

# The SecureAuth® End-User Experience

SecureAuth is the only authentication solution that removes the burden of secure authentication from end-users and administrators. SecureAuth's unique 2-Way authentication model validates both the end-user and the server, while offering a scalable solution to millions of end-users.

This Document is organized in the following manner:

1. Overview of SecureAuth Authentication for the End-user	Page 1
2. User Experience for Device Registration (Private Mode)	Page 3
3. User Experience for subsequent authentications (Private Mode)	Page 7
4. User Experience in Public Mode	Page 9
5. SecureAuth User Authentication, IT Architecture	Page 12

## 1. Overview of SecureAuth Authentication for End User

SecureAuth® abstracts “credential management” from the end-user by using native JRE client-side technology, to perform the authentication. A secure and signed java applet is executed on the client's machine. This code is 100% server-side, which means the enterprise has no client-side code to maintain.

The end-user is not burdened by any software install such as a Microsoft Active-X, FireFox, or Apple Safari browser extension. Solutions that use these add-ons require the end-user to have administration privileges; and as a result, often break in domain deployment scenarios.

SecureAuth can operate in a non-administrative role on a browser, and have the SecureAuth client code execute in the ubiquitous Java Run Time Engine (JRE). This holds true for Microsoft and non-Microsoft environments. The SecureAuth crypto keys are securely stored in hidden files in the Java JRE.

The end-user is required to perform **no** management or porting of this credential.

SecureAuth is designed to register an end-user by using information stored in the enterprise's own directory (AD, LDAP, etc), not a dedicated data store. This information includes cell phone numbers, land phone numbers, e-mail, and other information. The end-user is guided through the registration process via the SecureAuth web work flow that creates a highly intuitive, user-friendly process (See authentication “walk-thru” below).

SecureAuth operates in (2) modes:

- Public
- Private

Public mode leaves no credential on the machine. This mode is ideal for a machine that is not owned either by the user or the issuing enterprise. For this mode the user can be configured to provide the 2<sup>nd</sup> factor via one of the various one-time-registration code methods: SMS, Telephony, E-mail, Static

PIN, Help Desk or KBA and KBQ. This method leaves no credential and utilizes no managed code. The drawback is that this has a higher-friction and the authentication takes longer to conduct.

In “private” mode, the SecureAuth server will “register” the user to the device with a X.509 private/public key pair. This key pair is stored in the JRE manage code in an encrypted file that is fingerprinted to the user and to the device. This credential can be configured to be non-functional if ported to another device.

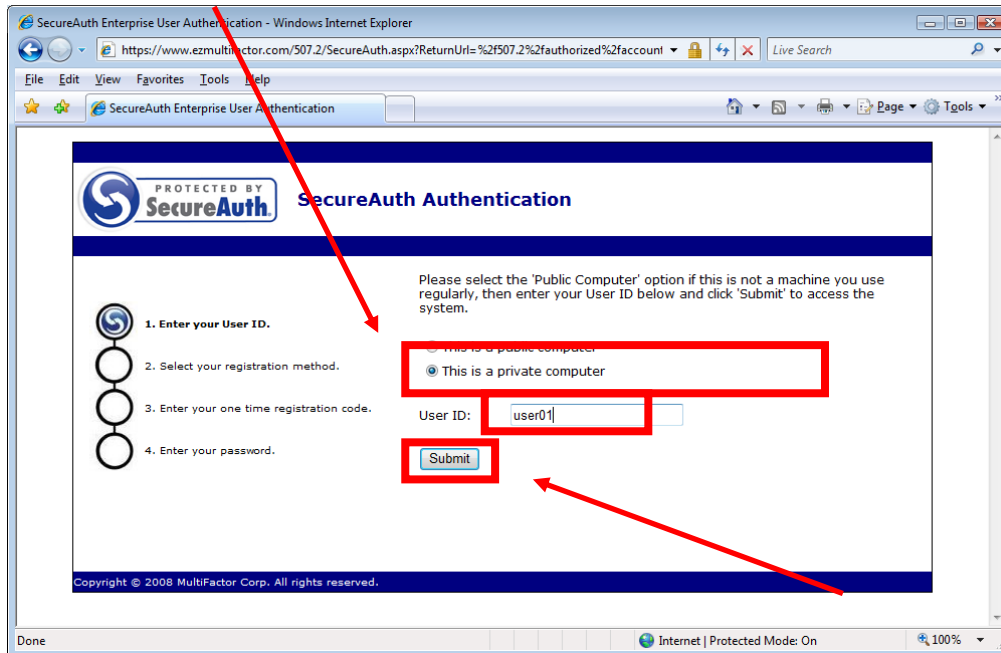
If the user attempts to use the device in “private” mode and the user does not have Java Runtime Environment (JRE) installed, the user is prompted to install the latest JRE. The user is walked through the web install.

