admin and user PIN at the first usage.

The maximal password/PIN length is 20 chars.

Please initialize new keys by start the option "Init encrypted volume" or "Destroy encrypted volume" in the submenu "Configure".

The encrypted / hidden volumes aren't formatted. For high access rates format with FATex, 32 kB block size or greater.

For high security you can fill the encrypted volume with random number by the option "Fill encrypted volume with random chars" in the submenu "Configure/Special Configure".
Warning this function runs very long, approximately over 1 hour for 32 GB. You can disable is message by the menu point "Clear – Fill encrypted volume with random chars"

LED's

Green LED	Smartcard access active
Red LED	SD card read access active
Green/red LED	SD card write access active

Command line options

Special functions are activated by starting the administration program with command line options:

-configAll

Enables the “Special Configure” submenu with the menu entries
- “Enable firmware update”
- “Export firmware to file”
- “Fill encrypted volume with random chars”
- “Set readonly unencrypted volume”

-lockHardware

Enables the menu entry “Lock stick hardware” in the “Configure” submenu. This enables a CPU hardware lock to protect the Crypto Stick Storage against hardware debugging. After activation you can’t update the firmware by software any more.

-debug

Enables a local debug log for the GUI.

-debugAll

Enables a debug log, same as the “-debug” option but with a poll function to get a debug log from the Crypto Stick firmware when a special firmware is flashed. This firmware is used only for development and not available.

-PWM

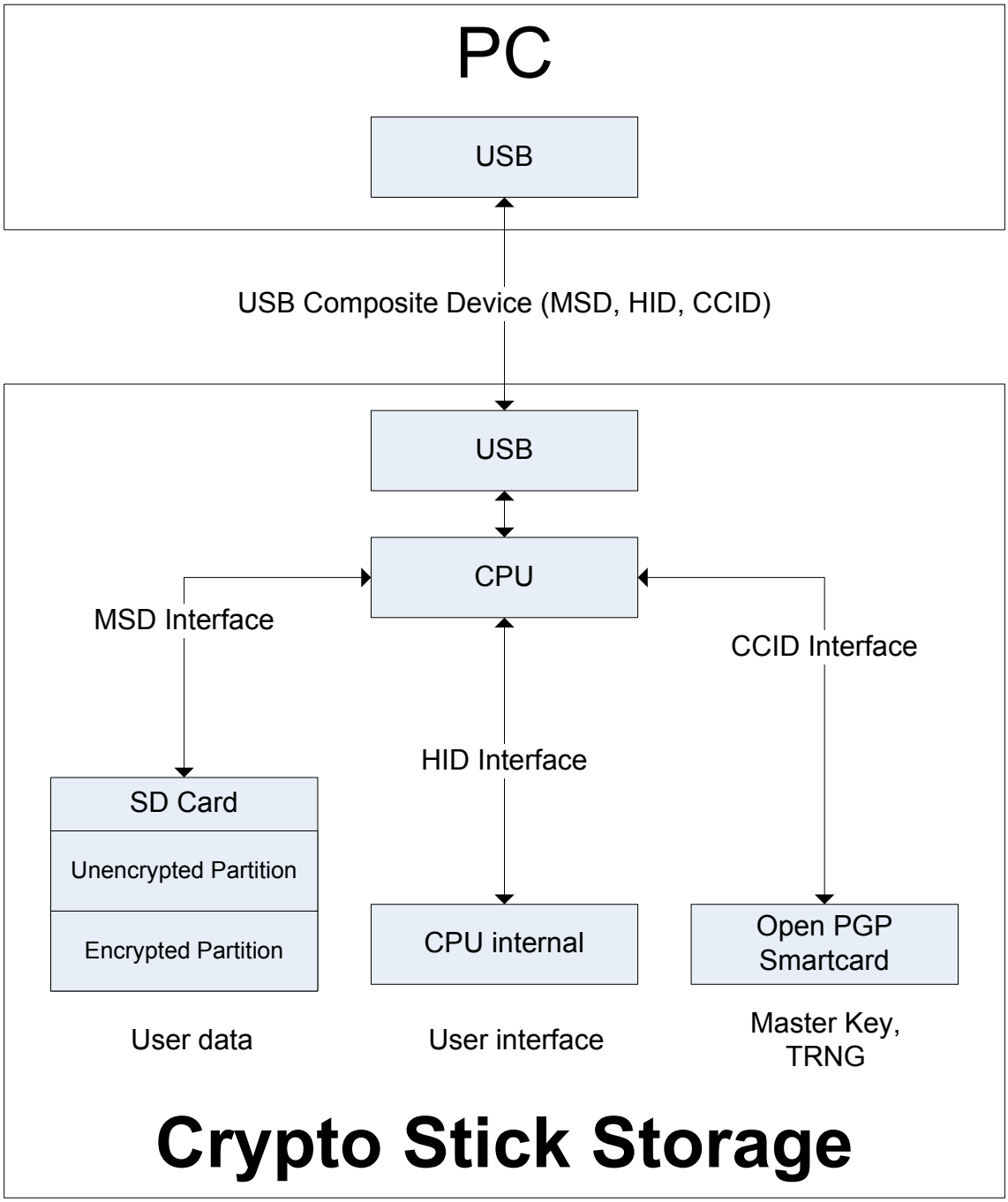
This option enables a secure way to enter a PIN in a monitored area.
For further information go to chapter “”

Architecture of the Crypto Stick Storage

The Crypto Stick Storage communicates with the PC via the USB interface. The USB interface connects 3 kinds of devices:

MSD device	Used for mass storage access
HID device	Used for administration of the crypto stick storage
CCID device	Used for smartcard access

