

---

# Web Authentication

**SecuTech Solution Inc.**

---

Nowadays, the demanding of high-level security is getting more and more a critical question for end users. Some of them trying to get a perfect solution to protect desktop, personal data, valued materials. SecuTech is dedicating to invest time and energy to provide satisfied solution for customers who are worrying about security and getting into a dilemma to pick up the best way to settle up.

**Are you worrying about the web logon security?**

A web authentication solution is a best choice for high-level security demanding. With a key inserting into a USB port, two-factor authentication ensures you are the right person to the right place online.

---

## Contents

1. Who should read this paper.....	4
2. System overview.....	5
3. System architecture.....	6
4. System highlights.....	9
5. What we can offer for you .....	10
6. System Setup.....	11
6.1 Package Check List.....	11
6.2 Server Setup.....	11
6.2.1 User Management .....	12
6.2.2 User Database .....	错误! 未定义书签。
6.2.3 Configure Server .....	14
6.3 Client Setup.....	14
6.3.1 Install ActiveX (COM component).....	15
6.3.2 Configure IE.....	15

---

## 1. Who should read this paper

SecuTech Solution Inc. and her partners offer **cost-effective** web logon solution for various customers. There is no need for a CA (certificate authority) and digital certificates. We provide customized service and special functions meeting different requirements raised by customers.

### System requirements:

#### Server:

- Windows 2000/2003 + IIS server
- ASP
- mysql database
- COM component

#### Client:

- Internet Explore
- COM component

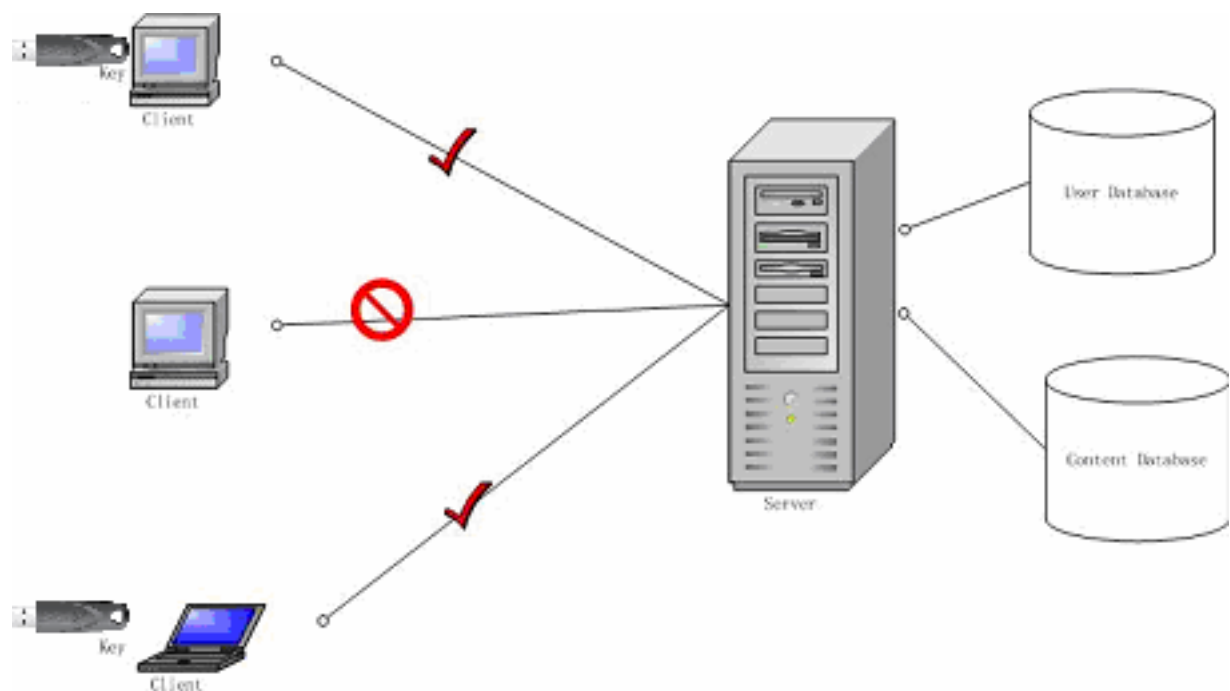
---

## 2. System overview

As shown in the chart, in order to perform strong web authentication, the system need only not a server with content database, but all a database that contains User ID information and keys attached to workstation.

The basic logical idea is that only the workstation with the correct key can access the server's content, on the other side, the workstation without a key or with a wrong key cannot retrieve the information from the server.