## 2. User Experience for Device Registration (Private Mode)

This is the mode utilized when the user will be utilizing the computer again. If the machine is a “public” (non-user owned), the user should proceed to “Public Mode Usage”, **section 4**.

### 2.a. Choose “Private”, and enter ID.

This lets the authentication system know that you will be utilizing this computer again.



SecureAuth Enterprise User Authentication - Windows Internet Explorer  
https://www.ezmultifactor.com/507.2/SecureAuth.aspx?ReturnUrl=%2f507.2%2fauthorized%2faccount

PROTECTED BY **SecureAuth** Authentication

Please select the 'Public Computer' option if this is not a machine you use regularly, then enter your User ID below and click 'Submit' to access the system.

1. Enter your User ID.
2. Select your registration method.
  - This is a public computer
  - This is a private computer
3. Enter your one time registration code.
4. Enter your password.

User ID:

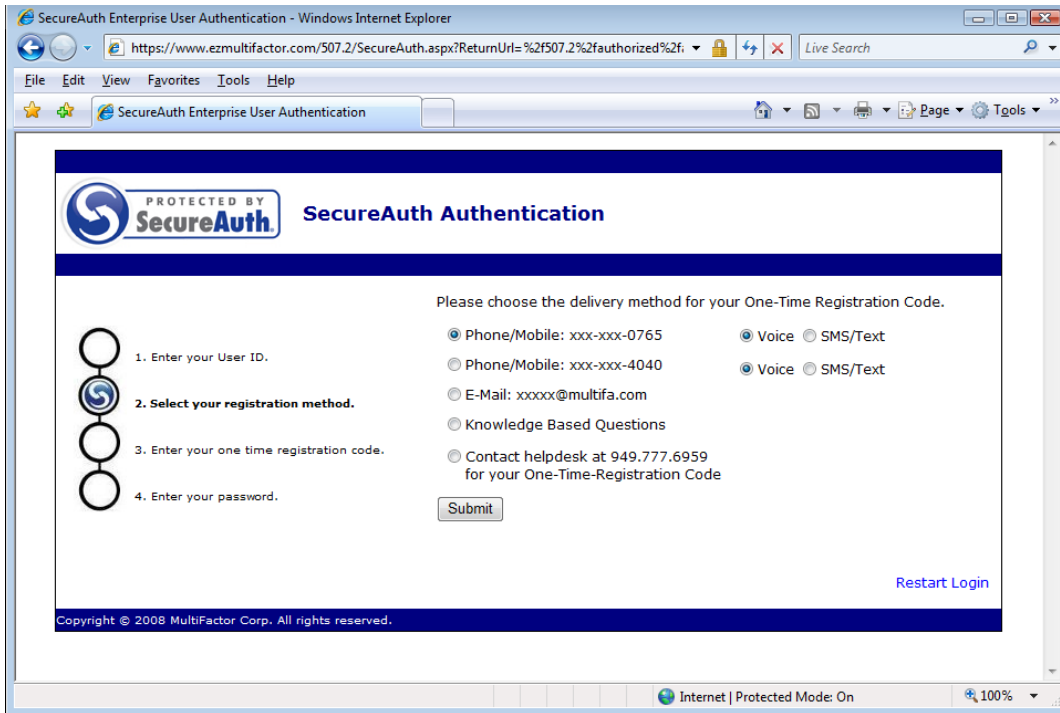
Copyright © 2008 MultiFactor Corp. All rights reserved.

Done Internet | Protected Mode: On 100%

### 2.b. Choose Your registration Method:

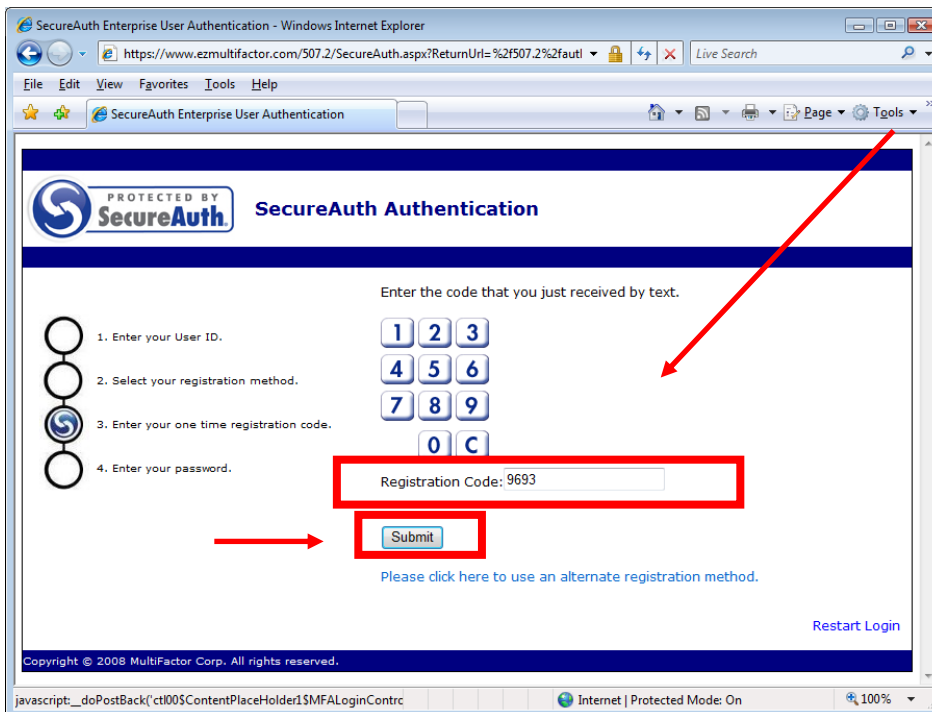
#### Possible:

