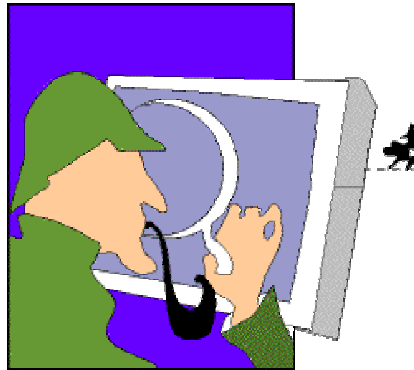


Highly Auditable Self-Service Life-Cycle Management for Electronic Security Credentials

Presentation by: Peter Tapling, Authentify, Inc.



2003 Annual Computer Security Applications Conference

Las Vegas, Nevada

Abstract

- » Userid's, digital certificates, one-time password tokens, smart cards -- whatever the form of electronic security credential, the purpose for the credential is to attempt to bind an individual to a given user profile on the network. The majority of an organization's cost to support a credential is in profile management -- the registration for and issuance of the credential and re-credentialing activities over the live of the credential (e.g. password reset) and authentication around those events. One way to reduce these costs is to have users "self-provision" the credentials. But how is it possible to do this in a trusted and auditable way? This session will present an approach to real time auditable self-service registration and discuss how two companies have implemented the approach -- one for PKI and the other for userid/password.

Case Study Applications

» Chicago Software Association

- Registration for access to “Members Only” section of web site
- Authentication for password reset
- Authorization for event/profile maintenance requests

» Hewlett Packard

- Business Partner Internet Access PKI (BPIA) application
- Issuance of digital certificates (VeriSign MPKI) to HP business partners for access to a secured extranet
- Recognized in Computerworld 2003 *CW Heroes* program
 - https://secure.cwheroes.org/briefingroom_2003/pdf_frame/index.asp?id=4484

Typical Registration Process for an Electronic Security Credential

- 1) Subject informed of eligibility
- 2) Subject requests credential
- 3) Authority vets individual/request
- 4) Authority approves request
- 5) Credential is activated
- 6) Subject receives credential

The trick is to bridge the silicon/carbon divide.

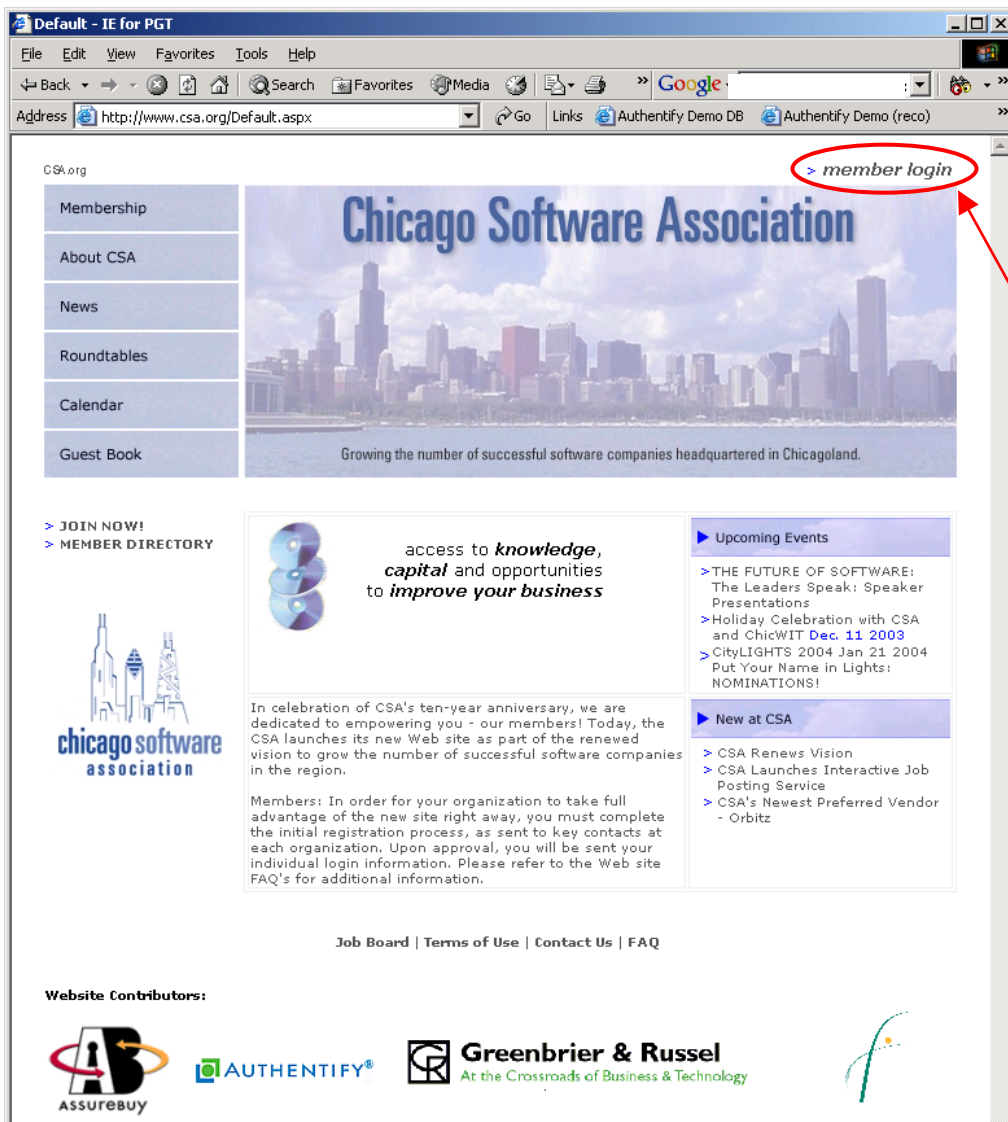
Challenges of Any Registration Process

- » Objective is to bind a carbon based persona to a credential
 - The **task** was performed user ID “dduck”, therefore the **person** who performed the task was [certainly] Donald Duck.