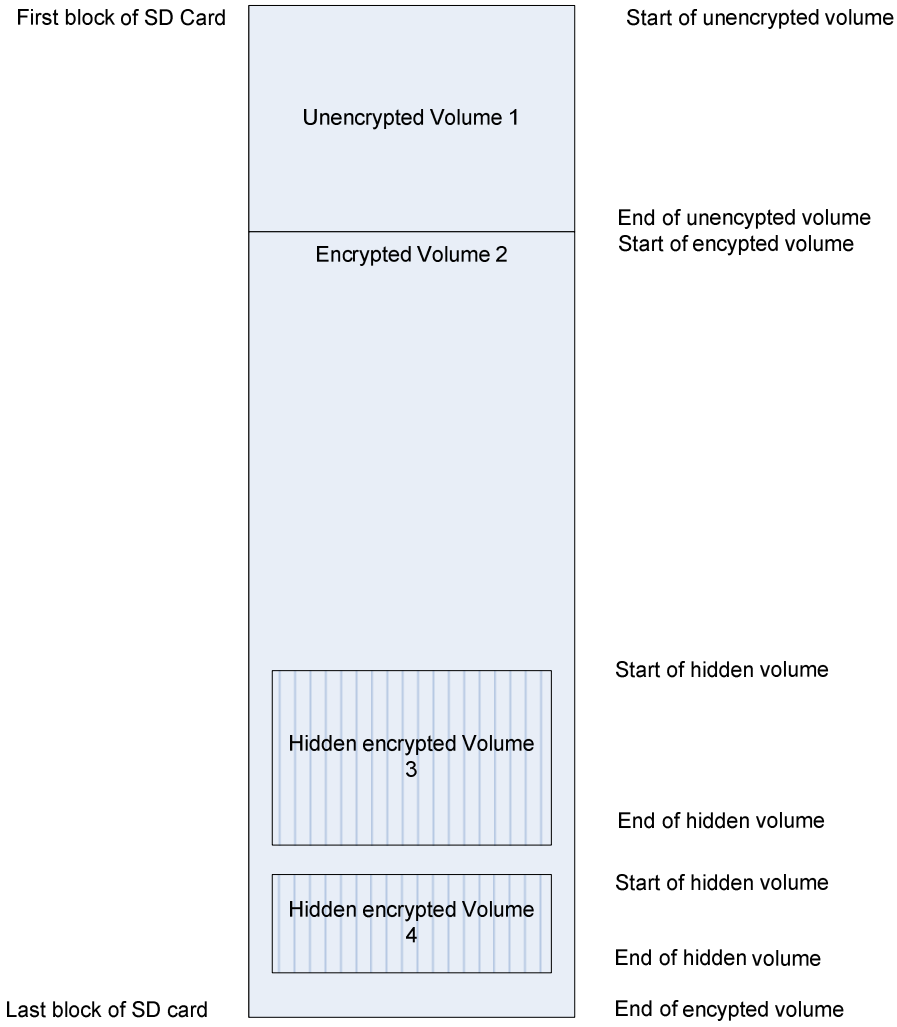
For administration and enabling the encrypted volumes you had to start a program that is delivered with the Crypto Stick Storage. The program was developed under QT.



Volumes of the crypto stick storage

Unencrypted Volume	Small volume which contains the PC software
Encrypted Volume	The “normal” encrypted volume
Hidden Volume	A hidden encrypted volume

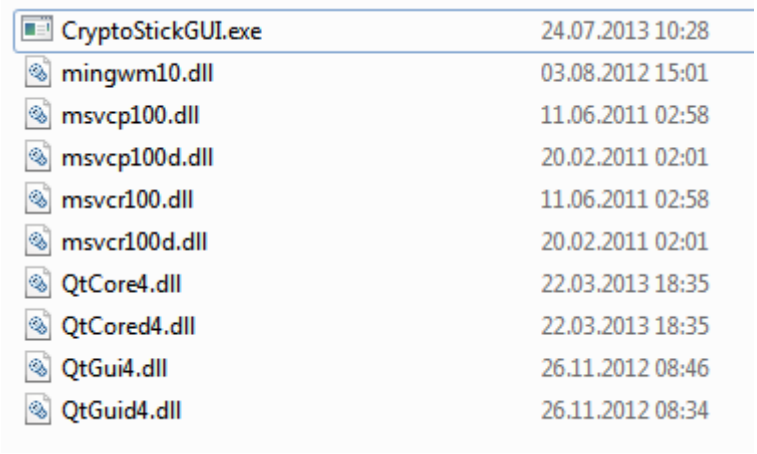
Example



Start of the administration program

Windows 7, XP
You can start the user interface for the CryptoStick direct from the unencrypted volume with the program “CryptoStickGUI.exe”

The content of the unencrypted volume is:



For development requirements the debug dll’s from QT are also includes.
In the beta stage the Software was built with debugging information’s.

Windows

After the start of the CryptoStick user interface you see the CryptoStick logo in the taskbar.
If it doesn’t appear it could be hided.

When you click on the logo a popup menu show you the connection state of the CryptoStick:

Unconnected state

This appears when the CryptoStick is not connected or building up the connection.

Connected State

Menu entries for the connected CryptoStick:

Unlock encrypted volume

This entry unlocks the “normal” encrypted volume. When you select this entry you had to enter your user password of the OpenPGP smartcard. To verify your input, you can select “Show password” to see your entered chars.

By pressing “OK” the password is send to the Cryptostick. During the processing time the state of the Cryptostick is displayed.

When the password was correct, the response dialog closed and the encrypted volume is accessible. In the menu the entry “Unlock encrypted volume” change to “Lock volume”.

Warning
If you change the SD card or compute a new encryption key, you had to format the volume.

If the password entry fails, the response dialog stays with an error message.

Unlock hidden volume (beta test)

This entry was show in the beta test stage for an easier access. Target is to unlock a hidden volume with no hind of their presence.

Attention:
Before you can unlock the hidden volume you had to unlock the encrypted volume.
Unlocking of the encrypted volume enabled the smartcard to decrypted keys for the hidden volumes.

This entry unlocks the hidden encrypted volume. When you select this entry you had to enter the password of the hidden volume that you want to enable. You can define up to 4 hidden volumes.
For further information see point “Setup hidden volume”.

To verify your input, you can select “Show password” to see your entered chars.

By pressing “OK” the password is send to the Cryptostick. During the processing time the state of the Cryptostick is displayed.

When the password was correct, the response dialog closed and the encrypted volume is accessible. In the menu the entry “Unlock hidden volume” changes to “Lock hidden volume”.

Attention:
If you change the SD card or create a new hidden volume, you have to format the volume.

If the password entry fails, the response dialog stays with an error message.

Sub menu “Configure”

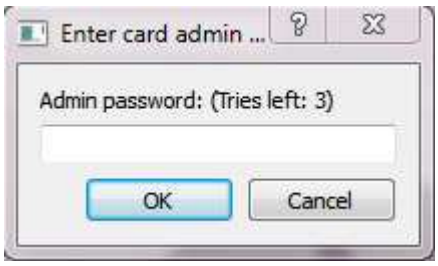
Configure OTP	Configure one time passwords
Change user PIN	Change user PIN of smart card
Change admin PIN	Change admin PIN of smart card
Setup hidden volume	Setup hidden volumes
Destroy encrypted volume	Destroy encrypted volume
Get stick status	Get the actual stick status