1. Phone/Mobile – “One-Time-Registration code” Telephony
2. Phone/Mobile - “One-Time-Registration code” SMS
3. E-mail: - E-mail “One-Time-Registration code”
4. PIN: - Static PIN
5. Help Desk - Help Desk OTP
6. KBA - Knowledge based Authentication – Questions/Answers

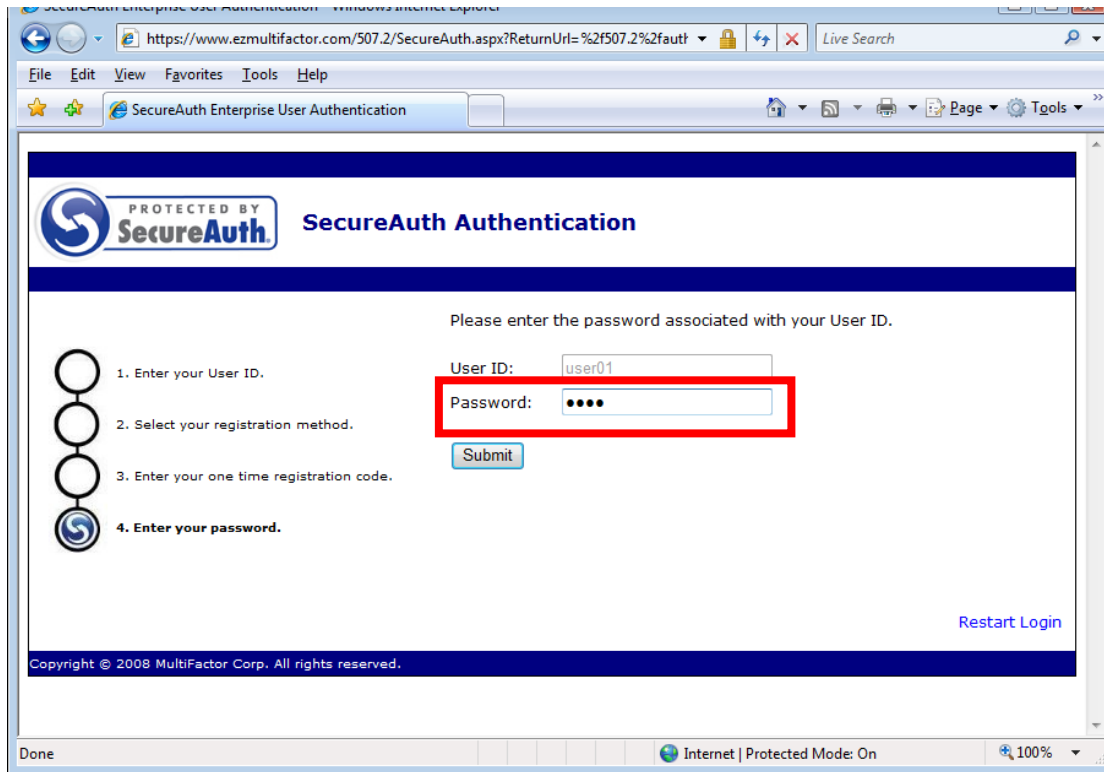


### 1.c. Enter your 1-time Registration Code

You can use the Pin-Pin or type the 4 digits in the field next to “Registration Code”, then click “Submit”.