- » Policies define process requirements
 - Policy will (should) reflect risk profile
 - [PKI has inherited some legal baggage (e.g. CPS)]
- » Authentication for first time issuance is weak link
 - Shared secret only not near strong enough
 - “Personal presence” models prevalent, but operationally weak
- » Delegation is often required to support broad communities
- » Automation is desired to keep costs down

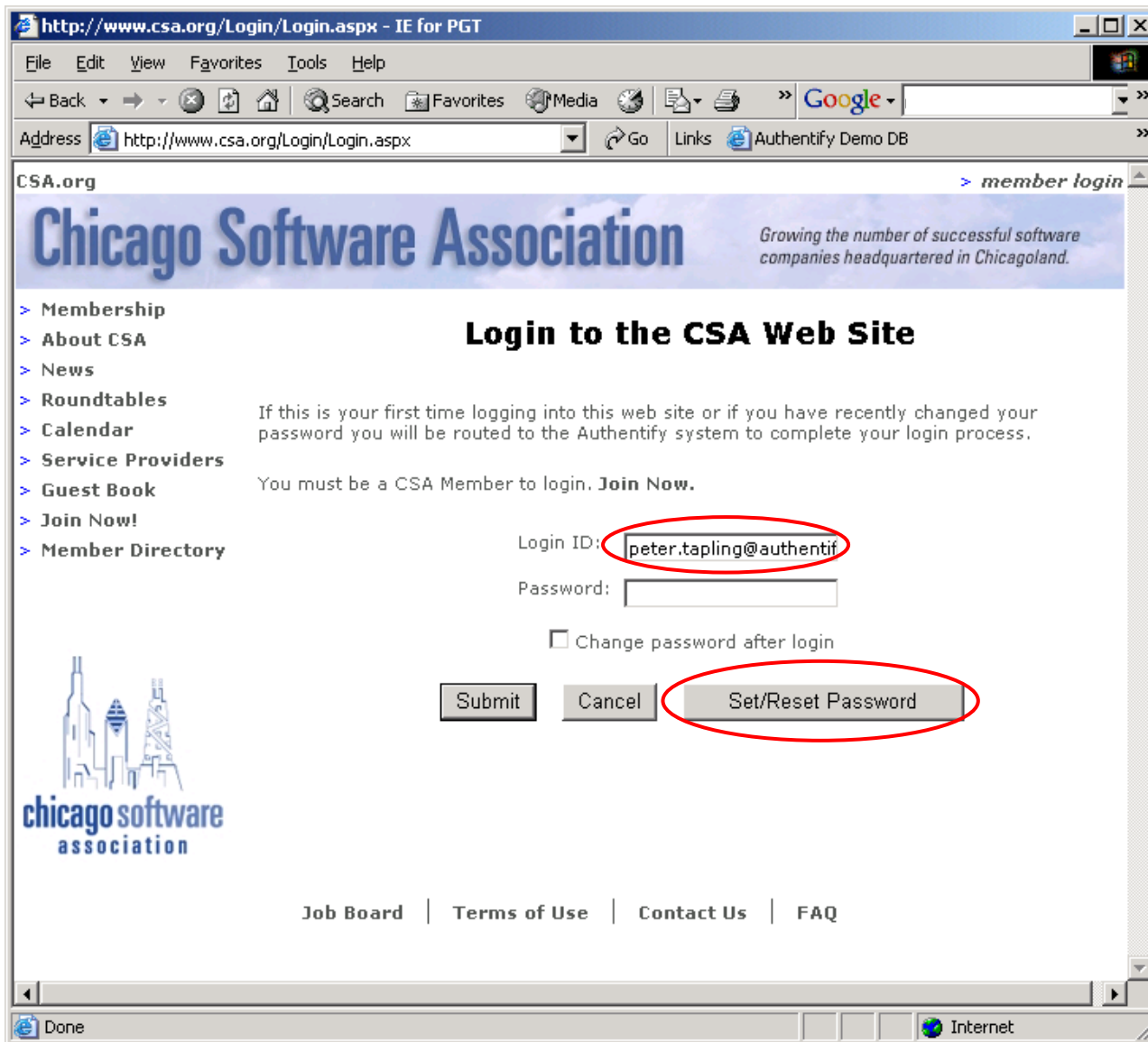
Chicago Software Application Web Registration

- » Fully self service approach for member registration
- » Moderate risk [relatively] application
- » Supports multiple functions
 - Registration
 - Password reset
 - Transaction Authorization



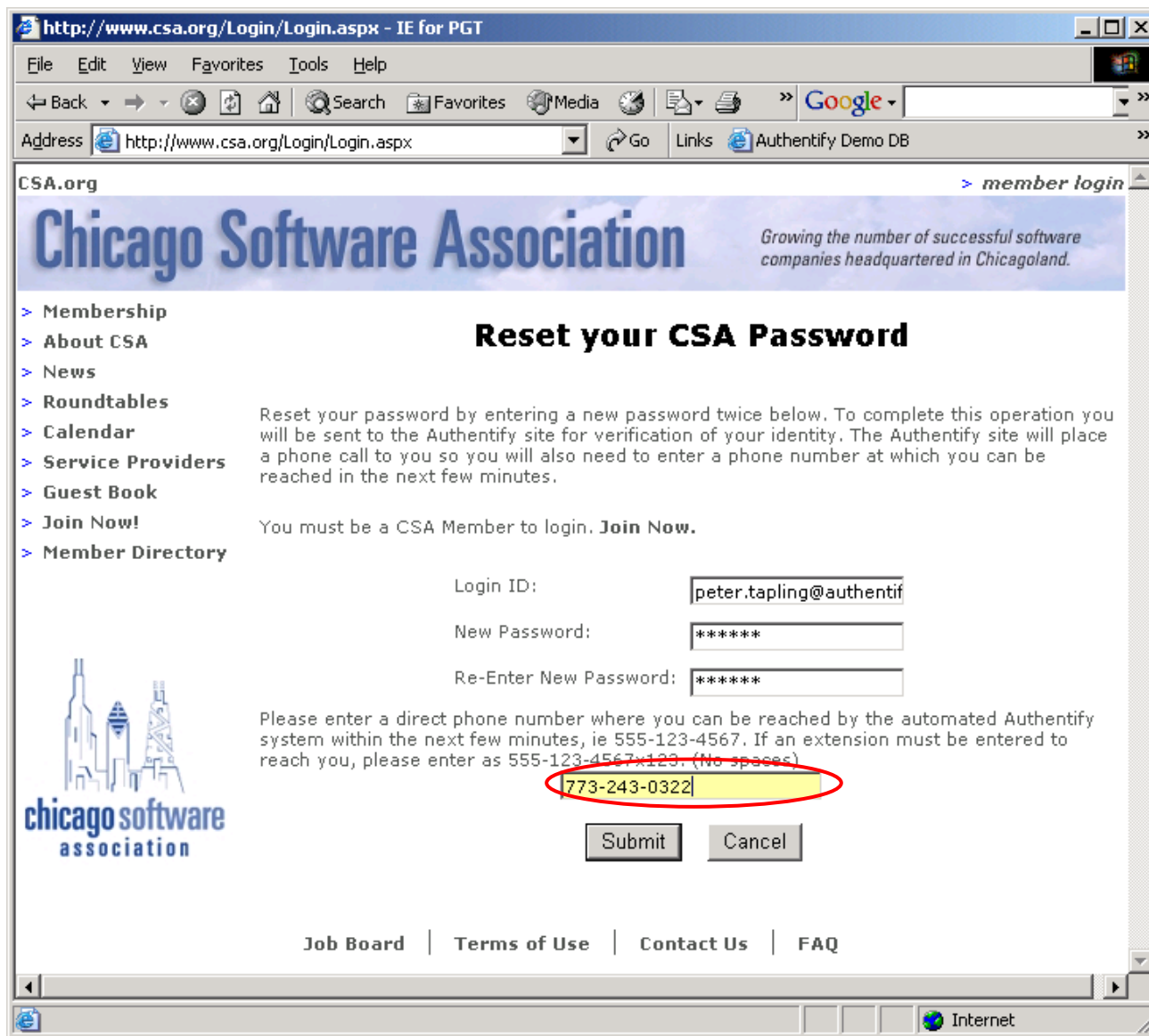
CSA is a regional association of software companies, service providers and end user organizations in the Midwest supporting 2000+ member organizations across 5 states.

