Enhancing PKI
With Voice and Telephony

Presentation by: Andrew Rolfe, Authentify, Inc.
What has Authentify built ...

- Customizable system to bind data and voice sessions together using independent networks

What does this attempt to solve ...

- Binding a human to a digital credential or process in an automated way
Use of Voice Biometrics

Biometrics is seen as a promising way to create a definitive, portable representation of someone’s identity. Many biometric solutions available today require some combination of specialized hardware, client-installed software, or significant user training in order for them to be successful. While applications for a controlled audience (such as employees) may find this acceptable, externally facing applications must overcome these problems. Authentify provides an approach to enabling networked applications with integrated voice biometrics.
Features of a system combining Web/Telephony/Biometric Technologies...

- Real-time, interactive, 2-way, out-of-band communication channel
- Simple Interfaces
- Familiar Paradigm
- Ease of Integration
- Undeniable Contact
- Multi-factor authentication in one session
Challenges of Any Registration Process

- Objective is to bind a carbon based persona to an electronic security 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 is not near strong enough
  - “Personal presence” models prevalent but expensive and inefficient
- Delegation is often required to support broad communities
- Automation is desired to keep costs down
Additional Challenges Attributable to Biometrics

- “Answer” is no longer discreet
  - Biometrics are by their nature statistically based
  - Equal Error Rate becomes something to manage
- Biometric approach needs to be socialized
- New risks to consider
- Required software/hardware footprint, user training
- Capture device integrity
- Still have “first time” problem
The *weakest link* in the chain is usually the enrollment process...

- **Cheap – no audit trail...**
- **Cheap, fast - insecure**
- **Fast, secure - expensive**
- **Improbable – if not impossible...**

©2003 Authentify, Inc.
There is a better way that is still tried and true...

Using the Internet and telephone network simultaneously...
Secure records remain secure, only enough information to place the authentication phone call and/or match telephone owner is passed to Authentify.

Authentify places telephone call over the PSTN, sync'ed to the user’s Web Session. A synchronized exchange requires the user to respond to the phone with real time info displayed on the Web page.
**Authentify Integration During Enrollment**

**End User:**
- Request enrollment form
- Submit request
- Enter enrollment information
- Request telephone enrollment
- Create record and store transaction data
- Place phone call and request confirmation number
- Enter confirmation number
- Collect confirmation number, shared secret, and voice recording
- Validate and store transaction data
- Display confirmation number
- Complete interaction
- Send email
- Retrieve certificate
- Issue certificate
- Install certificate
- Congratulations page
- Click URL link
- Submit request
- Retrieve certificate
- Issue certificate
- Store certificate
- Sign request

**Web Site:**
- Submit request
- Evaluate request
- Apply policy
- Request telephone enrollment
- Get trusted phone number(s)
- Display confirmation number
- Complete interaction
- Send email
- Retrieve certificate
- Issue certificate
- Store certificate
- Sign request

**Automated RA:**
- Validate trusted data
- Request telephone enrollment
- Get trusted phone number(s)
- Display confirmation number
- Complete interaction
- Send email
- Retrieve certificate
- Issue certificate
- Store certificate
- Sign request

**Trusted User Database:**
- Store results + VID
- Issue certificate
- Store certificate
- Sign request

**CA:**
- Store certificate
- Sign request

**Certificate Database:**
- Store certificate
- Sign request

**VP Database:**
- Store voice print + VID
- Store results + VID
- Complete interaction
- Send email
- Retrieve certificate
- Issue certificate
- Store certificate
- Sign request

**Authentify:**
- Validate trusted data
- Get trusted phone number(s)
- Display confirmation number
- Complete interaction
- Send email
- Retrieve certificate
- Issue certificate
- Store certificate
- Sign request

**Authentify Integration During Enrollment**

©2003 Authentify, Inc.
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
- Highly auditable
- Phone is socialized as your “handle” for business
  - commercial or personal
- Can temporally bind digital transaction with authentication event
- Phone number or shared secret is a “something you know”, controlling trusted phone acts as a “something you have”, verification of a voice biometric is “something you are”
Benefits of Telephone as Biometric Security Tool

- Eliminates cost of special devices - only need access to a phone
- No user training
- No device compatibility problems
- Can be handled at a central site
- Strong audit trail
Detection error trade-off: Best of 3 attempts

©2003 Authentify, Inc.
Use of Voice Biometric To Enhance Digital Certificates

- Store voice-print ID as signed attribute of Certificate
- Now the Certificate is truly linked to a person
- Provides ability to verify user of Certificate in real-time
- Enables longer Certificate lifespan
- Can be handled by a networked or third-party service:
  - More secure due to separation of biometric and identity info
  - Can handle biometric aging
  - Can manage multiple voice prints
  - Isolate the impact of technology enhancements
  - Archived audit trail
- Provides a multi-faceted solution – both speed and security
Application Examples

- PKI Certificate Registration & Enhanced Audit Trail
  - HP, Atrion, Identrus, Bank of America ...
- Self-service SSL Certificate Pickup
  - VeriSign
    - Multiple calls
      - originator direct
      - originator navigated via D&B central number
  - GeoTrust (international)
- Account Activation / Maintenance
  - SSA (email + telephone authorization)
  - PayPal (location verification)
  - Associated Bank (branch & on-line biometric capture)
  - Bank of America (on-line cash management)
  - Payment One (account authorization)
- E-Signing
  - NYC Dept of Health, Inviva
Ease of Use & Intrusiveness

Rate the ease of the overall registration process, using Authentify.

Rate the intrusiveness of the Authentify process:

“I very much like the idea of voice identification. This process surpasses any other method of protecting my identity and SSN that I have seen. BRAVO!!

JoAnn W., Financial Advisory Firm
Conclusion

- The telephone can be employed as an effective security tool to enable out-of-band processes to occur in real time.

- If the requirement is self-service + out-of-band + auditable + scalable, then telephony presents the only viable solution.

- Coupled with Biometrics & Digital Certificates can provide a multi-faceted solution.

- Questions? Discussion...
“On the Internet, nobody knows you’re a dog.”

… except Authentify