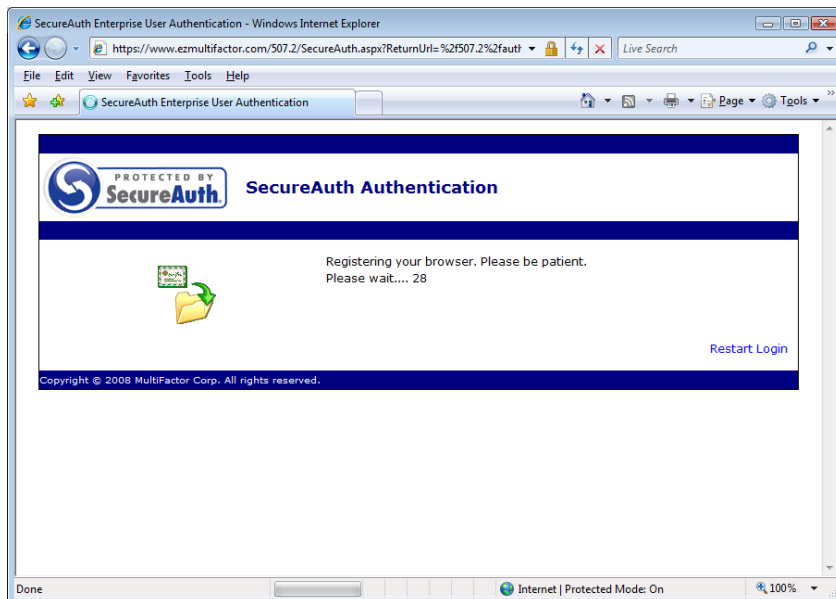


### 1.d. User enters their directory password



### 1.e. Browser becomes registered.

SecureAuth registers the user's browser, process is usually under 10 seconds.



### 1.f. User is granted access



SecureAuth Health Care Accounts

[About Us](#) | [Locations](#) | [Contact Us](#) | [Careers](#) | [Site Map](#)

SecureAuth Login 

**Log Out**

Last login: 01/28/2009

Your Accounts

- [View Accounts](#)
- [Transfer Funds](#)
- [Pay Bills](#)
- [Update Profile & Settings](#)

Account Name	Account Type	Available Balance	Ledger Balance
<a href="#">Personal Checking - 0411</a>	Checking	\$3,187.38	\$3,187.38
<a href="#">Online CD - 8905</a>	Savings	\$20,560.10	\$20,560.10
<a href="#">ATM Access Savings - 9432</a>	Savings	\$12,855.21	\$12,855.21
<a href="#">Roth IRA - 4323</a>	Retirement	\$50,320.00	\$50,320.00

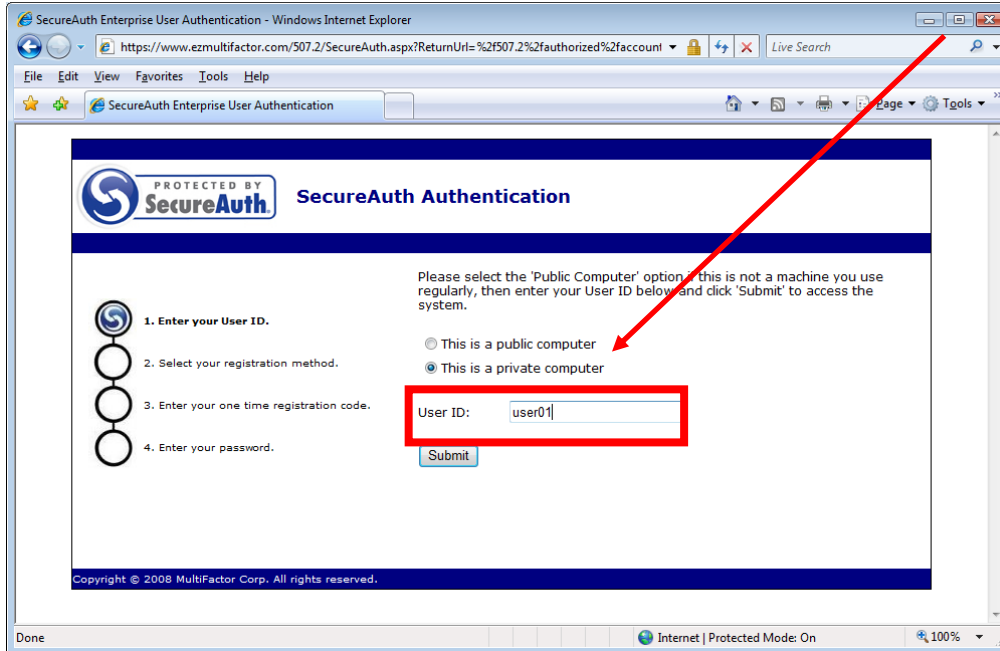
PROTECTED BY  **SecureAuth**

Done | Internet | Protected Mode: On | 100%

### 3. User Experience for Subsequent Authentications (Private Mode)

The browser is now registered to this user, subsequent authentications require no registration.

#### 3.a. Insure that the Browser Button is set to “Private” and enter “ID”



SecureAuth Enterprise User Authentication - Windows Internet Explorer

https://www.ezmultifactor.com/507.2/SecureAuth.aspx?ReturnUrl=%2f507.2%2fauthorized%2faccount

SecureAuth Authentication

PROTECTED BY SecureAuth

Please select the 'Public Computer' option if this is not a machine you use regularly, then enter your User ID below and click 'Submit' to access the system.