The web site provides a "members only" area to manage member profile information and to support sign up for members only events.



Self-administration for password reset and profile maintenance has saved CSA ½ FTE.

Email address must already exist in their system – a light form of delegation.



http://www.csa.org/Login/Login.aspx - IE for PGT

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Google

Address http://www.csa.org/Login/Login.aspx Go Links Authentify Demo DB

CSA.org [member login](#)

Chicago Software Association

Growing the number of successful software companies headquartered in Chicagoland.

- > Membership
- > About CSA
- > News
- > Roundtables
- > Calendar
- > Service Providers
- > Guest Book
- > Join Now!
- > Member Directory

Reset your CSA Password

Reset your password by entering a new password twice below. To complete this operation you will be sent to the Authentify site for verification of your identity. The Authentify site will place a phone call to you so you will also need to enter a phone number at which you can be reached in the next few minutes.

You must be a CSA Member to login. [Join Now.](#)

Login ID:

New Password:

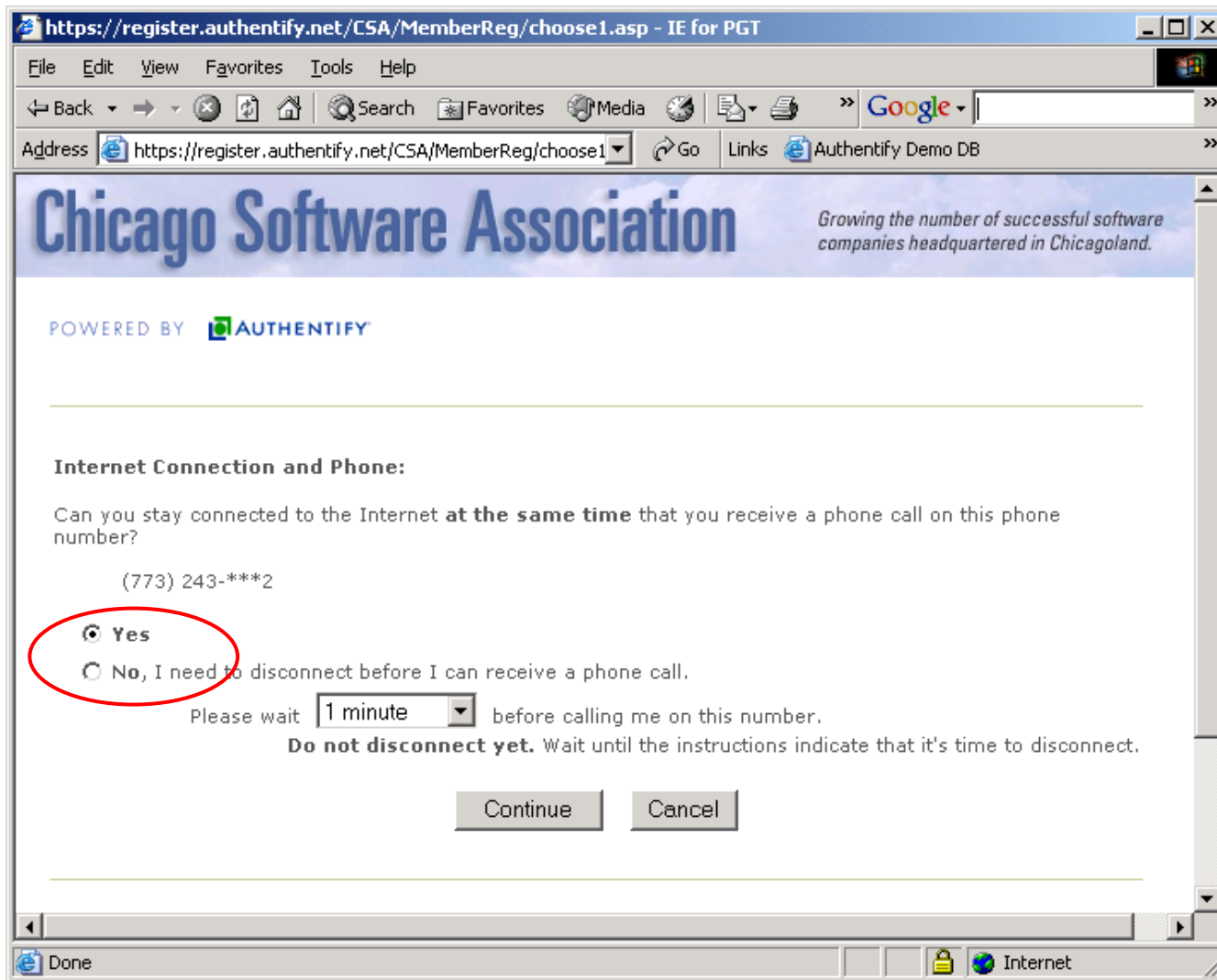
Re-Enter New Password:

Please enter a direct phone number where you can be reached by the automated Authentify system within the next few minutes, ie 555-123-4567. If an extension must be entered to reach you, please enter as 555-123-4567x123. (No spaces)

[Job Board](#) | [Terms of Use](#) | [Contact Us](#) | [FAQ](#)

Internet

Self-selected phone number reflects limited risk profile of application.



https://register.authentify.net/CSA/MemberReg/choose1.asp - IE for PGT

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print

Address https://register.authentify.net/CSA/MemberReg/choose1 Go Links Authentify Demo DB

Chicago Software Association

Growing the number of successful software companies headquartered in Chicagoland.

