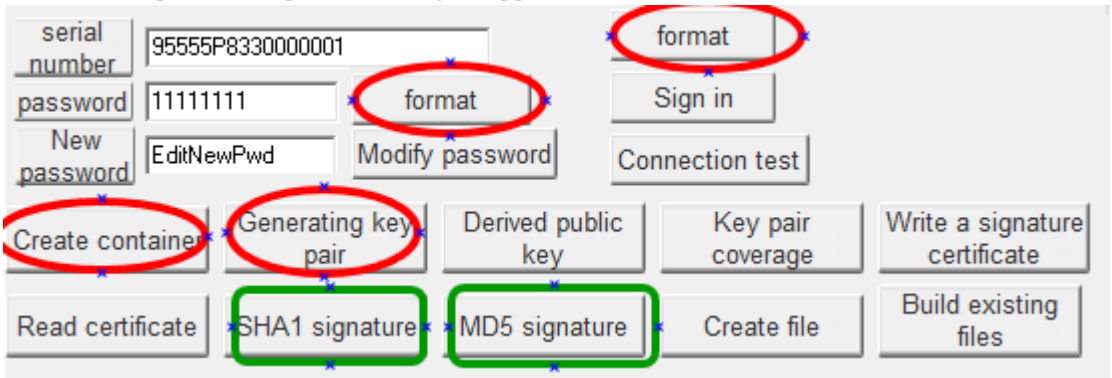
WatchKeyOTP User manual

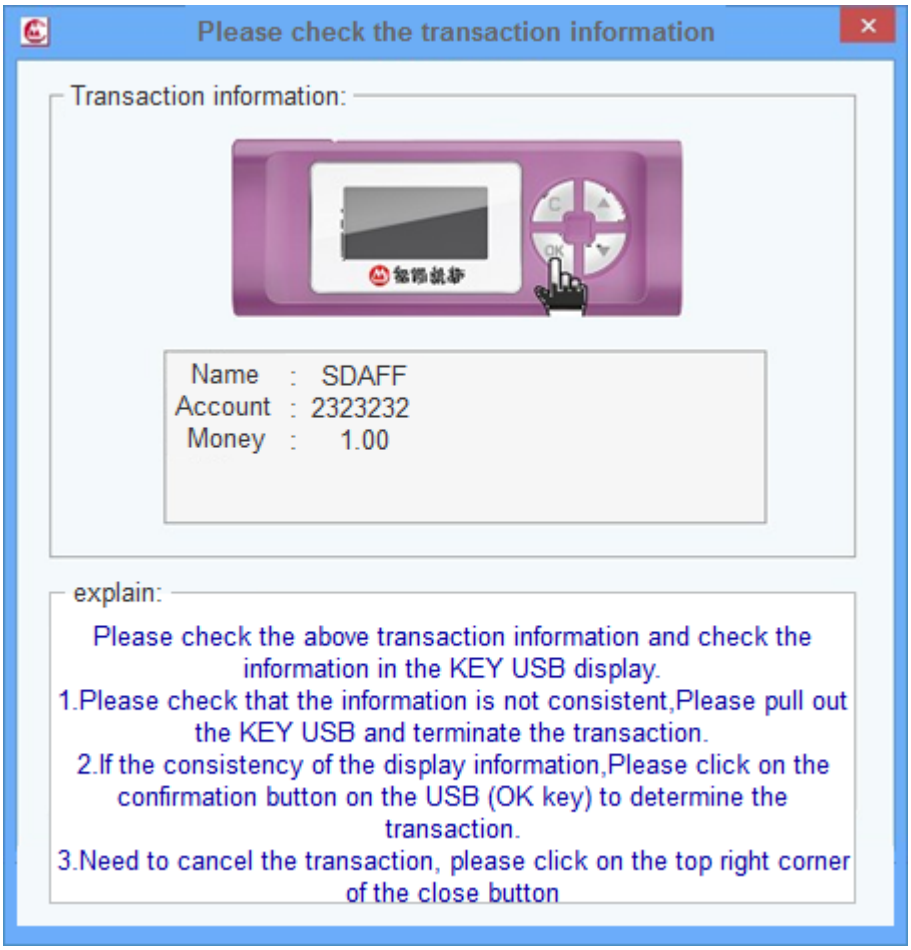
List

1.1 Key transaction testing

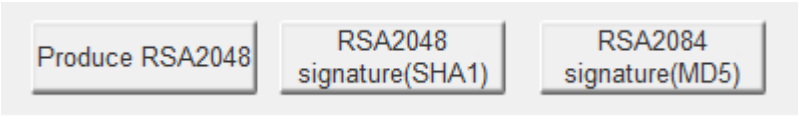
1. First run UsbkeyTest.exe, and then insert the WatchKeyOTP;
2. Read the serial number: insert KEY, click the "read serial number" button, in the "serial number" box to display the serial number of KEY；
3. Formatting: click the format button, the bottom end of the tool in the status bar to display the "OK Init", indicating the success of the initialization, the default password is the password input box enter the password. (password length supports 6-20 characters);