1. Enter your User ID.

2. Select your registration method.

3. Enter your one time registration code.

4. Enter your password.

This is a public computer

This is a private computer

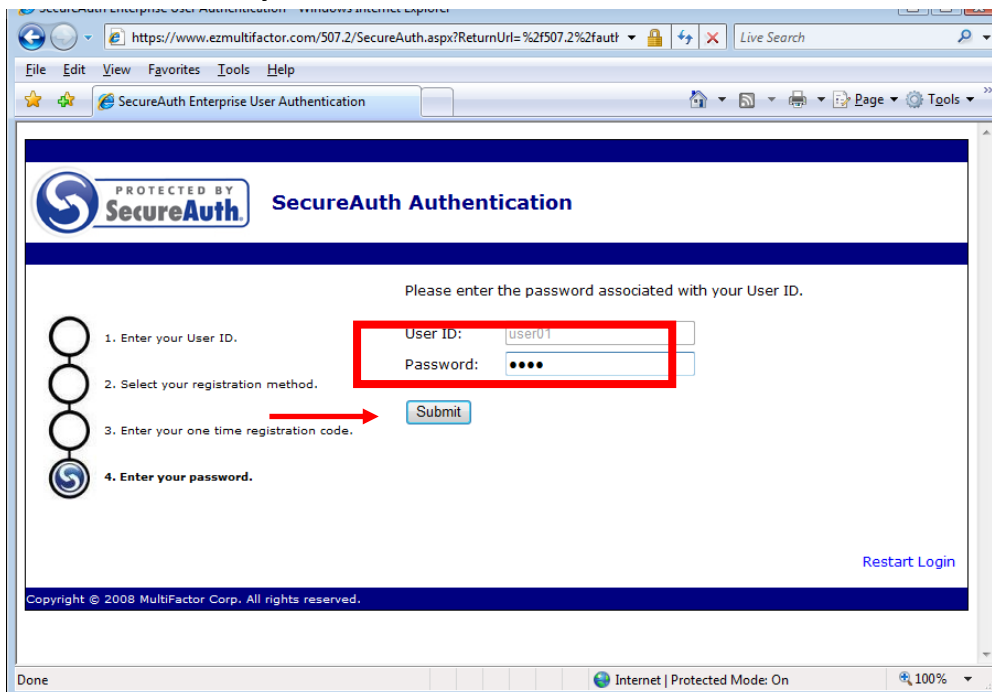
User ID: user01

Submit

Copyright © 2008 MultiFactor Corp. All rights reserved.

Done Internet | Protected Mode: On 100%

#### 3.b. Enter Directory Password and then click “Submit”:



SecureAuth Enterprise User Authentication - Windows Internet Explorer

https://www.ezmultifactor.com/507.2/SecureAuth.aspx?ReturnUrl=%2f507.2%2faut

SecureAuth Authentication

PROTECTED BY SecureAuth

Please enter the password associated with your User ID.

1. Enter your User ID.

2. Select your registration method.

3. Enter your one time registration code.

4. Enter your password.

User ID: user01

Password: ●●●●

Submit

Restart Login

Copyright © 2008 MultiFactor Corp. All rights reserved.

Done Internet | Protected Mode: On 100%

### 3.c. User is allowed access.



SecureAuth Health Care Accounts

[About Us](#) | [Locations](#) | [Contact Us](#) | [Careers](#) | [Site Map](#)

SecureAuth Login 

**Log Out**

Last login: 01/28/2009

Your Accounts

- [View Accounts](#)
- [Transfer Funds](#)
- [Pay Bills](#)
- [Update Profile & Settings](#)

Account Name	Account Type	Available Balance	Ledger Balance
Personal Checking - 0411	Checking	\$3,187.38	\$3,187.38
Online CD -8905	Savings	\$20,560.10	\$20,560.10
ATM Access Savings -9432	Savings	\$12,855.21	\$12,855.21
Roth IRA -4323	Retirement	\$50,320.00	\$50,320.00