POWERED BY AUTHENTIFY

Internet Connection and Phone:

Can you stay connected to the Internet **at the same time** that you receive a phone call on this phone number?

(773) 243-***2

Yes

No, I need to disconnect before I can receive a phone call.

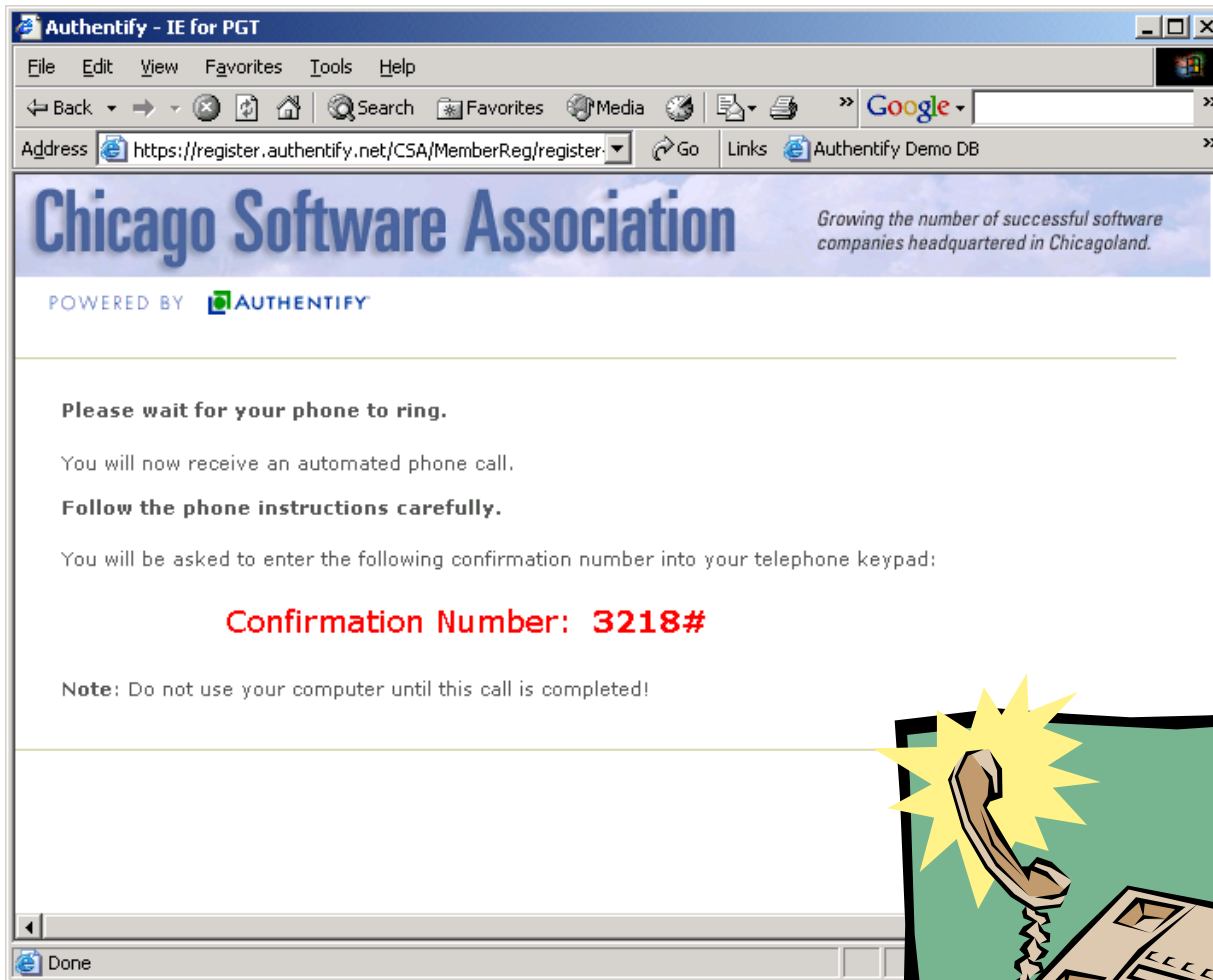
Please wait before calling me on this number.

Do not disconnect yet. Wait until the instructions indicate that it's time to disconnect.

Done Internet

Employ Authentify's patent-pending process to enable telephone as an "out of band" network.

Process determines ability of user to answer phone and stay connected to Internet. (Process works either way, answer merely defines flow.)



Authentify - IE for PGT

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Google

Address <https://register.authentify.net/CSA/MemberReg/register> Go Links Authentify Demo DB

Chicago Software Association

Growing the number of successful software companies headquartered in Chicagoland.

POWERED BY AUTHENTIFY

Please wait for your phone to ring.

You will now receive an automated phone call.

Follow the phone instructions carefully.

You will be asked to enter the following confirmation number into your telephone keypad:

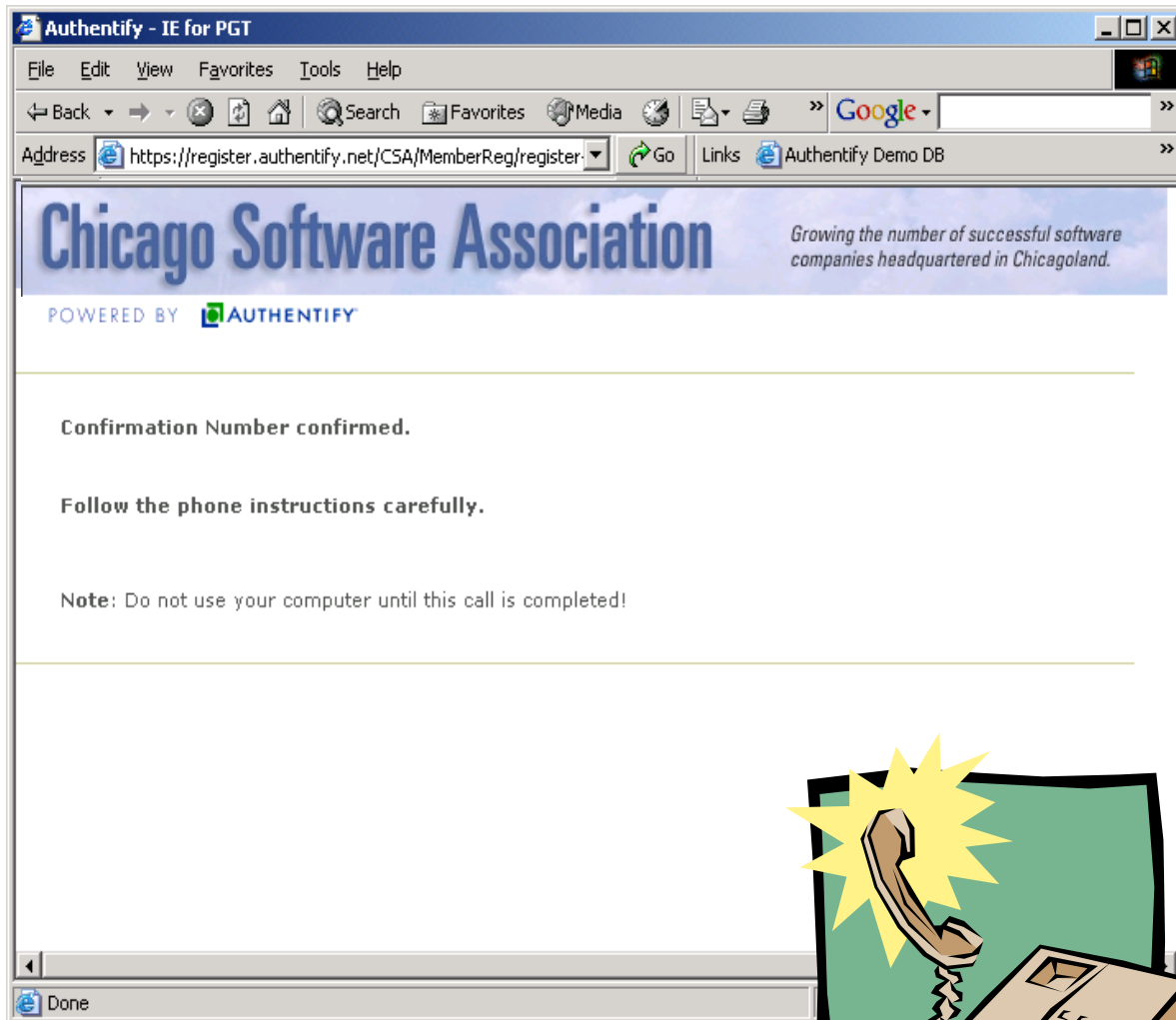
Confirmation Number: 3218#

Note: Do not use your computer until this call is completed!



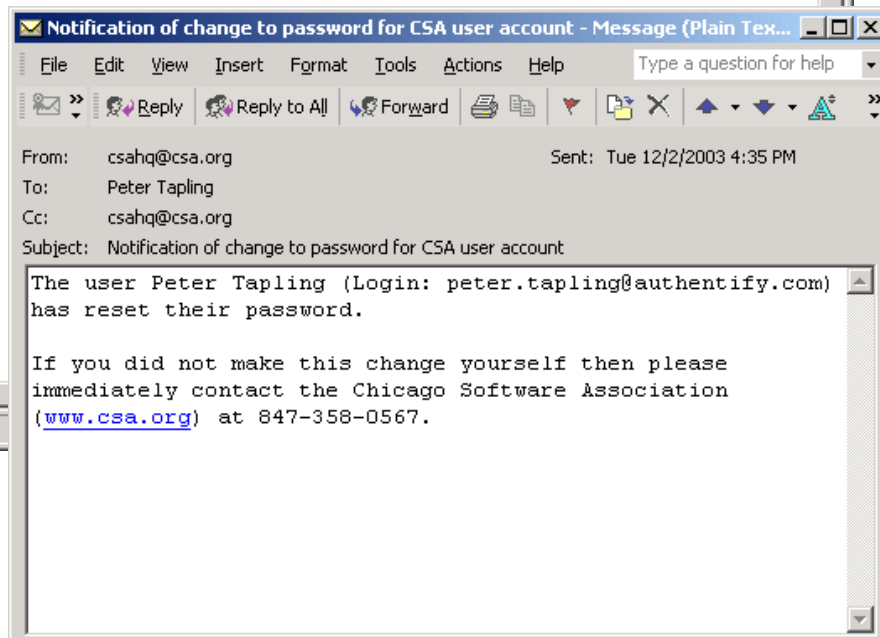
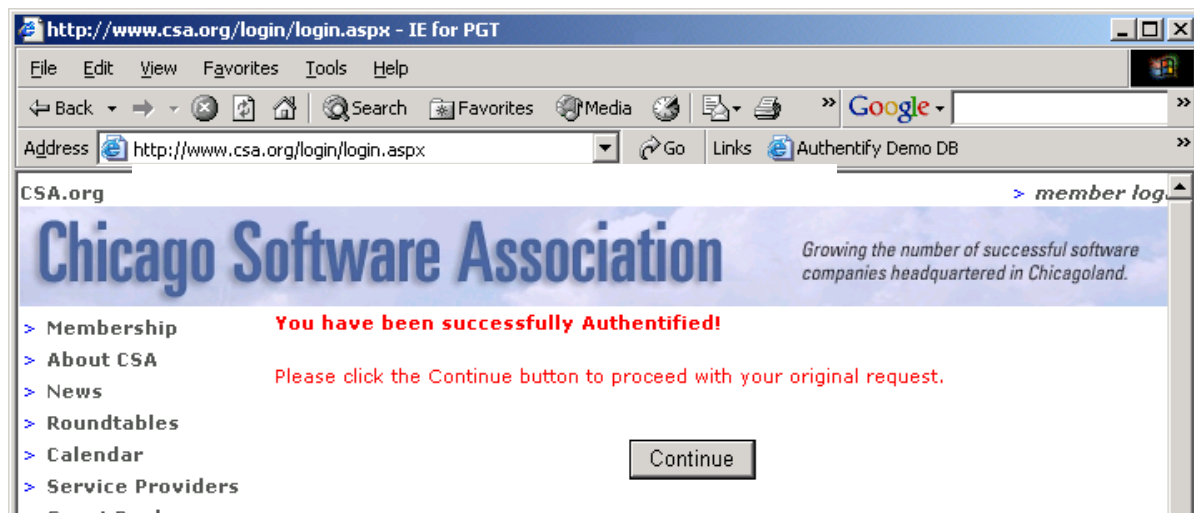
Authentify process uniquely binds an Internet session with the telephone call.