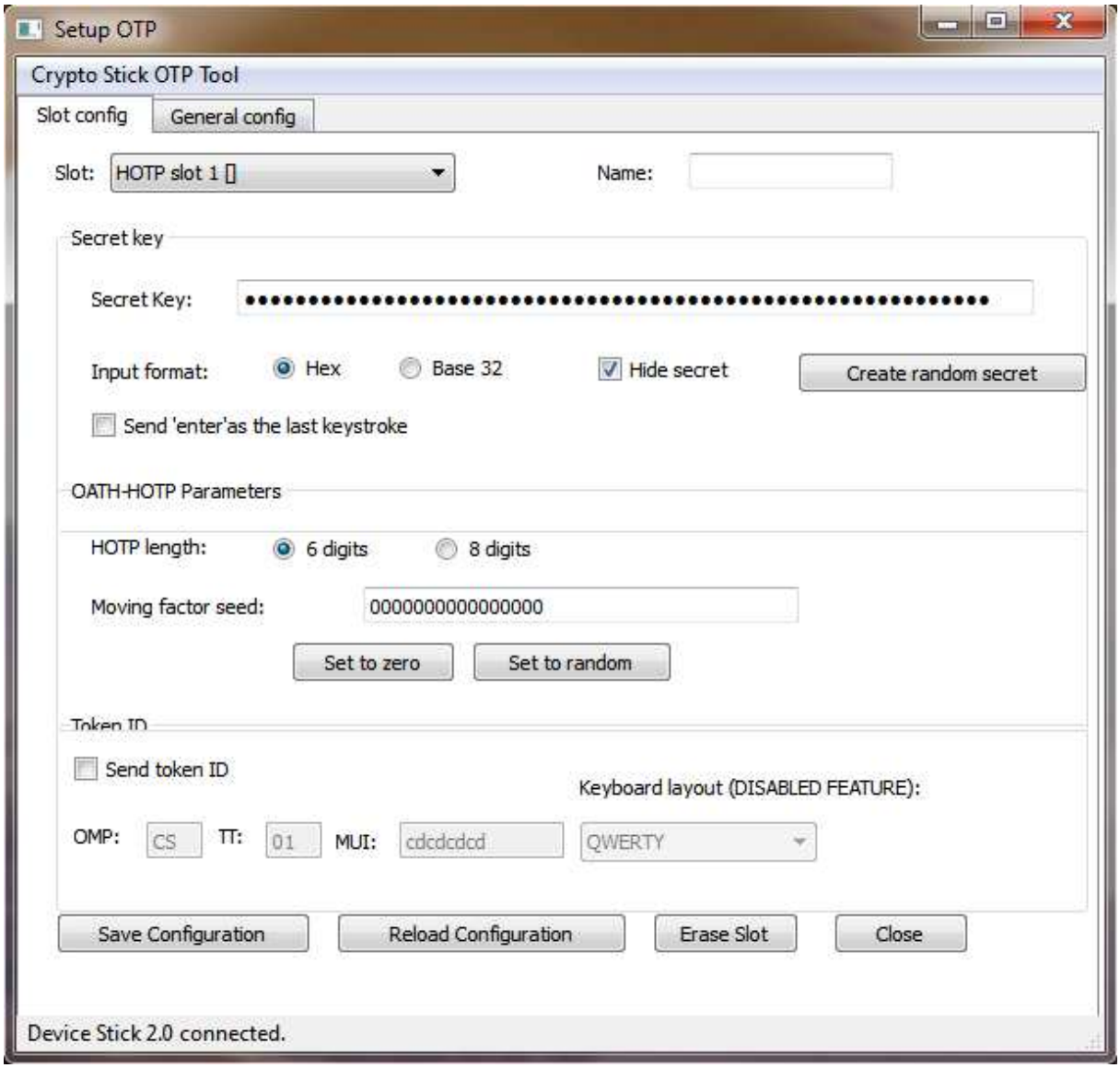
Configure OTP

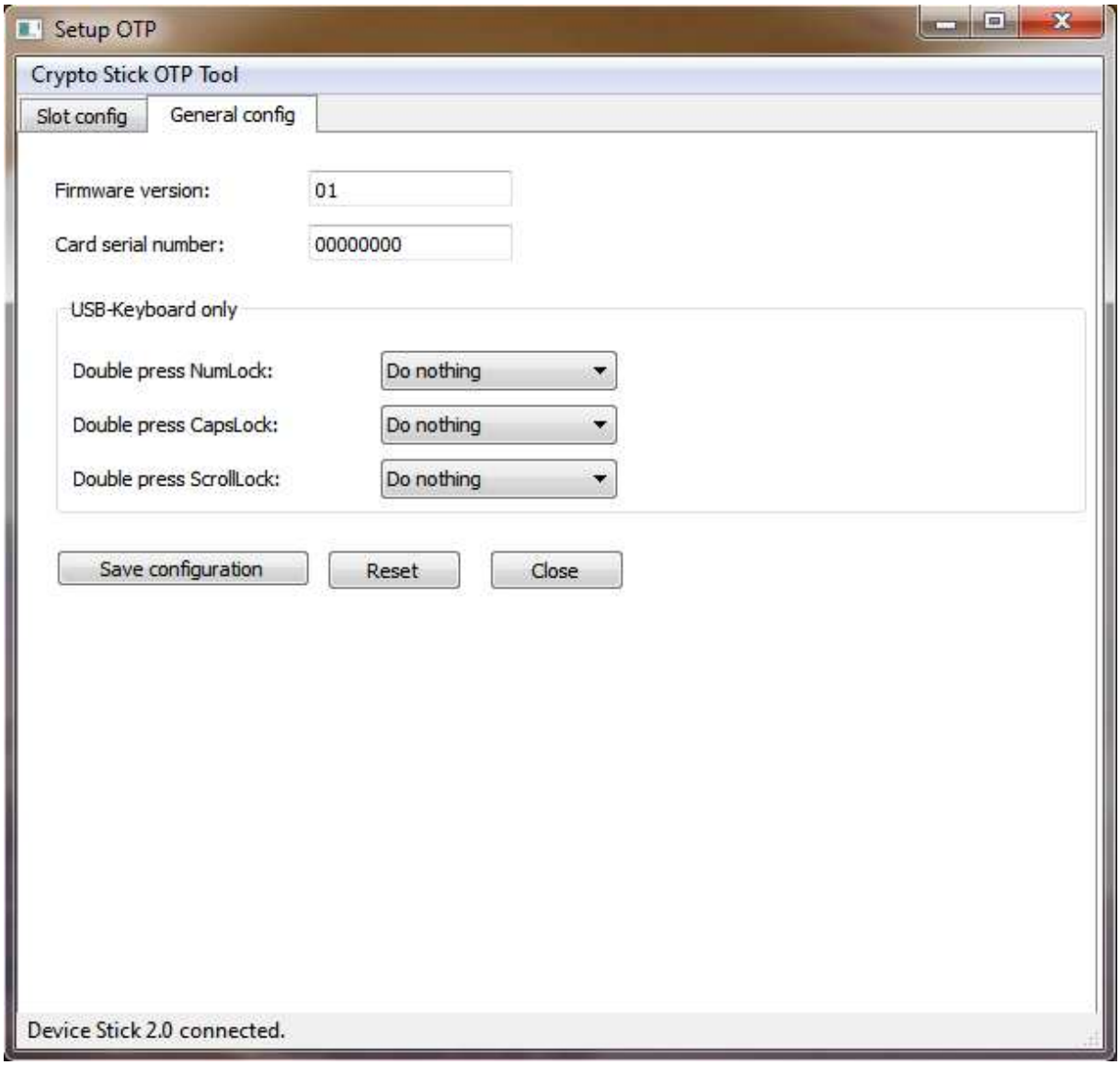
This entry configures the one time password. You can configure HOTP und TOTP entrys.