PROTECTED BY  **SecureAuth.**

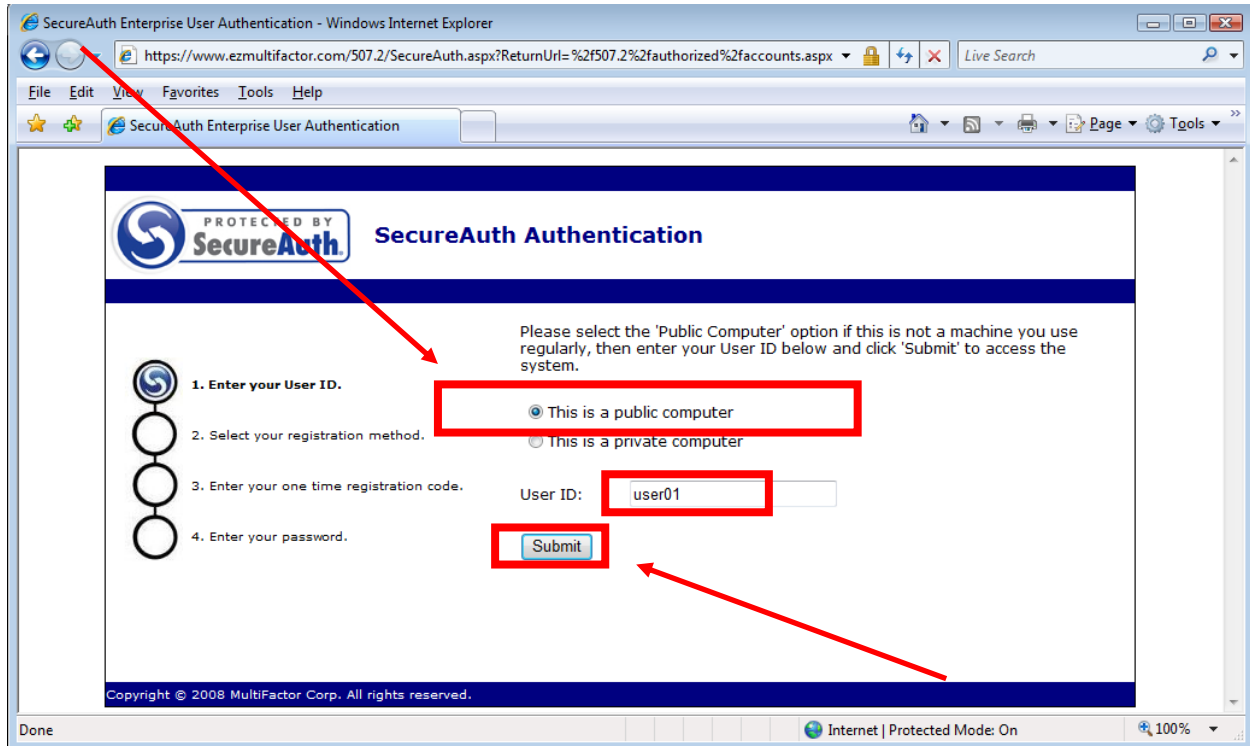
Done Internet | Protected Mode: On 100%

## 4. User Experience in Public Mode

If the machine is a “public” machine, e.g. one that the user does not own – the user should click the “public” browser button in step 4.a.

### 4.a. Choose “Public”, and enter ID.

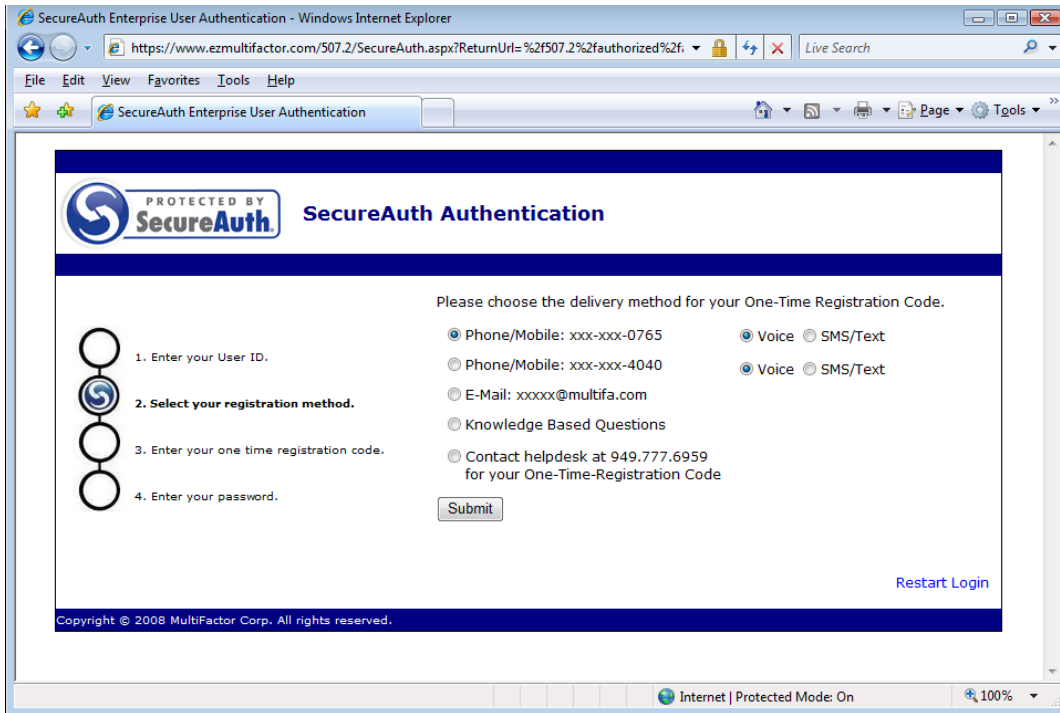
This lets the authentication system know that you will be utilizing this computer again.



