Caveat

- Intent is to present an approach for risk-based multifactor authentication and how it might be used in a trust-elevation environment.
- To this end, I will be using Daon’s IdentityX product as an example only to demonstrate these ideas.
Agenda

- The technology
- The methods
- Use cases
- Example
Identity is …

- A unique risk-based, multi-factor authentication capability that leverages latest generation smart phones (e.g., iPhone, Blackberry, Android), smart tablets (e.g., iPhone/Playbook) and traditional mobile devices

- Identity technology combines multiple authentication techniques for greatest identity confidence:
  - Device (What you have)
  - PKI Certificate (What you have)
  - PIN/PW (What you know)
  - OOB OTP (What you have)
  - Face (Who you are)
  - Voice (Who you are)
  - Palm (Who you are)
  - GPS (Where you are - context)
  - (other as devices enabled)

- Placing multiple levels of identity assurance in the hands of consumers

- Designed to run both as an in-app framework and out-of-band authentication product
Multifactor fusion for greatest identity accuracy/fidelity

- GPS
- PIN/Passphrase
- Face
- Palm
- Voice
How is ‘risk aware’ identity assurance achieved?
<table>
<thead>
<tr>
<th>Relying Party</th>
<th>SMS Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>IdentityX Service Provider Gateway (IXSPG)</td>
<td>IdentityX SMS Broker</td>
</tr>
<tr>
<td>IdentityX Administration Gateway (IXAG)</td>
<td>(IXSB)</td>
</tr>
<tr>
<td>IdentityX Configuration Manager (IXCM) Web Portal</td>
<td>IdentityX Key Manager</td>
</tr>
<tr>
<td></td>
<td>(IXKM)</td>
</tr>
</tbody>
</table>

### IdentityX Components

- **IdentityX SRP**
- **IdentityX Device Gateway (IXDG)**
- **IdentityX Key Manager (IXKM)**
- **IdentityX SMS Broker (IXSB)**

### Device Frameworks

- **iPhone Component Device Framework**
- **Android Component Device Framework**
- **Blackberry Component Device Framework**
- **Symbian Component Device Framework**
- **Windows Component Device Framework**
Authentication Policies

RP Transaction ID

Abc1

Xyz2

. . .

Policy Selections

Method: PIN, Duress PIN
       Face, Face Liveness
       Voice, Voice Liveness
       Palm

Context: Location limits
       Time limits

Number of retry attempts

. . .
Simple flow

RP Application

Authentication Server

Request Authentication

Authentication Results

Request Transaction

Authentication Challenge(s)

Authentication Response
Alternatives:

- Request specific set of methods or request based on an assurance level (assumes equivalence established)
- Report results as pass/fail or assurance level achieved
- Allow users choice as to preferences, additional methods/levels of assurance beyond minimum
- When trust is elevated, require only delta to current level or full set of challenges for new level
Bridging the gap between Security and Convenience

Trust, Security, Customer Service

Traditional Convenience/Security Trade-off Curve

Security vs. Convenience

- Username/Password
- Static Card
- PKI / Card
- RSA Token

Goal
Why include biometrics?

- Biometrics is the most preferred additional form of authentication for US online banking users
User logs into the bank website using simple username/password.

User initiates low value transaction and is challenged to authenticate on their mobile device. Proof of possession (cert based mutual authentication and user action to approve) is sufficient for this risk level.

Subsequently, the user chooses to perform a higher value or more fraud-prone transaction. They are then asked to again authenticate using their mobile device; however, this time in addition to the cert check, they are asked to enter a PIN and speak a passphrase, after which they are provided a one-time password which they enter on their screen.
Use Case – Leveraging Geoposition

- Authentication policy which is location sensitive
- Financial transaction: funds transfer
- Authentication request –
  - if in US, use policy A (methods a + b)
  - if outside US, use policy B (a + b + c)
- Example –
  - a = PIN
  - b = face
  - c = OOB OTP
- [Note – cert check done on every transaction]
For each transaction type, the bank has set a minimum set of authentication methods.

Users desiring additional protection are given the ability to add methods.

Example – Transfer of $5000

• Default setting: Cert + PIN + OOB OTP
• User adds: voice
Transaction Steps
Initiate Transaction
Authentication Instruction
Select App

- App is pre-loaded as part of phone registration process
  - Or can be downloaded directly from app store

- App may be standalone (as shown) or integrated into a service provider’s app
Transactions may be generated from multiple service providers and multiple transactions can be queued for approval.

Familiar Service provider icons can be used to help to differentiate transactions.

Additional transaction information such as transaction type, transaction value, transaction items or title helps the user easily identify acceptable and non-fraudulent transactions.
Make Decision

- Transactions in the system require a user action in order to be completed.
- On a per transaction basis, the user has the option to approve, decline, or mark a transaction as fraud.
A number of actions can be set by the service provider and/or the consumer – including face, voice, palm, PIN etc.

IdentityX™ supports a wide variety of verification methods.

Verification methods are matched to transaction risk as defined by the business rules of the Service Provider.

Some transactions may require the use of a PIN.
Facial verification provides an additional method of verification appropriate for certain transactions.

The user simply takes a picture of their face which is matched against a reference image.

Facial “Liveness” detection ensures the user is present and not an imposter (e.g., taking a photo of a photo).
Palm verification provides an additional method of verification appropriate for certain transactions.

The user simply takes a picture of their palm which is matched against a reference image.

Palm is a very innovative (unique) authentication solution that is extremely convenient for users and highly resistant to fraud.
Authentication Option D - Voice

- Depending on risk level defined by Service Provider, user may be asked to speak a phrase to conduct voice verification.

- As with other types of verification, the user’s unique voice can be matched to a previously captured reference sample.

- Voice liveness detection can be implemented to eliminate “playback attacks” (e.g., playing a pre-recorded voice sample).
More than one verification method may be used. Once all methods have been submitted, they are evaluated and “fused” using proven mathematical algorithms.

The Service Provider defines the transaction risk which maps to a minimum assurance score to accept the transaction.

If the transaction is accepted, the Service Provider may utilize a One Time Password, show a virtual card, or simply complete the transaction and move the user to the next step in their digital interaction.
Completion

Transfer Funds Successful...

Your transfer was successful.
More Information

Catherine J. Tilton, CBP
VP, Standards & Technology, Daon
11955 Freedom Drive, Suite 16000
Reston, VA 20190
703-984-4080
cathy.tilton@daon.com