Slot count	
HOTP entries	3
TOTP entries	15

To enter the configuration you had to enter the admin PIN of the smartcard.




Setup OTP
Crypto Stick OTP Tool
Slot config
General config
Slot:
HOTP slot 1 []
Name:
Secret key
Secret Key:
Input format:
Hex
Base 32
Hide secret
Create random secret
Send 'enter'as the last keystroke
OATH-HOTP Parameters
HOTP length:
6 digits
8 digits
Moving factor seed:
0000000000000000
Set to zero
Set to random
Token ID
Send token ID
Keyboard layout (DISABLED FEATURE):
OMP:
CS
TT:
01
MUI:
cdcdcdcd
QWERTY
Save Configuration
Reload Configuration
Erase Slot
Close
Device Stick 2.0 connected.


Setup OTP
Crypto Stick OTP Tool
Slot config
General config
Firmware version:
01
Card serial number:
00000000
USB-Keyboard only
Double press NumLock:
Do nothing
Double press CapsLock:
Do nothing
Double press ScrollLock:
Do nothing
Save configuration
Reset
Close
Device Stick 2.0 connected.

Change user PIN

With this menu entry you can change the user PIN of the openPGP smartcard.

Old PIN	Enter the existing PIN of the openPGP smartcard
New PIN	Enter the new PIN of the openPGP smartcard
New PIN	Reenter the new PIN of the openPGP smartcard
Show PIN	Select this checkbox to see the text in the text fields

Change admin PIN

With this menu entry you can change the admin PIN of the openPGP smartcard.

Old PIN	Enter the existing PIN of the openPGP smartcard
New PIN	Enter the new PIN of the openPGP smartcard
New PIN	Reenter the new PIN of the openPGP smartcard
Show PIN	Select this checkbox to see the text in the text fields

Setup hidden volume

This point configures the hidden volumes.
A hidden volume is an encrypted volume that is place in the normal encrypted volume.

Warning: There is no overwriting check between the encrypted and the hidden volumes.

The AES 256 bit keys for each encrypted or hidden volume are different. If a volume read data from another volume it gets only random chars.

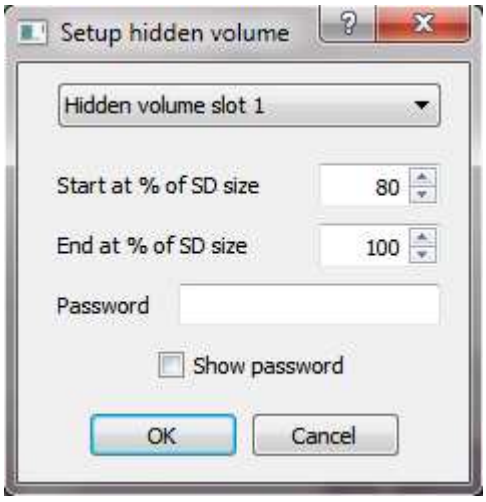
Hint:
Normally a FAT file system fills the volume from down upwards. When you have a new formatted encrypted volume from 32 GB and write 3 GB into the volume the only the first 10% the volume are used. A hidden volume that is created in the upper area (for example in the area 80-100%) is not touched.

Also you can fill the encrypted volume with 100 % data and create then a hidden volume in the used area. Then the hidden data overwrite the data in the encrypted area. The hidden data is secure until the data of the encrypted that was previously was stored in the area of the hidden volume is changed. Because normally only the operating system knows where data is placed on a volume it is unclear when the operating system writes into a hidden volume.

Best practice for hidden volumes:

- Format the encrypted volume
- Fill the encrypted volume with some data
- Now use the encrypted area only for reading
- Create and use a hidden volume in the upper SD area

If you create several hidden volumes avoid overlapping.
You can overwrite all hidden volumes when you fill the encrypted volume with 100 % data.



Combo box	Select the entry for the setup, 4 hidden volumes are possible
Start at % of SD size	Position of the start block of the hidden volume in % of SD size
End at % of SD size	Position of the end block of the hidden volume in % of SD size
Password	Password for unlocking the hidden volume

Example for 2 hidden volume:

Hidden volume slot 1	
Start at % of SD size	80
Start at % of SD size	100
Password	abcdef
Hidden volume slot 2	
Start at % of SD size	60
Start at % of SD size	80
Password	abcdefg

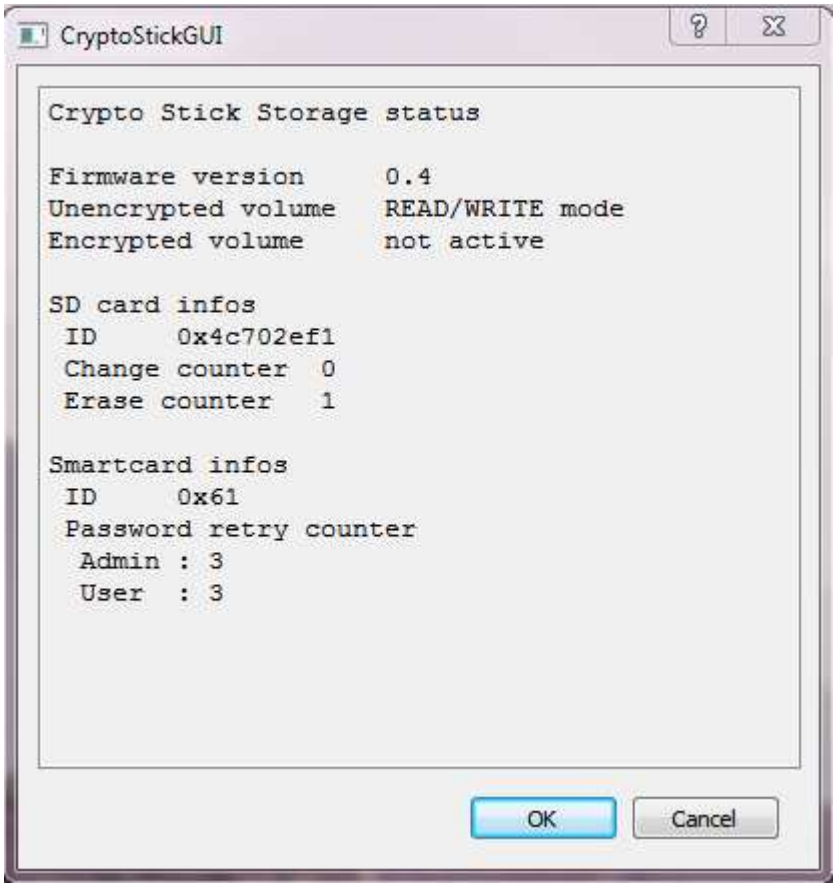
Destroy encrypted volume

This is a fast way to delete the encrypted und hidden volumes.