### 4.b. Choose your authentication Method:

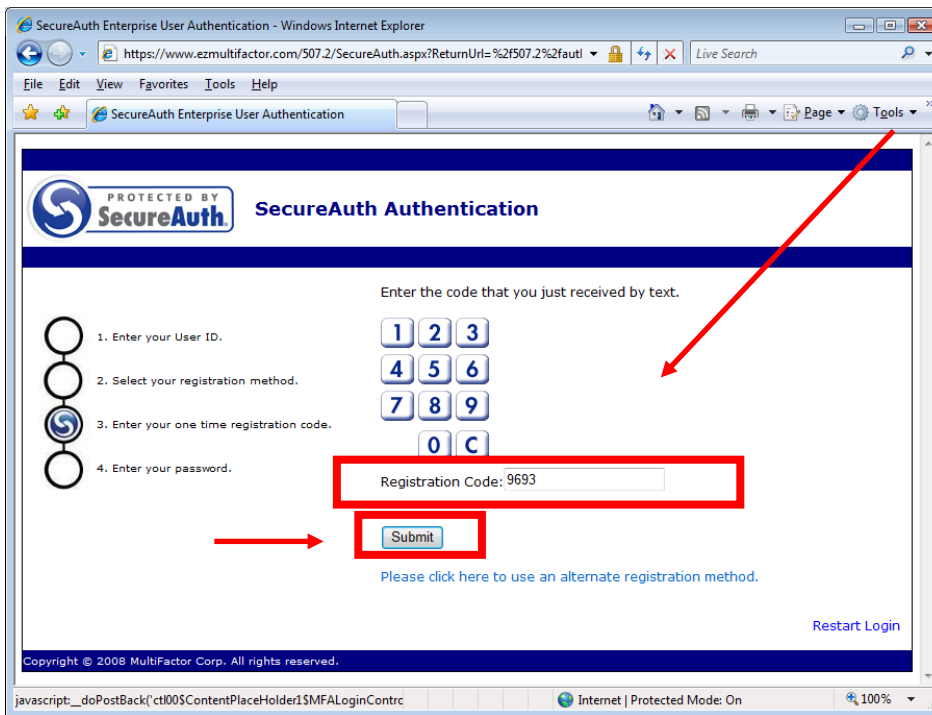
#### Possible:

1. Phone/Mobile – “One-Time-Registration code” Telephony
2. Phone/Mobile - “One-Time-Registration code” SMS
3. E-mail: - E-mail “One-Time-Registration code”
4. PIN: - Static PIN
5. Help Desk - Help Desk OTP
6. KBA - Knowledge based Authentication – Questions/Answers

