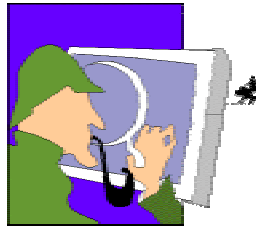




PKI and Certificate Management: A new model for Authentication

Presentation by: Peter Tapling, Authentify, Inc.



2001 Annual Computer Security Applications Conference
New Orleans, Louisiana

©2001 Authentify, Inc.

All Rights Reserved



Abstract

- » Strength of digital certificates rests in strength of issuance process.
- » Issuance process must “touch” the certificate Subject.
- » Audit trail of any issuance process must pass the “reasonable man” test.
- » Large scale deployments (>1,000 certificates) must provide an automated issuance process with delegated administration to be successful.
- » Prudent use of the telephone can enable automated yet auditable real time certificate issuance process.

©2001 Authentify, Inc.

Page 2

Typical Certificate Registration Process

- » Subject informed of eligibility
- » Subject requests certificate
- » Certificate request queued for processing
- » Registration Authority vets individual/request
- » Registration Authority approves request
- » Subject notified of availability of certificate
- » Subject receives certificate

The trick is to bridge the silicon/carbon divide.

Challenges of Certificate Issuance Process

- » Objective is to bind a carbon based persona to a digital certificate
- » Typically a “Certificate Practices Statement” or similar
- » PKI has inherited some legal baggage
- » Authentication for first time issuance is weak link
 - Shared secret only not near strong enough
 - “Personal presence” models prevalent, but operationally weak

Benefits of Use of the Telephone

- » Out-of-band trusted network
- » Operates in true real-time
- » 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 temporarily bind digital transaction with authentication event
- » Phone number is a “something you know”, controlling a phone acts as a “something you have”

Delegated Administration of a PKI

- » Registration Authority typically seen as a central power
- » No one person can “know” every Subject
- » Time is of the essence
- » Delegation broadens trust circle, requires stronger audit trail
- » Delegation spreads risk among sub-communities

- » Challenge of automation without sacrificing trust becomes paramount under a delegated administration scheme

A Sample Issuance Process

- » Two “faces” to an automated registration system
 - Administrative Application
 - Subject (end user) experience

Common Functions of Administrative Application

- » Add Delegated RA or Subject
- » Batch add a list of Subjects
- » Retrieve a shared secret for a Subject
- » Edit a Subject’s profile
- » Renew a Subject’s profile – new certificate
- » Suspend or delete Subject’s profile
- » Batch suspend or delete Subjects

THE INTERNET IDENTITY SPECIALISTS

Sample Admin home page

©2001 Authentify, Inc. Page 9

THE INTERNET IDENTITY SPECIALISTS

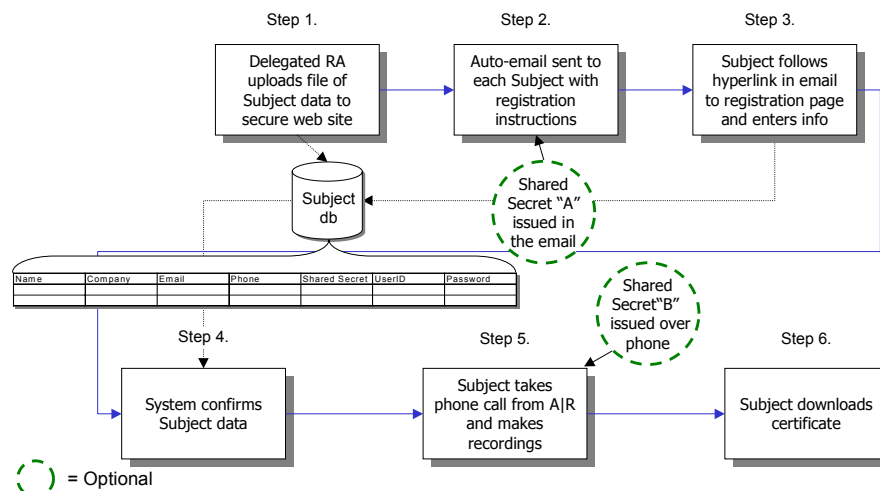
Sample Admin page – this page allows Delegated RA to enter Subjects into the application