The option creates a new AES storage key and a new AES master key stored on the smartcard.
The AES storage key is placed on the CPU internal flash, encrypted by the master key which is stored in the OpenPGP smartcard.

Warning:
When you activated this option the encrypted and hidden volumes are destroyed by delete the encryption keys.

Get stick status



Crypto Stick Storage status

Firmware version

Version of the flashed firmware

Unencrypted volume

READ/WRITE mode	You have write access to the unencrypted volume
READ only	You have read only access to the unencrypted volume

Encrypted volume

Not active	The encrypted volume is locked
Active	The encrypted volume is unlocked

Change counter

This counter rises when the SD in the stick was changed

Erase counter

This counter counts the “Fill encrypted volume with random chars” calls

SD card info’s

ID

Serial ID of the SD card

Smartcard info's

ID

Serial ID of the smartcard card

Password retry counter

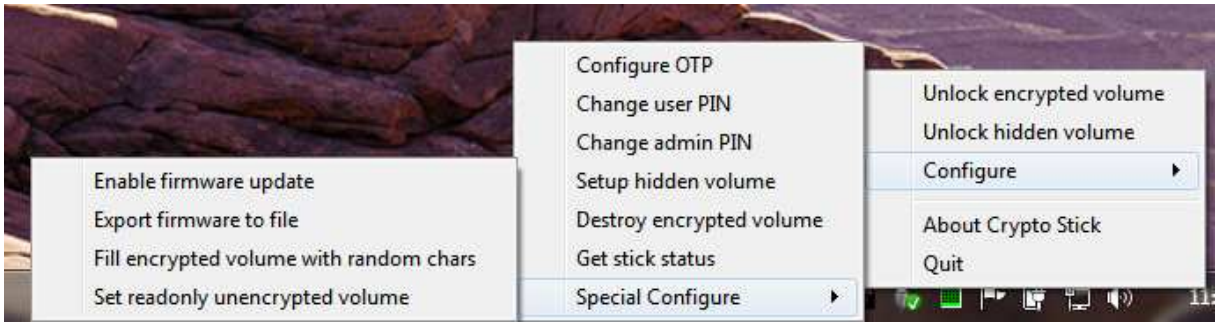
Admin	Possible retries before the smartcard is locked
User	Possible retries before the user password is locked

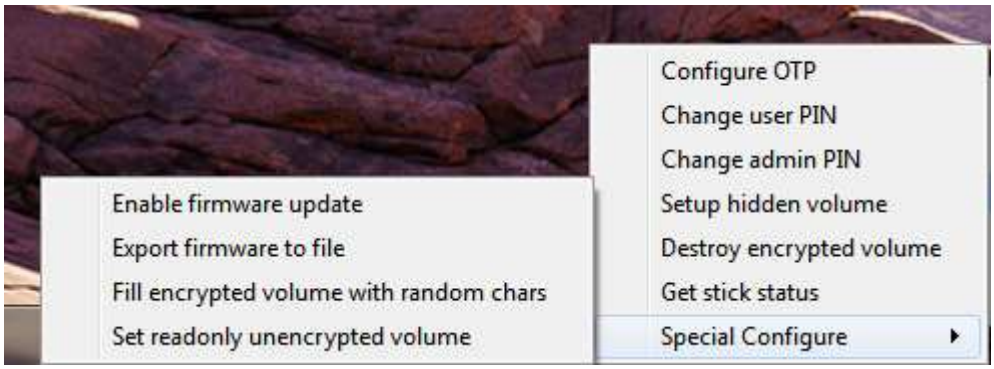
Information's for special stick situations

ARS Storage key and Master key are not initiated

A new SD card was found

Sub menu “Special Configure”





Enable Firmware Update

Warning: Warranty lost by flashing an unauthorized firmware

With this command the Crypto Stick Storage goes into the update mode for the firmware.

Activation by the admin PIN of the OpenGPG card.

After pressing “OK” the Crypto Stick starts the flash loader at the next power on.

Warning

- After OK you had to flash the Crypto Stick Storage.
- Normally the keys of the encrypted and hidden volume are deleted so that the encrypted and hidden volumes are lost. The keys on the smartcard are not affected.

Flashing the new Crypto Stick Storage software

Command line to flash the new software

The new CryptoStick software is flashed by the ATMEL© software “batchisp“ which is installed during the FLIP installation.

You can generate the new CryptoStick software by the development environment or download it form your web site.

The file you need is the XXXXX.elf file. In our example it is named USB_MASS.elf.

```
batchisp -device AT32UC3A3256S -hardware usb -operation erase f memory flash
addrange 0x80002000 0x8002ffff blankcheck loadbuffer USB_MASS.elf program verify
start reset 0
```

Output of the flash program

During the flashing the blank check shows an error, this is normal because the flash loader (bootloader) of the CryptoStick is marked as read only. You had to ignore the error. Also the warning is normal because the ELF file contains the flash loader.

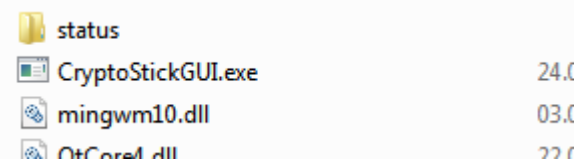
```
Running batchisp 1.2.5 on Wed Jul 24 10:42:34 2013


AT32UC3A3256S - USB - USB/DFU


Device selection..................... PASS
Hardware selection................... PASS
Opening port......................... PASS
Reading Bootloader version.......... PASS    1.1.0
Erasing.............................. PASS
Selecting FLASH...................... PASS
Setting Address Range................ PASS    0x80002000      0x8002ffff
Blank checking....................... FAIL    Address is out of range.
(A)bort, (R)etry, (I)gnore ? i

Parsing ELF file..................... PASS    USB_MASS.elf
WARNING: The user program and the bootloader overlap!
Programming memory................... PASS    0x00000 0x2e133
Verifying memory..................... PASS    0x00000 0x2e133
Starting Application................. PASS    RESET   0

Summary:  Total 12   Passed 11   Failed 1

C:\Program Files\Atmel\Flip 3.4.5\bin>
```

Export Firmware To File

This command allows you to save the active firmware of the Crypto Stick Storage to the unencrypted volume. With this command you can check that the active firmware the firmware you guess.

Activation by the admin PIN of the OpenGPG card.