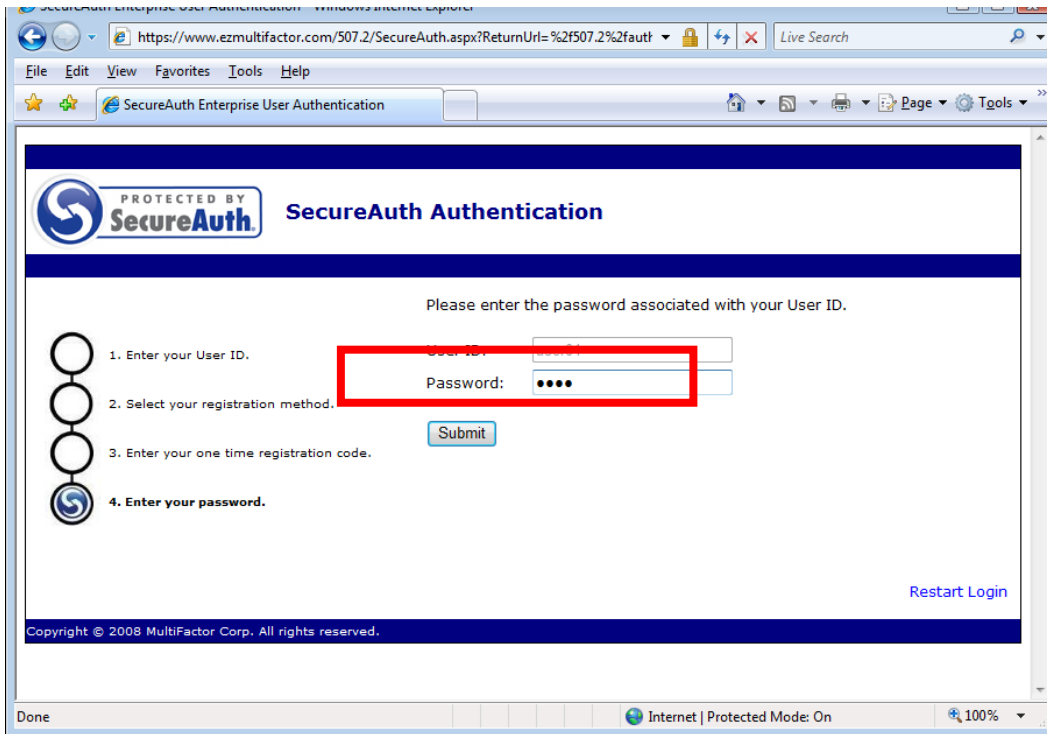


#### 4.c. Enter your 1-time Registration Code

You can use the Pin-Pin or type the 4 digits in the field next to “Registration Code”, then click “Submit”.



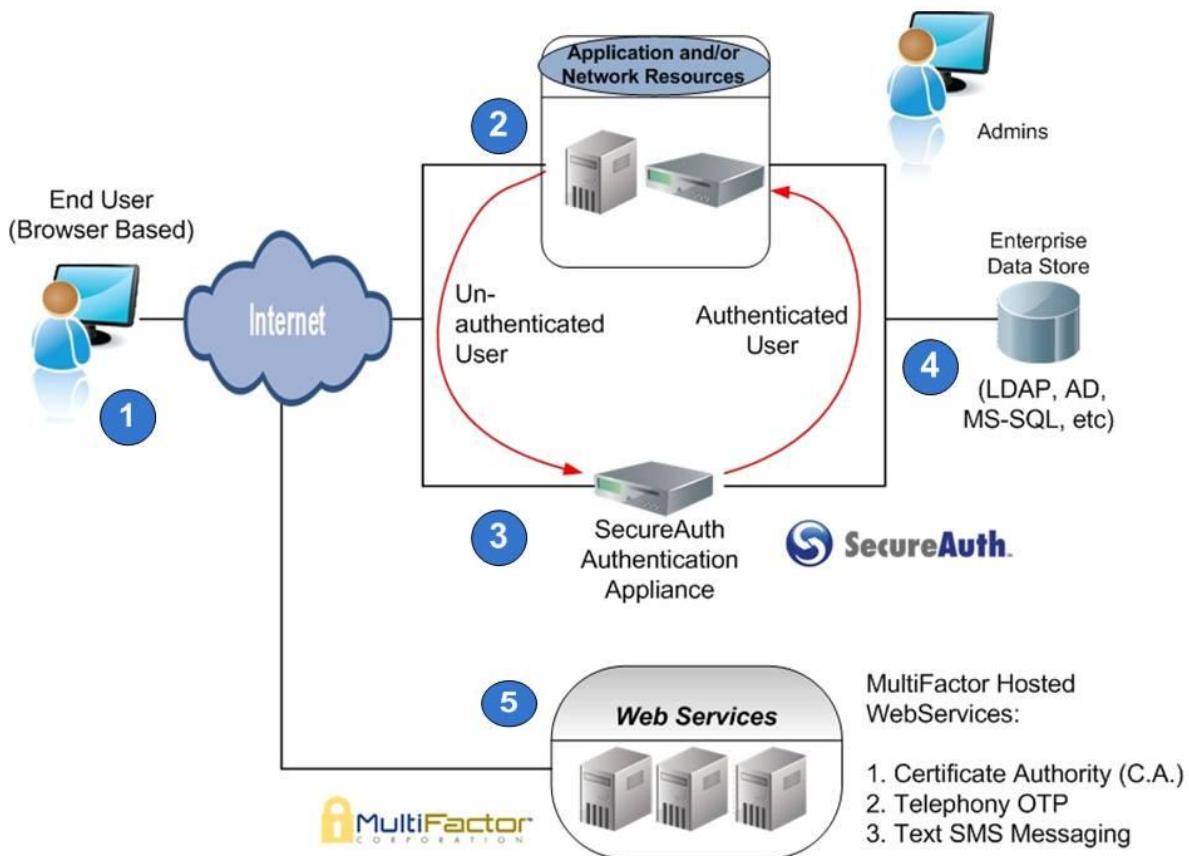
#### 4.d. User enters their directory password



#### 4.e. User is granted access



## 5. SecureAuth for User Authentication and Validation - Architecture



- 1 The end-user experience is 100% browser based. The end-user identifies his machine as either a private computer or a public computer, and enters his UserID .
- 2 The SecureAuth® authentication solution is an external mechanism that does NOT need to be integrated into the application or network appliance. The application or network appliance redirects the unauthenticated user to SecureAuth®.
- 3 The SecureAuth® authentication appliance authenticates the user and redirects him back to the application.
- 4 SecureAuth® utilizes the enterprise's native data store for account validation.
- 5 SecureAuth® can utilize SecureAuth's web services.