
HANOOL
ROBOTICS

CAUTION: Changes or modifications not expressly approved by the manufacturer responsible for compliance could void the user's authority to operate the equipment

•WARNING

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.

INFORMATION TO USER:
This equipment has been tested and found to comply with the limits of 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:
1. Reorient / Relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit difference from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help

What is the Hanool USB-KEY?

HANOOL ROBOTICS

• Recently, with the increase in the Internet companies and related equipment and the establishment of the information infrastructure through the Internet, companies and schools as well as homes can now easily use the Internet through the PC. As a result, Internet users increased with the activation of the electronic finance transactions using the Internet, and various types of security storing devices were developed to solve the many problems concerning the safety and security during electronic finance transactions. Of these security storing devices, they were developed as the early network type cards and the IC type cards called the smart cards and other various devices, but the early network type cards had problems that the security data had to be left on the PC which the e-commerce was executed on, and the smart cards that solved this problem required an additional card reader device which was expensive to general users. As a result to solve these problems of the existing devices, the USB KEY was developed as the security storing device for safe and convenient e-commerce for general users without any needs of additional equipment and leaving no security data on the PC.

The method for certifying

• The method for identifying and certifying the person or processor using the system can be divided into the following 3 methods.

1. Authentication based on something the user knows

2. Authentication base on something the user processes

3. Authentication based on something the user is

User knows

• The easiest method is to identify the user by inputting the ID and password when the user wishes to access the system, and the system compares the data with the stored data and permits access only when the two coincides. This method was used for a long time and was recognized for its usefulness and efficiency, but due to the changes in the computing environment, the following problems were indicated.

※ Problems

- Easy password assumption
- Password sharing
- Password exposure on the network

※ Enhancement schemes

- Password generators
- Login failure amount limitation
- Password setting restrictions
- Periodical password changing

• As a method to improve the password identification(=user knows), the token method, largely divided as the memory token and the smart token according to the token's characteristics which uses a physical identification method to prevent password stealing through the network from a far distance and using a complex mechanism(H/W) to make it hard to assume the password by trial and error. But both of these require to use a password as well to prepare for a case where the token is lost..

a. Memory token

• The memory token simply stores the information and identifies the user through a special token reader, in contrast with the smart token which self-processes using the stored information. A good example is using the cash card in the automatic transaction machine.

※ Pros

• It is more safer than using only a password in that it requires a physical token as well as the password.

• It is more cost effective than the smart token.

※ Cons

• The cost for installing the card reader is fairly high.

• The hardware security is relatively simple which makes it weak to duplication and hacking.

b. Smart token

• A token that processes security related data and password related processing through its integrated circuit other than the memory token that simply uses only the stored data.

※ Pros

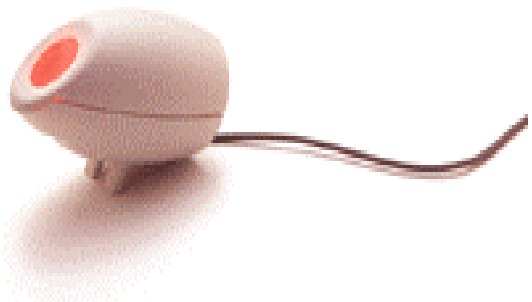
- Disposable password
- reduced danger of damage
- useable for various uses

※ Cons

- More expensive compared to the memory token

User is

• As a way to completely solve the danger of loss of the token of information exposure in the case of the passwords and tokens, a way of using the physical characteristics that are different for each individual such as the finger print, pupil pattern, and personal behaviors such as signatures, voice patterns to identify the user was developed. This method is highly complicated, expensive and has possible failures, but as the technology develops, it is a field that can be solved significantly.



Authentication based on Hanool USB-KEY

HANOOL ROBOTICS

- The basic user authentication is identical to giving the user the token(Authentication based on somethin the user processes). However, by applying the USB(Universal Serial Bus) communication type, it was possible to get the advantages of the existing token type as well as solving the problems.

• Limits of the memory authentication

The existing authentication uses the User ID/Password, and is inconvenient to store and is critical in security when exposed to others. .

• Solving by carrying authentication

A way of applying the direct carrying method such as smart cards or organic authentication(finger prints, iris) was thought of, but the price and the infrastructure problem of the reader diffusion was a problem for wide spreading.

• Hanwool KEY a solvent

Since it uses the USB ports on the current PCs, a Hahnwool KEY that does not need a reader can be a realistic solvent. Especially, it is becoming a alternative that would make it possible to move and carry the personal keys in the PKI based solutions such as the Internet Banking, cyber trading etc.