The command create the directory “status” on the unencrypted volume



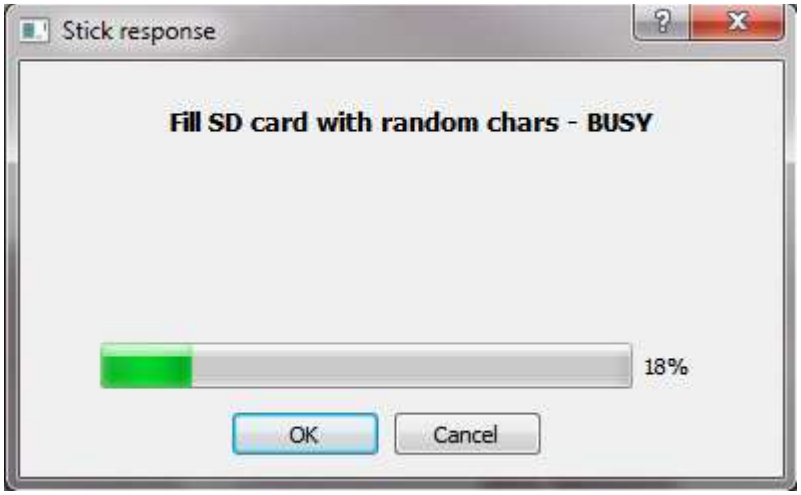
and save the firmware in the file “app.bin”. The length of the file is 248KB. Keys, saved in the upper part of the flash, are not save in the file.

Note
The keys stored in the flash are encrypted with the master key in the OpenPGP smartcard and are not transferred.

Warning
The firmware could be changed and the old firmware could be saved on the SD card, so if you export the firmware the hacked firmware send you the store old firmware. The attack requires a very good knowledge of the firmware.

To be really sure that you have the correct firmware, you had to insert and format (FAT32, block size 512 byte) a new SD card in the Cryptostick 2.0 before you export the firmware. In this case it is not possible to save a fake firmware, because the CPU flash have only a size of 256KB.

Fill encrypted volume with random chars



Set readonly unencrypted volume

To do …

Password matrix based commands

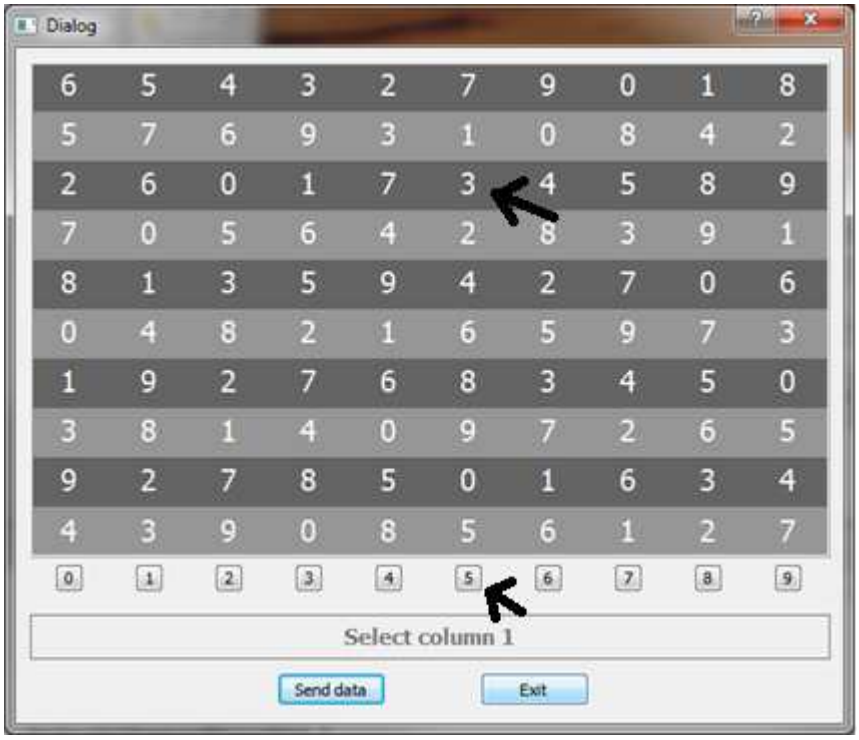
Setup the matrix based password

The matrix based password entry is a method to enter a numeric password in a monitored environment. The every digit of the numerical password was entered by the selection of the column of a 10x10 matrix of digits in which row the digit occurs. The 10x10 digit matrix was computed by the Crypto Stick Storage and transferred to the pc. In every row and column occurs every digit from 0-9 only one times.

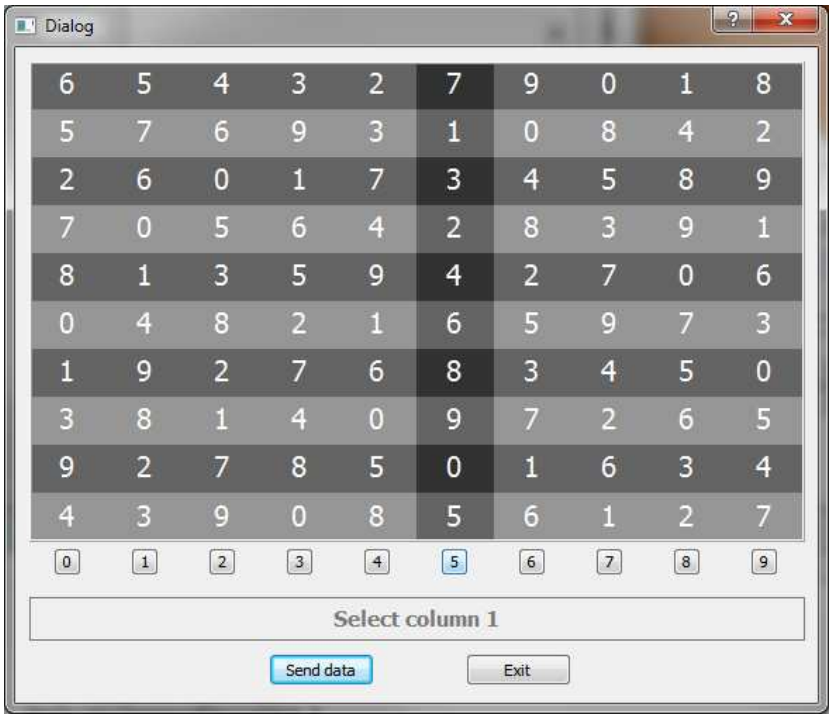
Simple Example:

Your password is	3	
The row for the selection of the first digit is	2	(counted from 0, from upside)

