Bluetooth USBKey/ComyiKEY-420

User Guide

1. Overview

This document describes how to use Bluetooth USBKey/ComyiKEY-420，a Bluetooth smart password key.

1.1 Install/uninstall

1.1.1 Install the management tools

Double-click the installer, then open the installation interface.Click "yes" to continue installation

After the installation is completed, 3 s interface will be automatically closed.

1.1.2 Uninstall the management tools

There are two ways to uninstall management tools:

1.From the start menu - all programs -the bank’s USB KEY-the KEY’s management tools - unloading;

2. Open the control panel, add or remove programs ways for unloading

1.2 Function is introduce

1.2.1 Management tool interface

User can "start" - >"all programs" - >"guiyang bank USB - KEY management tools" - >"Watertek information" - >"guiyang bank USB - KEY management tool" find a shortcut to the management tool, click the shortcut management tool startup management tool.

1.2.2 Check the certificate

In certificate management tool interface, click the "view certificate" button, on the right side of the "view certificate" into the interface, in the "view certificate" interface will show the detailed information of the certificate and the certificate such as "The issuer".

1.2.3 Verify the USBKey’s password

In the certificate management tool’s, click on the right side of the "validation USBKey password" button, the pop-up input password dialog box.

Enter the password and then click the "ok" to verify password.

1.2.4 Modify the USBKey’s password

In certificate management tool interface, click the "modify USB - KEY password" on the right side of the button, the pop-up modify password dialog box.

The bluetooth KEY initial password is "12345678", you can modify the password.

Note:At the same time of Password change box appearing , the management tools will start security desktop.In the secure desktop state, the entire desktop will be dark, only the password box is highlighted.Can only enter the password at this time, most of the other operations will not be able to undertake, including window monitoring means of attack.Therefore, the security desktop can effective prevention and control of the attacker to steal the user's password.Users can choose to use soft keyboard to prevent Trojan program to the user keyboard input password to monitor, if the user selects "opens the soft keyboard".

User input password automatically check password security intensity and complexity.

If the original password is not correct, will have a corresponding prompt interface.

1.2.5 Modify the USBKey's name

Management tools main screen click on "modify USB - KEY name" interface, you can type in the name of the new bluetooth KEY, to modify the bluetooth KEY name.

2 Administrator tools use instructions

Administrator tools is on the basis of the installation management tool, through the "initialization" button to initialize the bluetooth KEY operation.

When the initialization, the user needs to press the "confirm" button at the bluetooth KEY equipment, initial success.

3 Trading/signature attestation tool

Transaction signature/attestation tool can generate a KEY pair, and write in the bluetooth KEY.You can also use this key to trading signature/attestation.

3.1 Generate the key pair

After inserting the bluetooth KEY, select the bluetooth KEY corresponding to the name of the CSP, enter any container name, click on the "generate the KEY pair" button, the pop-up prompts request confirmation, buttons on the bluetooth KEY equipment, press the "ok" button, generate a KEY to success.

3.2 Transaction signature/attestation

In transaction message choose adaptable to the rules of the bluetooth KEY message, click on the

"signature" button, input the correct bluetooth KEY password, will pop up in the transaction message choose adaptable to the rules of the bluetooth KEY message, click on the "signature" button, input the correct bluetooth KEY password, tips will pop up: In the Bluetooth KEY equipment, press "ok" button, a successful deal.

FCC Warning

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

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.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment .

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.