Introduction

• The Hanwool KEY is an inexpensive identity token that can be used on any universal serial bus(USB) equipped computer. It is technical innovation for identifying and certifying the person and have various application field.

• The Hanwool KEY is a storing device that doesn't need a certificate of authentication

• The Hanwool KEY does not require a reader like the smart card in that it uses the USB port on the PC to communicate with the PC.

[Hanwool KEY Sample]

Feature

• Convenience

1. It is easy to install and use due to the P&P and Hot Plug-In features of the USB.
2. There is no need for external power to activate the Key.

• Safety

1. Personal information is not left on the Internet or the PC, but is stored in the Hanwool KEY and is carried by the individual.
2. User authentication is processed only through the Hanwool KEY, therefore nobody except the owner can be authenticated.
3. Strong material to prevent damage.
4. The connector cover prevents damage from stain and external pressure.
5. The HID is stable due to its dependancy on the OS(Windows).
6. CE, EMC certification acquired.

• Portability

1. It is possible to be authenticated on a different PC as well.
2. It is smaller than a general key to make it convenient for carrying and can also be used as an accessory..

Feature

- Other
  1. Various designs to meet the user's tastes are possible.
  2. The A-type male standard USB connector is used.
  3. A extension cable for desktop PC users is offered.

- Convenient Developer's Environment
  1. It is possible to realize the appropriate specifications and functions according to the user's system.
  2. The control of all the tasks of the Hanwool KEY activation(USB communication, data storing) is done by the upper application program interface, and this is offered as a library(DLL files) of functions in API. In other words, the developer does not have to intervene with the USB or the related control tasks to activate the Hanwool KEY, and the application is realized by using the offered functions. Also, the I/O related tools and the USB related tools are offered to help with the problems during development.

Specification

• Performance environment of Hanwool KEY
- OS : Microsoft Window 98/ 98se/ ME/ 2000
- CPU : Higher than Pentium 100MHz
- Memory : More than 32MB
- Interface : At least one USB port

• Device driver
- HID(Human Interface Driver) used
- All the files that are needed to install the driver in basically included in the OS install pack.

• Memory size
- 2Kbytes ~ 16Kbytes

• Hanwool KEY size
- 65 x 20 x 10 (mm)

•USB Connector
-A Type male

API

• API(32K)

- The functions that activate the Hanwool KEY are made by the Visual C++ based API in DLL files.

- The Hanwool KEY can be controlled by using the functions that are registered in the library by the programmer who designs the Hanwool KEY application.

• Hanwool KEY's Functions

- Initialization functions for the device installing.

- Find function for KEY recognition.

- Read/Write function for storing the data on the KEY.