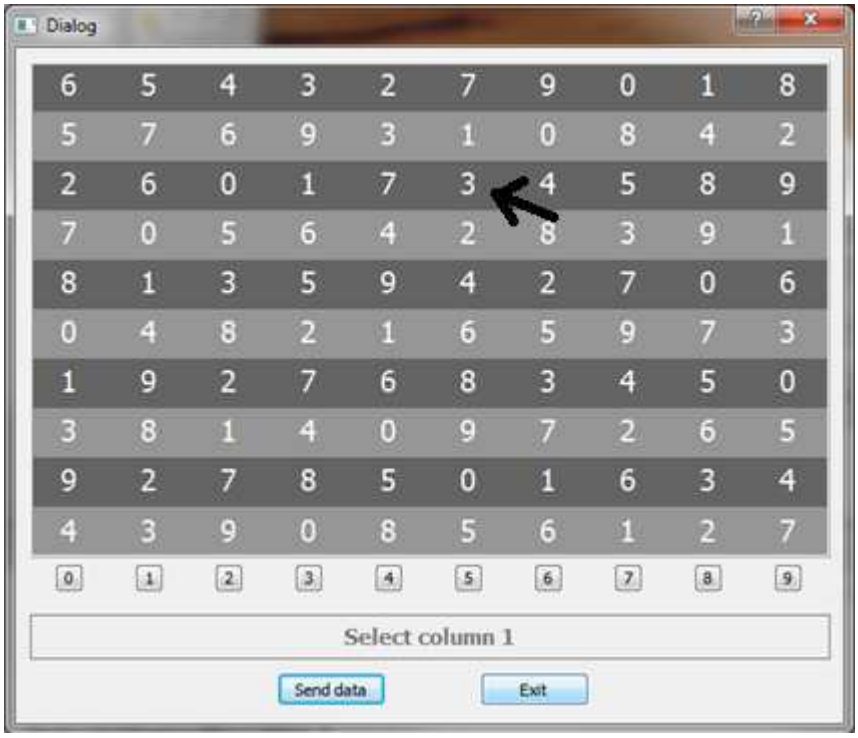
You entered your first digit of your password, in the setup you had defined
that the column of the first digit is column “3”. Now you see that in column “5” the digit “3” is in row “2”.



Now you had to press button “5” to enter the digit. When your mouse cursor moves over the selection button the corresponding column is highlighted:

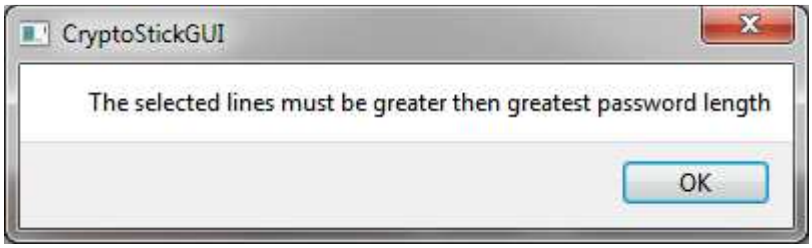


The Cryptostick 2.0 converted now the selection “5” into the digit “3”. For a longer password it works similar for every digit. For higher security reasons the matrix was computed new for every digit.



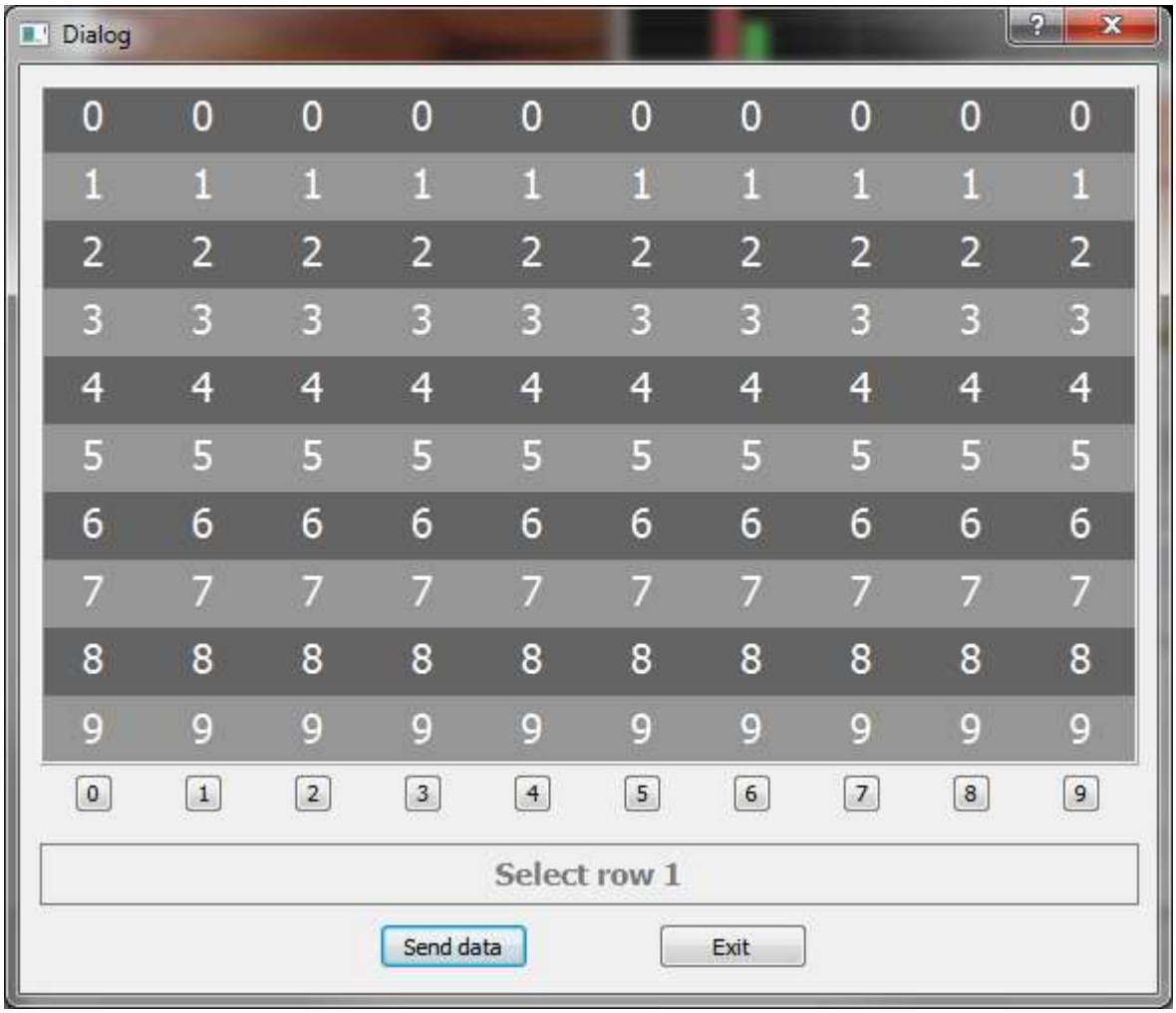
Setup the order of the rows which contains the digits of the password

First the message



was displayed.