Voice Prompt:
"Please locate the confirmation number on the screen and enter it into the keypad of the telephone."



Telephone allows for direct interaction with a human – capture data, deliver data, capture voice recording or voice biometric.

Voice Prompt:
"Please speak your name and company."



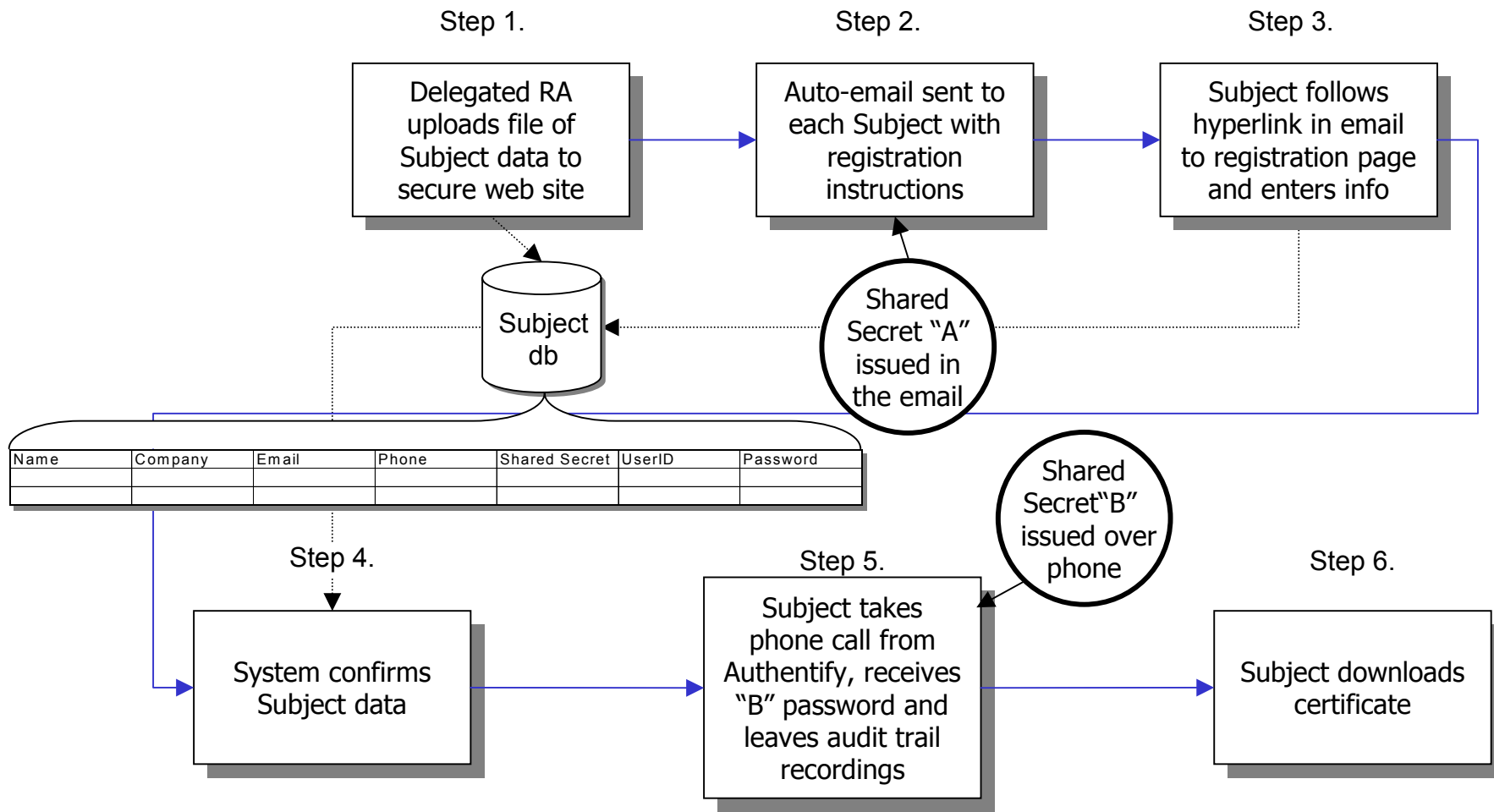
Subject inputs the data received from the two communications channels (phone, email) into a web-based certificate request form.