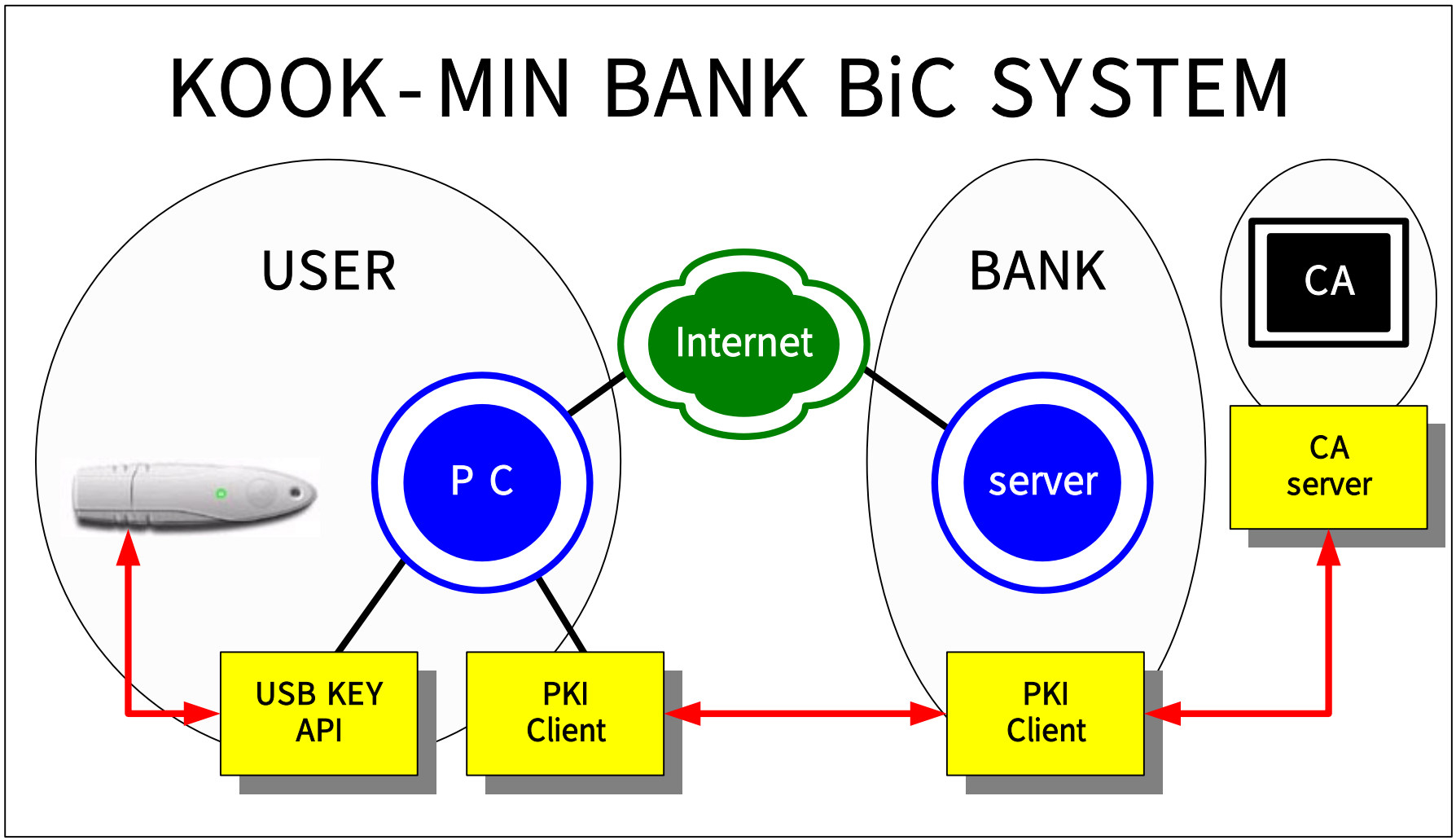
- LED control function

- PIN(Personal Identify Number) control function

Application field of The Hanool USB-KEY

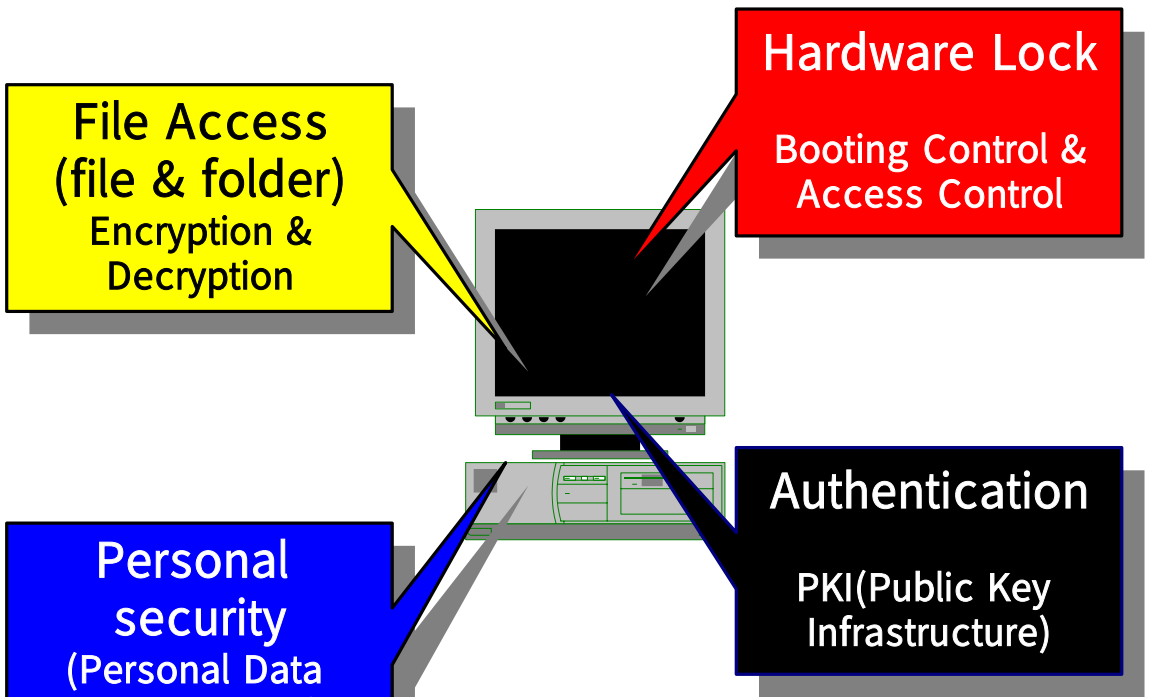
HANOOL ROBOTICS

• The Hanwool KEY application is not limited to the use of e-commerce security devices and its derivations. This is due to the characteristics of the Hanwool KEY as a security function and a storing device for Internet banking, e-commerce, e-cash as well as security devices like lock-keys, hardware lock-keys, personal password cards, for its application field is very wide and especially useful for personal user management and security devices in the charged contents business.

