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
©2003 Authentify, Inc.
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
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.
Self-selected phone number reflects limited risk profile of application.
Employ Authentify’s patent-pending process to enable telephone as an “out of band” network.

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 [1 minute] before calling me on this number.

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

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

Confirmation Number: 3218#

Note: Do not use your computer until this call is completed!
Telephone allows for direct interaction with a human – capture data, deliver data, capture voice recording or voice biometric.

Confirmation Number confirmed.

Follow the phone instructions carefully.

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

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

Step 1.
Delegated RA uploads file of Subject data to secure web site

Step 2.
Auto-email sent to each Subject with registration instructions

Step 3.
Subject follows hyperlink in email to registration page and enters info

Subject db

Shared Secret “A” issued in the email

Step 4.
System confirms Subject data

Step 5.
Subject takes phone call from Authentify, receives “B” password and leaves audit trail recordings

Subject downloads certificate

Shared Secret “B” issued over phone

Name | Company | Email | Phone | Shared Secret | UserID | Password
--- | --- | --- | --- | --- | --- | ---

©2003 Authentify, Inc.
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 B Business Partner Profile (password needed)

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

- Add an Approver or Find User via Web Enrollment Pages
- Batch Add a list of users by uploading a properly formatted file
- Retrieve a user's "P" enrollment password
- Edit another user's profile
- Renew a user's 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
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.
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.
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.
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
“On the Internet, nobody knows you’re a dog.”

... EXCEPT AUTHENTIFY!

Contact:
Peter Tapling
President & CEO
Phone: 773-243-0322
email: peter.tapling@authentify.com

©2003 Authentify, Inc.