Each workstation in such strong authentication need a key installed. The key is driverless so no need to install a driver on the workstation and only a small daemon is enough. The basic system requirement is Windows 98SE, Windows 2000 and Windows XP.

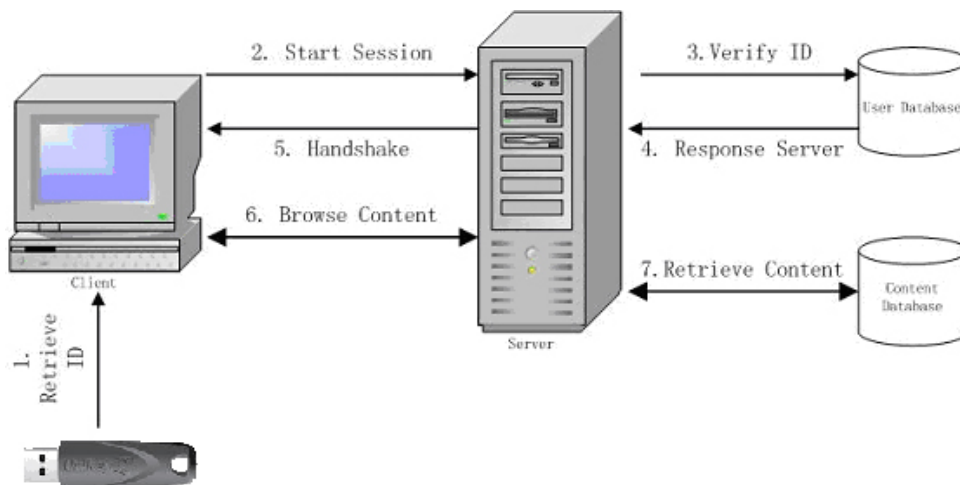


Compared with traditional username/password authentication, this two-factor authentication brings more security to the system, and provides more flexible web management.

---

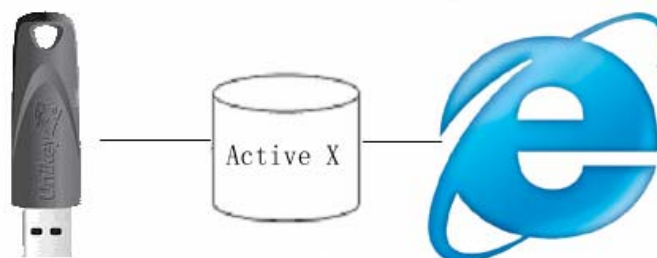
### 3. System architecture

To perform strong authentication, the daemon on the workstation retrieve the user credential from the hardware key, and setup communication with the credential. In the second step, the server attracts credential and verifies these in the user ID database. Thus, the server will respond the valid user and feedback the invalid user a warning. Finally the verified user can browse the content in the server via server.



When next communication is launched, the same steps will be performed again as above.

The browser acts as the media between authentication server and a user. There is an ActiveX control which working as the bridge between a UniKey and the browser. The ActiveX control collects the info inside UniKey and sends the info to the authentication for the further authentication process. The ActiveX control is only for the data delivery and it is not involved in the later authentication process.

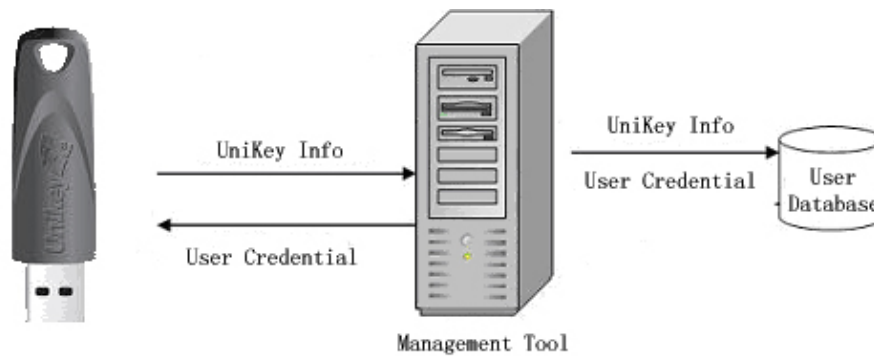


The authentication process is not strait forward, because we need a strong authentication. This process is called Challenge-Response authentication. The