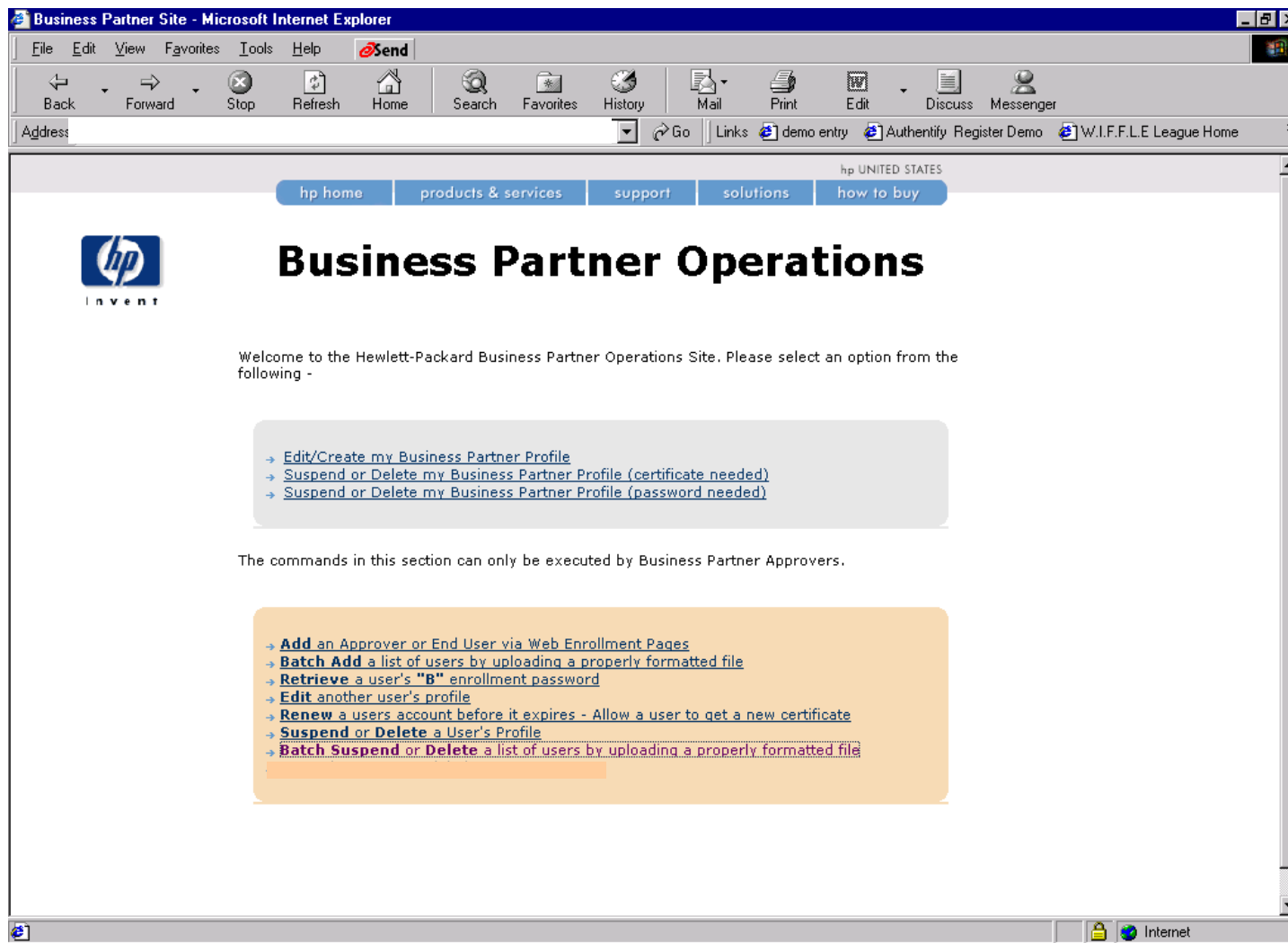
Telephone prompts:
“Thank you. Please complete the process via the web forms.”

HP BPIA application

- » “Delegated administration” approach
- » Two “faces” to the automated registration system
 - Administrative Application
 - Subject (end user) experience
- » Functions of Administrative Application
 - Add Delegated RA or Subject
 - Retrieve a shared secret for a Subject
 - Edit/renew/suspend a Subject’s profile
 - Enable “batch” processing

Telephone as Foundation a PKI Registration Process





Business Partner Site - Microsoft Internet Explorer


File Edit View Favorites Tools Help Send

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss Messenger

Address Go Links demo entry Authentify Register Demo W.I.F.F.L.E League Home

hp UNITED STATES

hp home products & services support solutions how to buy



Business Partner Operations

Welcome to the Hewlett-Packard Business Partner Operations Site. Please select an option from the following -

- [Edit/Create my Business Partner Profile](#)
- [Suspend or Delete my Business Partner Profile \(certificate needed\)](#)
- [Suspend or Delete my Business Partner Profile \(password needed\)](#)

The commands in this section can only be executed by Business Partner Approvers.

- [Add an Approver or End User via Web Enrollment Pages](#)
- [Batch Add a list of users by uploading a properly formatted file](#)
- [Retrieve a user's "B" enrollment password](#)
- [Edit another user's profile](#)
- [Renew a users account before it expires - Allow a user to get a new certificate](#)
- [Suspend or Delete a User's Profile](#)
- [Batch Suspend or Delete a list of users by uploading a properly formatted file](#)

Internet


Sample
Admin home
page

Add New User - Microsoft Internet Explorer

File Edit View Favorites Tools Help Send

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss Messenger

Address demo entry Authentify Register Demo W.I.F.F.L.E League Home



Business Partner Operations

Add New User or Approver

[Return to Main Page](#)

Add New User or Approver

Please provide the following information. Fields marked with an asterisk (*) **must** be filled in. All other fields are optional.

Is this user an approver? Yes No

Email Address*:

First (Given) Name: Last Name*:

Telephone Number*: DUNS Number (if different from headquarters DUNS):

Country*: US State (if applicable):

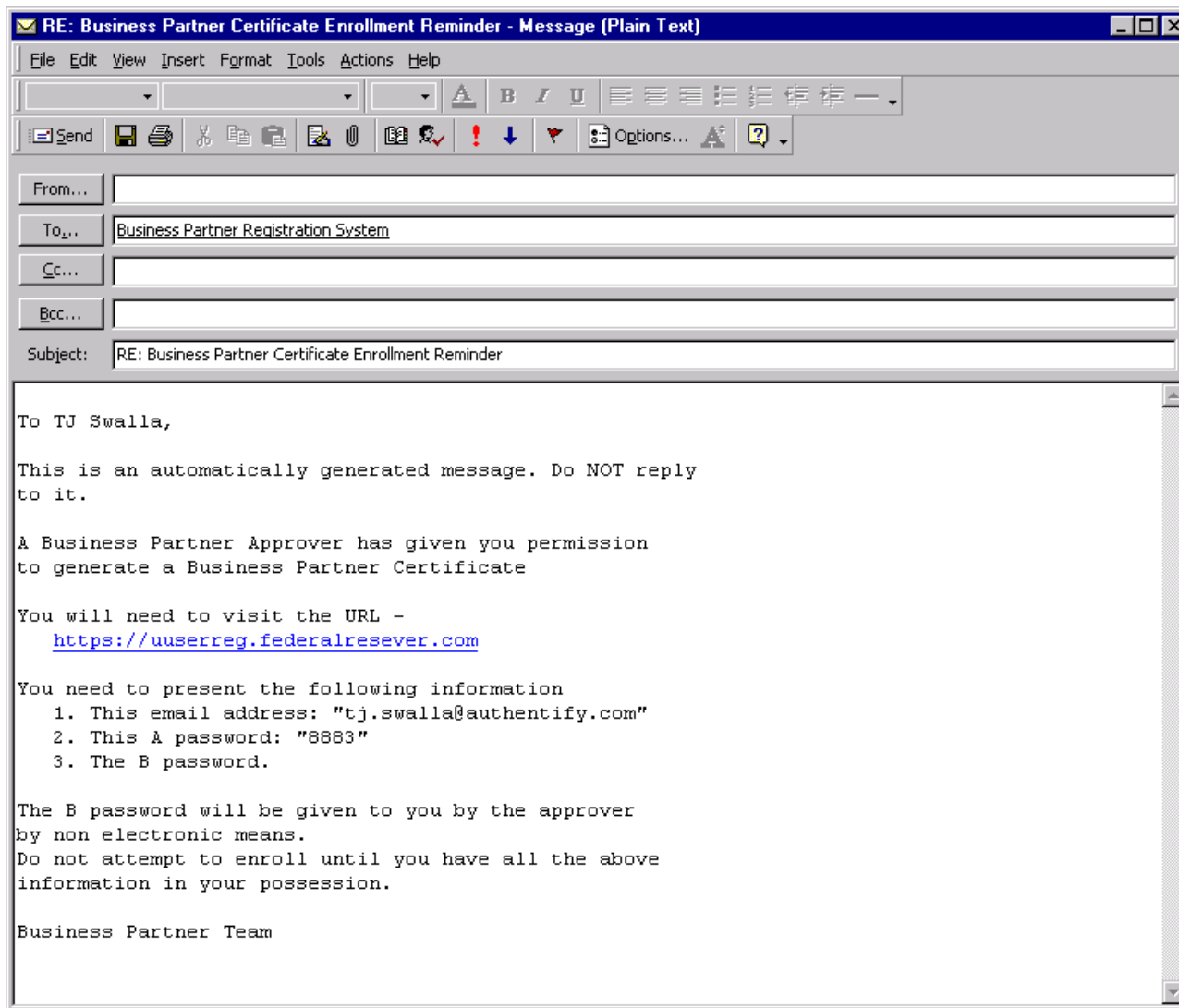
Main Role*: Auxiliary Roles: (see Note below)