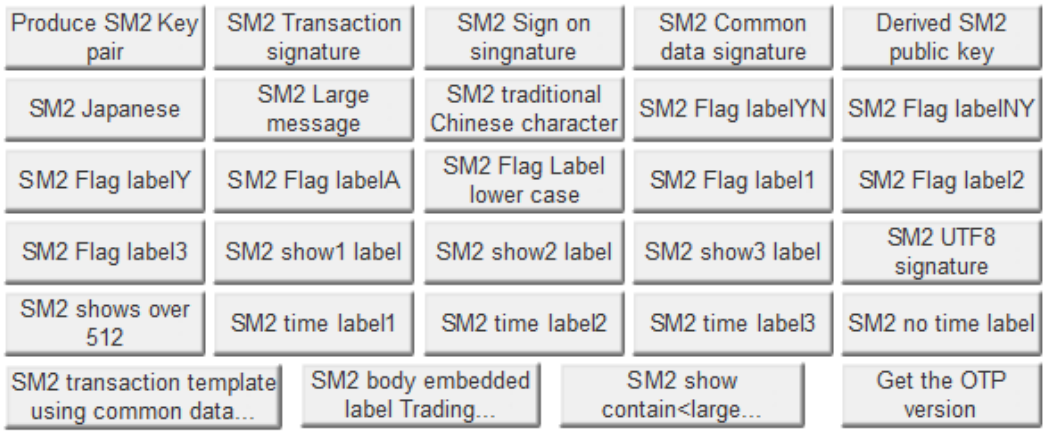
4. RSA1024 transaction testing：
   1) Formatted key, point "create container" to return CryptAcquireContext OK；
   2) And then point "for generating a secret key" button, RSA1024 certificate, GenKey OK said the successful return；
   3) Then point SHA1 signature and MD5 signature for the transaction signature, pop-up prompt window, and then to the Key button to confirm, return to the Verify OK Sign, said the success of the transaction.



5. RSA2048 Transaction testing;
   1) Formatted key, point "create the container", return to OK CryptAcquireContext;;
   2) Finish step "to produce RSA2048 key button to generate the rsa2048 certificate, GenKey OK said the successful return;
   3) 在 In the middle of the tool position, to find the RSA2048 signature (SHA1) and the RSA2048 signature (MD5) for the transaction, the pop-up window prompts the Key side button to confirm. To the key side by confirmation after the completion of the transaction, the return of Verify OK Sign".



6. SM2 Transaction testing:
   1） Formatted key, point "create the container", return to OK CryptAcquireContext;
   2） Finish step in tools in the lower part, find out the causes of SM2 key button, as shown in Fig;. :



3） Click "SM2 key", have SM2 certificate, successful return "GenKey OK"；

4） Click "SM2 transaction signature", the pop-up window and prompt the key button to confirm that the transaction was successfully returned to the "OK SM2_verify".

1.2 OTP Dynamic password test"

1） Confirm that PC system time is the same as OTP：

a) Changan OTP power button, enter the boot password 1111"；

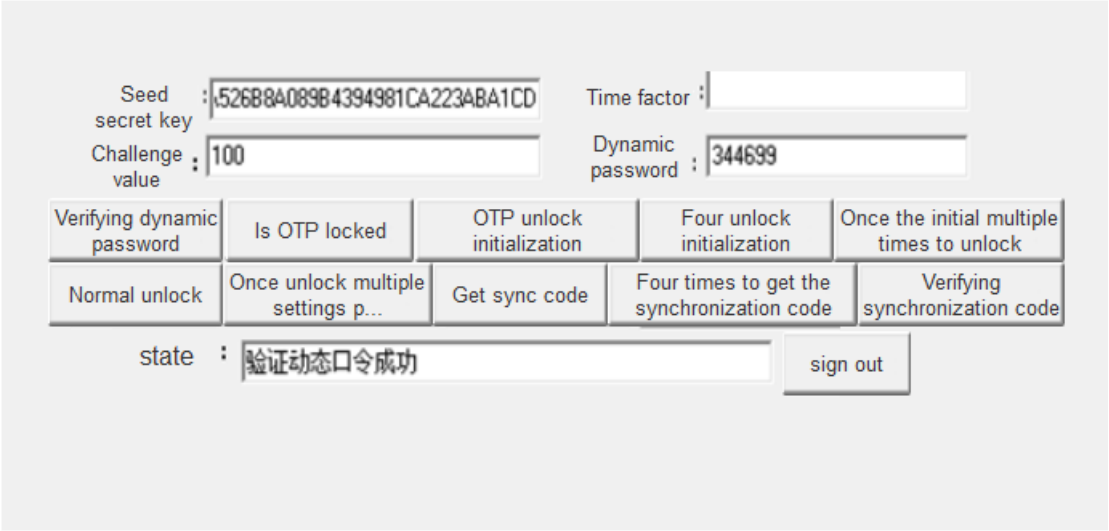
b) When key prompts to enter the transaction elements for a long time press the Cancel button, will display the OTP system time, modify the PC time and the same OTP；

2） Generate dynamic password：

a) Modify the system time to open the WatchKeyOTP device, prompted to enter the transaction elements when the input "100" to confirm, resulting in dynamic password; (the value of the transaction value is not more than 12)；

3） Verifying dynamic password

a) Insertion WatchKeyOTP device to PC, running UsbkeyTest.exe. In the lower of the tool seed secret key field, enter the corresponding serial number of the seed secret key (seed secret plaintext. Txt), enter a key input elements of the transaction value in the challenge value, the Enter key end display the password in the dynamic password, check card dynamic password, prompt success in verifying dynamic password。


Seed secret key
526B8A089B4394981CA223ABA1CD
Time factor
Challenge value
100
Dynamic password
344699
Verifying dynamic password
Is OTP locked
OTP unlock initialization
Four unlock initialization
Once the initial multiple times to unlock
Normal unlock
Once unlock multiple settings p...
Get sync code
Four times to get the synchronization code
Verifying synchronization code
state
验证动态口令成功
sign out

FCC Caution.

§ 15.19 Labelling requirements.
This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

§ 15.21 Information to user.
Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

§ 15.105 Information to the user.
Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
-Reorient or relocate the receiving antenna.
-Increase the separation between the equipment and receiver.
-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-Consult the dealer or an experienced radio/TV technician for help.