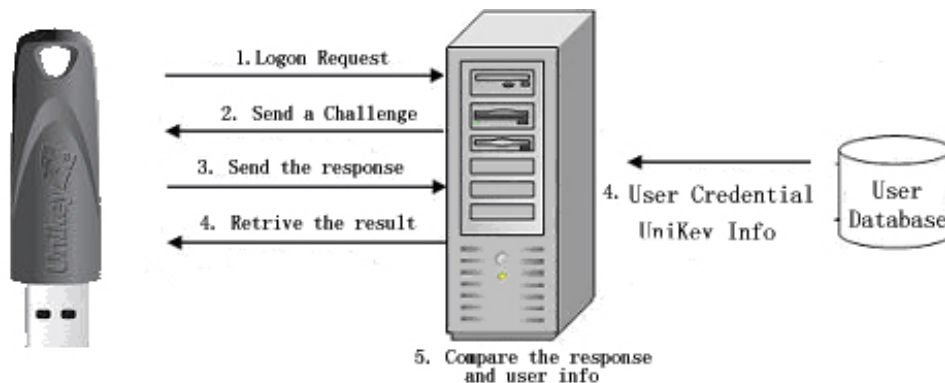
---

process is shown in the detailed.

The first step is to burn a UniKey. The management tool can generate a unique user credential for each UniKey key. It will retrieve the UniKey info and generate the user credential. Then the management tool store the user credential into the UniKey hardware key. Finally it add a user record into the user database. The user record contains at least the UniKey info and the user credential.



After adding the user record to the user database, we can say the user's info is created. All the users in the user database have permission to logon the server.



The first step in the authentication process is the client to send a logon request to the server.

Then the server sends a challenge to the client. The challenge in general is a random string.

Client receives the challenge, and it should compose a response. The response is generated by the UniKey info, user-credential and the challenge. The algorithm is based on HASH algorithm, so it is in-reversible.

$$\text{Response} = \text{HASH\_ALGORITHM}(\text{UniKey Info}, \text{User Credential}, \text{challenge})$$

Now, the server gets the response and it can retrieve the corresponding info from the user database. Then the server does the same computation again, and compares the

---

result from the client. If the result is the same, we can say the client is authorized, and vice versa.

Finally, the server sends the result to the client. If the client is authorized it can logon the server.

Please note, the challenge is always different each time, so the response should be not be the same. User credential is also unique to each key and user.

---

#### 4. System highlights

**No need for a CA**, CA is difficult and expensive. If you do not have a CA, you have to buy digital certificates from a third party, and it might increase the cost.

**Easy implemented**. The system is easy to be implemented. Our technical engineers will work with you.

**Cost-effective**. Getting rid of the full PKI system, we arrive at a cost-effective solution.

**Customized functions**. We can provide some customized functions based on customers request.

**Easy of use**, we design the system in order to provide a simple but secure solution for customers. Our customers can forget all the rigid technical terminologies.

**Acceptable security**, though the process is simple, the security is good. We use irreversible algorithm and each user holds a unique hardware key and digital credential.

---

## **5. What we can offer for you**

We are happy to provide our service to our valuable customers. We can offer

- a. User management tool, which add/edit/remove user info into/from the database
- b. The ActiveX control which deliver info
- c. Samples (based on your language and script)
- d. Integration guide (if know your server configuration/setting)
- e. Professional suggestions according to your system
- f. Prompt support

---

## 6. System Setup

UniKey Web Authentication Package is a completed solution for cost-effective strong security. It includes several components for both server and clients sides.

### System requirements:

Server:

- Windows 2000/2003 + IIS server
- ASP
- mysql database
- COM component

Client:

- Internet Explore
- COM component

### 6.1 Package Check List

- | -Document-|
  - | | -Web Authentication.pdf ----- This paper
- | -Admin-|
  - | | -Management ----- Tool to add/management users
  - | | -Server-|
    - | | | -ServerActiveX ----- Server COM Component
    - | | | -ServerScript ----- Server ASP scripts sample
- | -User-|
  - | | -WebActiveX ----- ActiveX at client side (browsers)
  - | | -Password ----- Tool for changing passwords

### 6.2 Management and Server Setup

The server should Windows server with COM components and ASP functions enabled.

---

### 6.2.1 User Database

The user database is MYSQL database. In this package, we provide a demo user database. In order to make the configuration easy, we store the database info in an INI file, named DBSetting.INI. If you have your own user database, please changing the record in the INI file.

All the user info related to web authentication is store in the table “Webuser”. There are 3 columns in the table, i.e. “UserName”, “UniKeyID”, and “Memo”. The SQL to construct this structure is

```
CREATE TABLE `webuser` ( `username` text NOT NULL, `unikeyid` text NOT NULL, `memo` text)
```

UserName and UniKeyID is 16 bytes long. Memo is 128 bytes string.