Buyer Limit (may not apply):

Note: To select multiple Auxiliary Roles, Windows users must hold the **Ctrl** key and click on each role entry; Mac users must hold the **Command** key and click on each role entry. To unselect an Auxiliary Role, Windows users must hold the **Ctrl** key and click on the selected role entry; Mac users must hold the **Command** key and click on the selected role entry.

Done Internet

Sample Admin page – this page allows Delegated RA to “sponsor” Subjects to receive a certificate the application



First, the intro email with the a "A" password.

Email explains process, directs Subject to URL to continue process.



Business Partner Site - Microsoft Internet Explorer

File Edit View Favorites Tools Help Send

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss Messenger

Address Go Links demo entry Authentify Register Demo >>

hp UNITED STATES

hp home products & services support solutions how to buy

 **Business Partner Operations**

Delivery of the B Password via the telephone

Fill in the e-mail address field and you will be contacted at the telephone number registered by your administrator. The information marked with a "*" is included in your Digital ID and is available to the public.

Your E-mail Address: * (required)

(example -- jbdoe@verisign.com)

 If the information above is correct, click Submit to continue.

Submit Cancel

[privacy statement](#) [legal notices](#) © 1994-2001 hewlett-packard company

Error on page. Internet

Subject asserts identity by entering info, e.g. email address.

Subject is notified that they will receive "B" password via the telephone.



Subject is instructed to accept a phone call at a number trusted by the Delegated RA.



Business Partner Site - Microsoft Internet Explorer

File Edit View Favorites Tools Help eSend

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss

Address Go Links demo entry

hp UNITED STATES

hp home products & services support solutions how to buy

 **Business Partner Operations**

You will now receive an automated telephone call and your B password will be read to you over the telephone.

Please do not use this computer until your call is completed!

[privacy statement](#) [legal notices](#) © 1994-2001 hewl

Done

A call is placed and the “B” password is read to the Subject over the phone and an audit trail recording is captured.

Telephone prompts:

“Your B password is X123.”

...

“Please speak your telephone number.”

Subject inputs the data received from the two communications channels (phone, email) into a web-based certificate request form.

Microsoft end-user Enrollment - Microsoft Internet Explorer

File Edit View Favorites Tools Help eSend

Back Forward Stop Refresh Home Search Favorites History Mail Print

Address Go Links demo entry


Complete Enrollment Form

Information for the Digital ID
Fill in all fields. Use only the English alphabet with no accented characters. The information marked with a "*" is included in your Digital ID and is available to the public.

Your E-mail Address: * (required) (example -- jbdoe@verisign.com)	<input type="text"/>
Password "A" that was e-mailed to you: (required)	<input type="text"/>
Password "B" that was given to you by your approver: (required)	<input type="text"/>
Please type the phrase "I Agree": (required)	<input type="text"/>

Digital ID Subscriber Agreement
By applying for, submitting, or using a Digital ID you are agreeing to the terms of the Verisign Subscriber Agreement, located at:

<https://onsite.verisign.com/OnSiteSUBAGR.htm>

 If all the information above is correct, click Submit to continue.

Accept Cancel

Lessons Learned

- » HP BPIA application in production for over a year
 - Several thousand certificates issued to individuals in over 35 countries
- » CSA application in production for over a year
 - Several hundred authentication events

- » The process works!
- » No need to “dumb down” the process, users “get it”
- » Users *like* the process – they feel in control
- » Native language support is important
 - More so than for a web based application

Benefits of Use of the Telephone

- » Out-of-band trusted network
- » Operates in true real-time
 - Can reduce exposure of temporary PINs to near-zero
- » Uniquely engages a human in the process
- » Requires no additional infrastructure or training
- » Public Switched Telephone Network is highly auditable
- » Phone is socialized as your “handle” for business
 - commercial or personal
- » Can temporally bind digital transaction with authentication event
- » Phone number is a “something you know”, controlling a phone acts as a “something you have”

Selected Authentify Customers



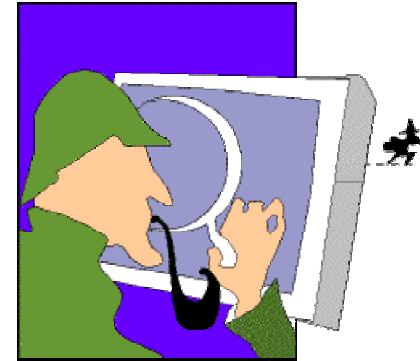
© The New Yorker Collection 1993 Peter Steiner from cartoonbank.com. All rights reserved.



“On the Internet, nobody knows you’re a dog.”

... EXCEPT AUTHENTIFY!

*Thanks to the
2003 ACSAC Team!*



Contact:

Peter Taping
President & CEO
Phone: 773-243-0322
email: peter.taping@authentify.com