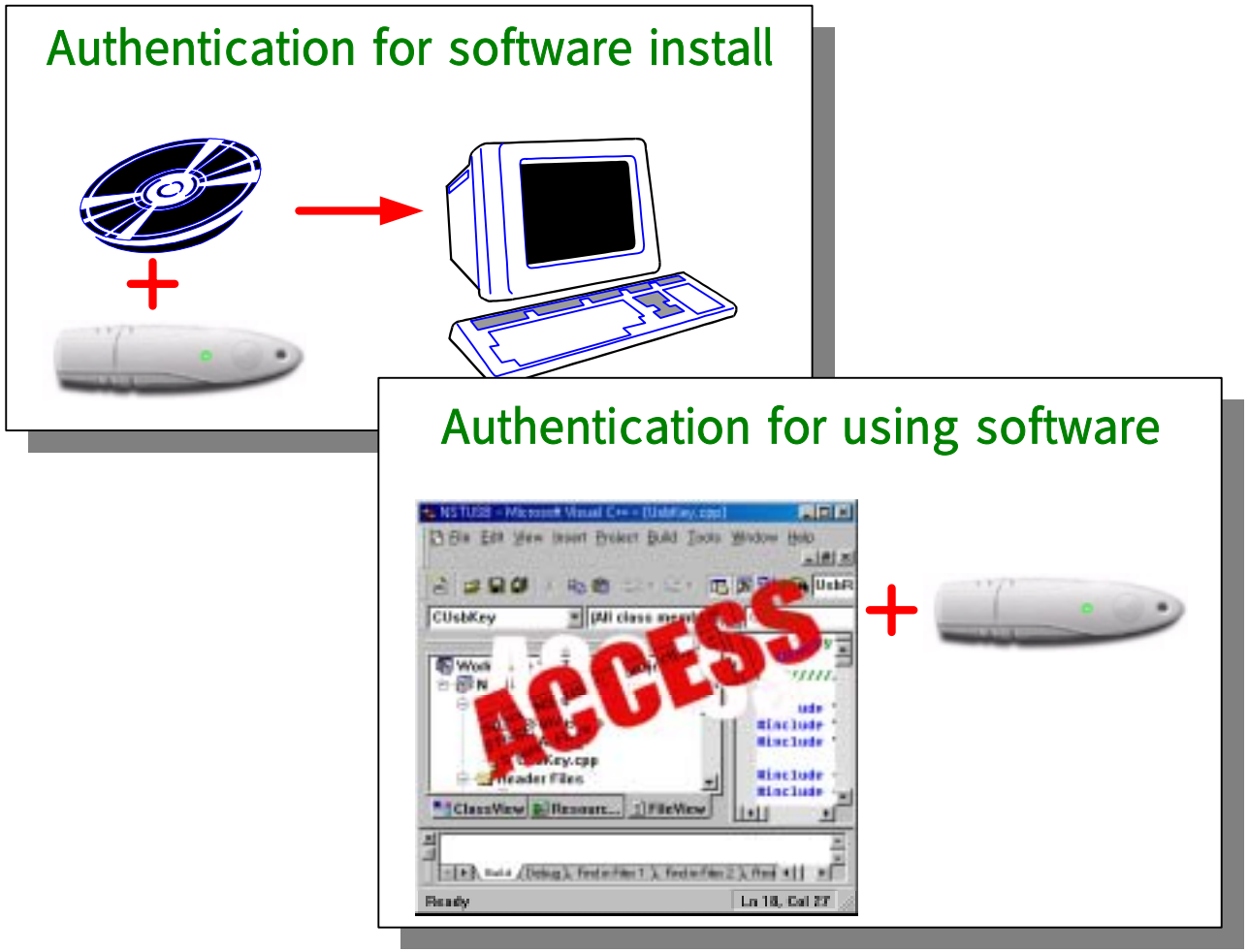

KOOK-MIN BANK BiC SYSTEM
USER
BANK
CA
Internet
P C
server
CA
server
USB KEY
API
PKI
Client
PKI
Client

HANOOL ROBOTICS

EnDe Pro for USB-Key



Applied case 3



Thank you!

Smile with HANOOL Robotics.