Here, UserName is used to store the username of legal users. This value is unique in the database.

UniKeyID is the UniKey credential generated when add a user. It is used to identify the relationship between a UniKey and a user. So each user has its own UniKeyID. Different username means different UniKeyID.

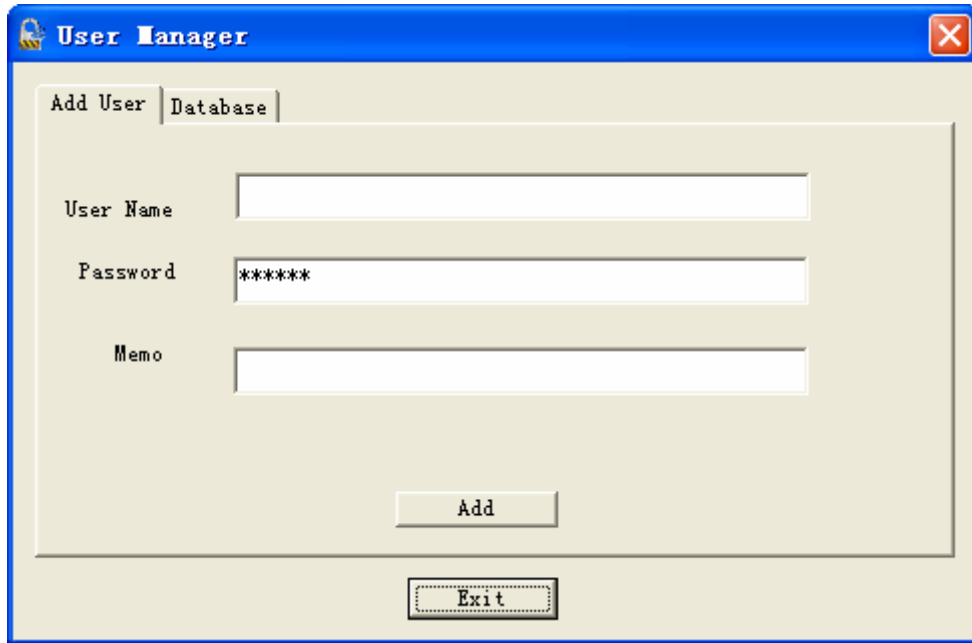
Note, end-user need not know the UniKeyID. The goal of this value is to make the authentication stronger.

### 6.2.2 User Management

User Manager.exe is to manage the web users. There 3 function enclosed in this tool, adding users, copy users and remove users.

Since the database is on the Internet, please make sure the info in the INI file is correct, and the computer has the access to the Internet.

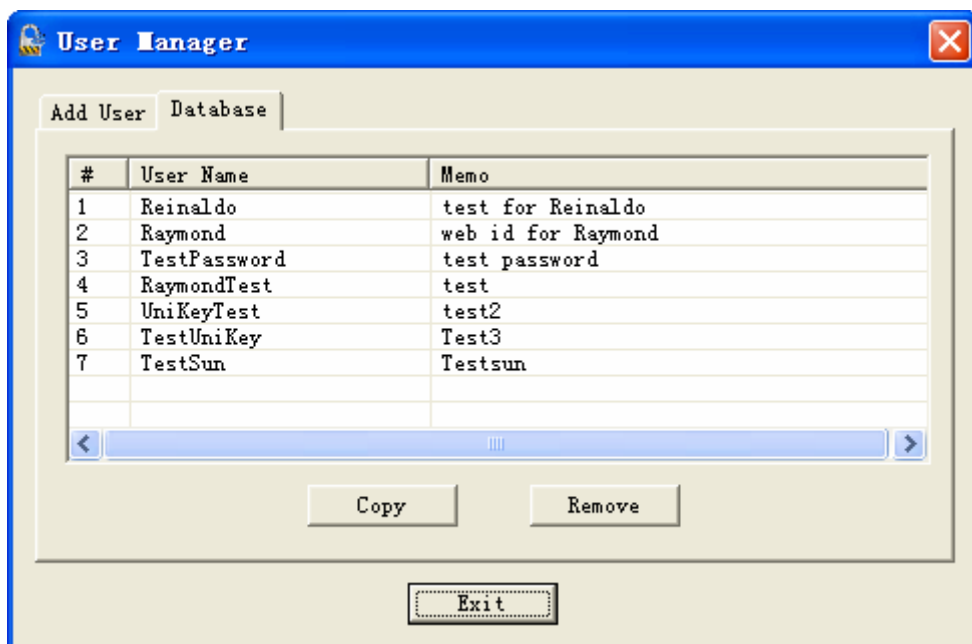
Running this tool, you can find 2 tabs, “Add user” and database.