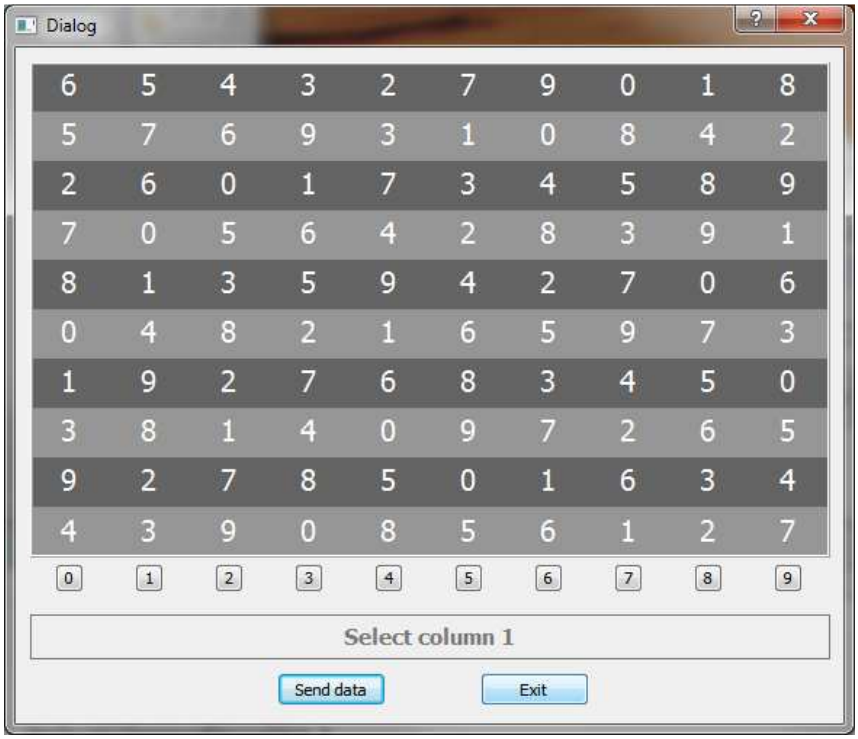
The number of the selected rows had to be equal or higher than the digits of the password.

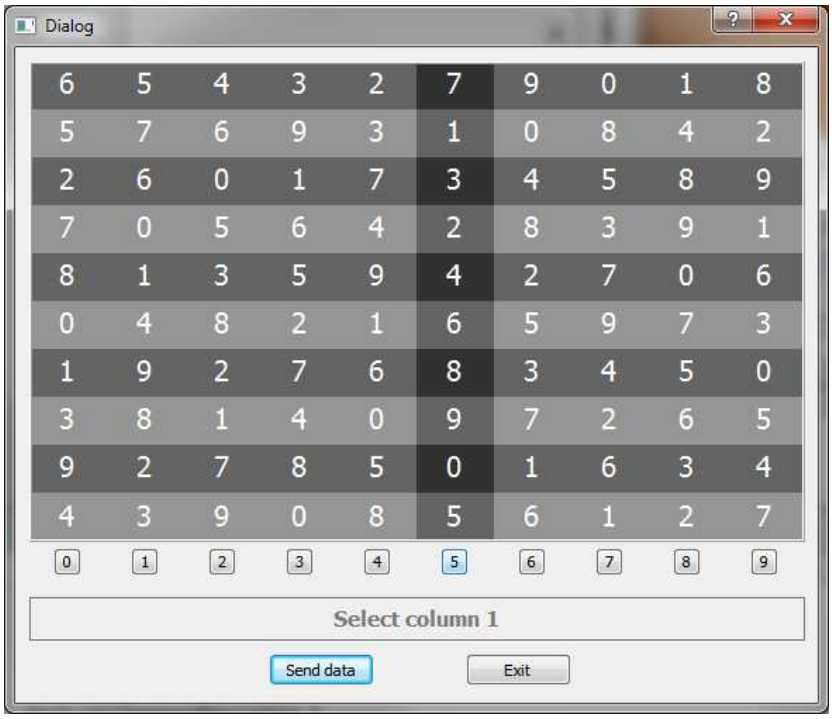


Now you had to select the first row

CryptoStick 2.0 – Document in development

Enter a Matrix based password




Dialog
6 5 4 3 2 7 9 0 1 8
5 7 6 9 3 1 0 8 4 2
2 6 0 1 7 3 4 5 8 9
7 0 5 6 4 2 8 3 9 1
8 1 3 5 9 4 2 7 0 6
0 4 8 2 1 6 5 9 7 3
1 9 2 7 6 8 3 4 5 0
3 8 1 4 0 9 7 2 6 5
9 2 7 8 5 0 1 6 3 4
4 3 9 0 8 5 6 1 2 7
0 1 2 3 4 5 6 7 8 9
Select column 1
Send data
Exit

CryptoStick 2.0 – Document in development

Todo ….

Changing the SD card

Open the case of the CryptoStick 2.0

Change the SD card

Connect the Cryptostick to the PC

Fill the SD card with random chars

Format the uncrypted volume

FAT32, block size 512 byte

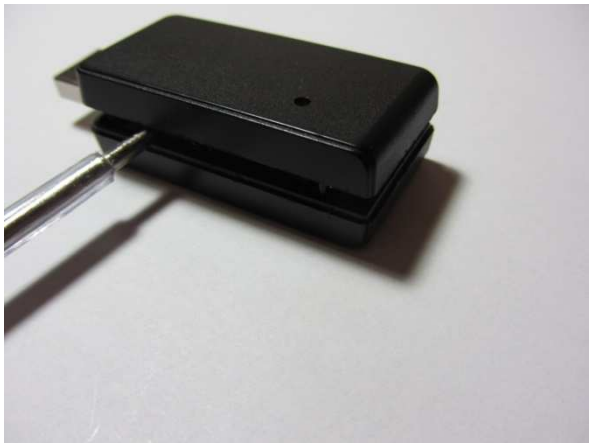
Enable the crypted volume

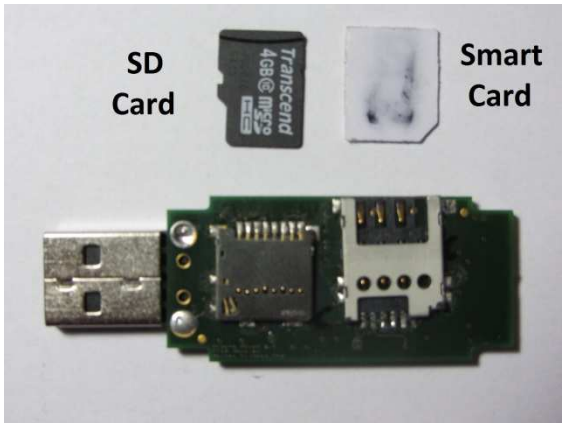
Format the encrypted volume

Opening the case of the Crypto Stick Storage

(Case version of prototype)

Warning: Warranty lost




SD
Card
Smart
Card