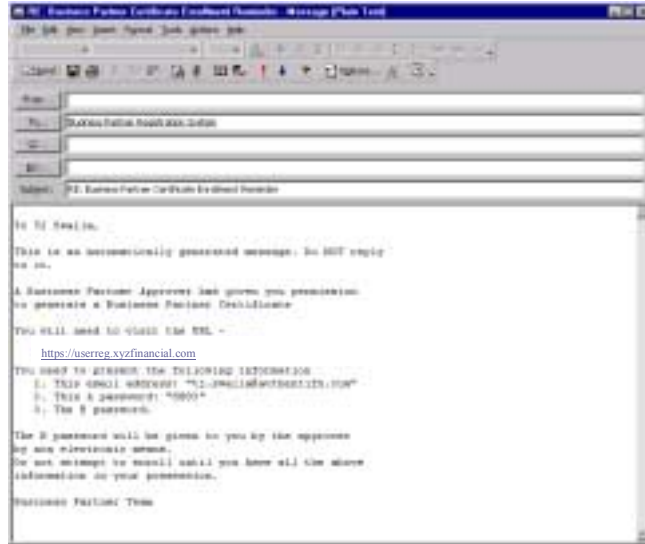
©2001 Authentify, Inc. Page 10

Subject Experience – a Sample PKI Issuance Process

- » **Step 1. Administrator loads candidate Subject data** – A Delegated RA uploads the pertinent Subject data (e.g., distinguished name, email address, phone number) into the central database.
- » **Step 2. Email notification to Subjects** – Subjects are automatically sent registration instructions with link to first registration page via email.
- » **Step 3. Subject enters Shared Secret** – Subject follows the link in the email to a registration web site and enters the pertinent data into the registration form.
- » **Step 4. Subject confirms their data** – Database checks shared secret and returns the Subject's trusted phone number(s) for selection – Subject clicks "Call Me Now".
- » **Step 5. Subject completes Authentify|Register process** – The Subject follows the Authentify|Register process with appropriate options.
- » **Step 6. Subject completes certificate issuance process** – Subject is walked through typical certificate request process – receives certificate in real-time.

Telephone as Foundation a PKI Registration Process





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.

THE INTERNET IDENTITY SPECIALISTS

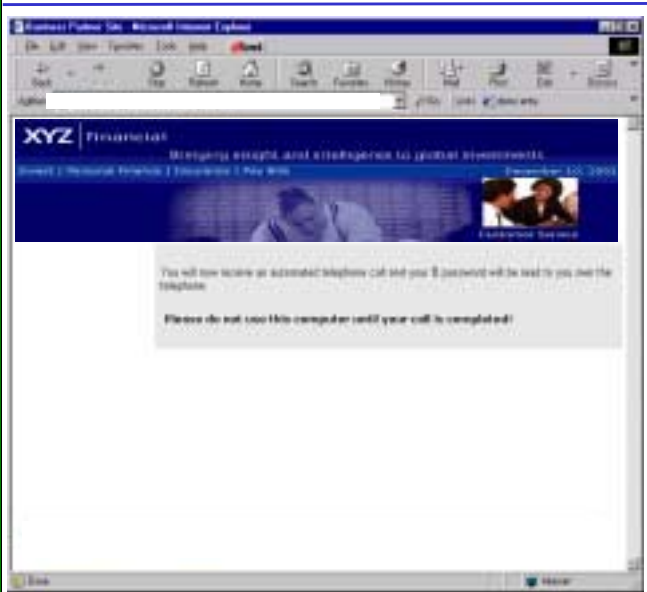


AUTHENTIFY™

In the Authentify-enhanced process, the Subject is asked to accept a phone call at a number trusted by the Delegated RA.

©2001 Authentify, Inc. Page 15

THE INTERNET IDENTITY SPECIALISTS



AUTHENTIFY™

A call is placed and the “B” password is read to the Subject over the phone.

Telephone prompts:
 “Hello this is Authentify calling on behalf of XYZ Financial, if you are expecting this call press pound.”
 “Your B password is X123.”

©2001 Authentify, Inc. Page 16



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.”

Trusted Certificate Issuance in True Real-time

- » Authentify|Register can assure intended party is present at the time the key pair is being created – not before or after the fact
- » The automated process it is enacted the same way every time – no risk of social engineering or human error
- » A human-understandable record of the entire event is captured

Options Provided by Phone

- » Speech Processing
 - Audible delivery of information
 - Speech recognition
 - Speaker verification
- » Supplemental data collection
- » Supplemental information delivered

Successful uses of Authentify process:

- » SingleSignOn.Net
 - Robust, easy to use/administer authentication appliance
- » Baltimore CDS
 - Fully automated, outsourced PKI solution
- » Digital Signature Trust
 - Interactive TrustID for digital signature applications
- » Entrust
 - Partner Café digital certificate registration/issuance
- » VeroTrust
 - Fraud management tool
- » AssureBuy
 - Transaction clearing, automated callback for transaction audit trail



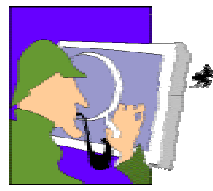
See us in the
Exhibition Hall

© 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
2001 ACSAC Team!*



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