Add User is to add a new user to the database, and burn a UniKey. Please insert a blank UniKey, and info the corresponding info. Then press “Add” to burn a UniKey and add this record into the database.

Note: The default password for authentication is “123456”. This password is different with the demo password.

If the operation failed, a warning will be shown. Otherwise, a successful message will prompt.



The database tab is to copy user info into a new UniKey or remove a user from the

---

database.

In order to copy a user, please insert a UniKey, and select a user record from the database, then press “Copy”.

Note, “copy” only copy the user info, but not password. After “copy”, the password is “123456”.

If you want to remove a user from the database, just simply select a user and press “Remove”

Note, you need not insert a UniKey when remove a user. After this removal, this user cannot logon again.

### 6.2.3 Configurating Server

UniKey Web Authentication package implements a COM component to perform the verification of web user logon. This component comes as a DLL file, named UniKeyComServerActiveX.dll. It works with Windows server with COM component function enabled.

Please copy UniKeyComServerActiveX.dll to //%WindowsPath%/System32. The INI file is storing the user database info. The INI file should be copied to //%WindowsPath%/.

Note, for Win2000, %WindowsPath is c:/winnt by default.

After copying the files, you should register the COM component by

Regsvr32 UniKeyComServerActiveX.dll
-------------------------------------

We provide RegServer.bat script to help you to copy and register the COM component.

In order to make the authentication clear, an ASP sample is provided in the package. Please copy the asp files into a folder of wwwroot. Since we want to show a clear idea of authentication, the sample is rather simple, and we even remove some HTML tags.

For the detailed authentication code, please refer to the asp files.

The logon.asp is the gateway page to start the web logon. It generates the challenge.

Verify.asp is to verify the response and determine whether this user can logon or not.

---

Demopage.asp is a normal page, shows how after user logon.

Please note, the authentication is bind with a session.

## 6.3 Client Setup

### 6.3.1 Install ActiveX (COM component)

In this package, we use an ActiveX control to working with browser, collecting UniKey info and generate the response.

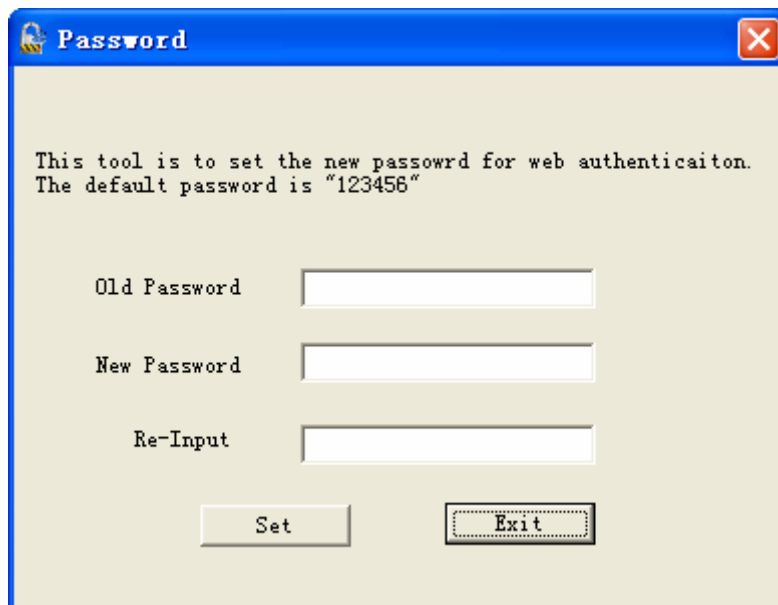
In order to active this ActiveX, please copy UniKeyComActiveX.dll to the system path, and register it. The install.bat will help you to do so.

### 6.3.2 Configurate IE

To enable this ActiveX, please setup your IE configuration. Please enable unsigned script and ActiveX.

### 6.3.3 Changing Password

Users can change the password for web logon.



The screenshot shows a Windows-style dialog box titled "Password". The text inside reads: "This tool is to set the new password for web authentication. The default password is '123456'". Below this text are three input fields labeled "Old Password", "New Password", and "Re-Input". At the bottom of the dialog are two buttons: "Set" and "Exit".

Input the old password and input the new password, then press "Set" to enable this change.