Biometrics and High-Trust Digital Identities
Creating opportunities for improved access, improved service and program ROI

Simplify ● Protect ● Secure
A little background
Strong Digital Identity Leadership

- Board positions on IDESG, UT Center for Digital Identity and the AAMVA eID Working Group
- Shaping NIST identity assurance guidance
- Working to establish ISO standards
- Building solutions that embrace the Identity Ecosystem Framework and FIDO guidance
- Executing 2 federal NSTIC Grants to leverage Digital Identity for state government
Challenges Facing Government

*biometrics can make a difference*

- People and agencies want improved channels of access including mobile and online.
- Moving access to services online requires trust that people are who they claim to be. To date that trust is not attainable at reasonable cost.
- High risk/value transactions are at risk and need to be secured to protect people and government budgets (i.e. Tax Refund Theft).
- Traditional approaches are no longer getting the job done:
  - Username/Passwords
  - Knowledge questions
  - Offline verification
Adding new ROI to DHHS Operations

Remote Self Service

Front Office

Back Office

Low Complexity – low or no-touch transactions

Mid-High Complexity – high-touch transactions

Triage

Low Complexity – low or no-touch transactions

Mid-High Complexity – high-touch transactions

Approve – Deny – Pend – Recertify

Instances of Identity Verification
The Challenge

Journey

- BUSINESS IN CYBERSPACE
- SOCIAL MEDIA
- eGOVERNMENT
- IN-PERSON BUSINESS
- IN-PERSON GOVERNMENT
The Challenge
Journey’s Challenge

We quickly lose our traditional human means of evaluating and verifying identity
The Challenge
Journey’s Challenge

In place of traditional means… we substitute
The Challenge
Journey’s Challenge

Why substitute? Can’t we transform what we already trust?
The Challenge

How can we transform our most trusted means of proving identity?

- Create **Electronic Identity (eID)** directly from our Driver Licenses for online use
- **Enhance trust** through standardized communications linking parties
- **Replace** physical visual verification with biometrics and multi-factor authentication
- **Build for the individual** we are trying to enable and protect
- **Provide for levels of assurance** (anonymous through definitive)

Simplify. Protect. Secure.
A growing concern...
**Balancing Authentication & Proofing**

![Graph showing the balance between single-factor, second-factor, and multi-factor authentication methods.](image)

**PROVEN IDENTITY**
- Top Secret
- In-Person Proofing (DMV, IdentoGO)
- Multi-Factor (Remote Proof) eID
- Sponsored
  - Employee, Academic
- Validated
  - Comparator, NetVerify, Data checks, Authify
- Corroborated
  - KBA, LinkedIn
- Friend Attested
  - Facebook, Google+
- Self-Attested
  - Yahoo, Hotmail

**AUTHENTICATION STRENGTH**
- Single Factor
  - ID: Weak Password
- Second Factor
  - ID: Strong Password
  - Token/phone
  - Biometric
- Multi-Factor
  - Crypto
  - MultiFactor Authentication
A growing concern...

**Balancing Authentication & Proofing**

**PROVEN IDENTITY**

- Top Secret
- In-Person Proofing (DMV, IdentoGO)
- Multi-Factor (Remote Proof)
- Sponsored ID
- Validated (Comparator, NetVerify, Data checks, Authenticity)
- Corroborated (KBA, LinkedIn)
- Friend Attested (Facebook, Google+)
- Self-Attested (Yahoo, Hotmail)

**AUTHENTICATION STRENGTH**

- **Single Factor**
  - ID: Weak Password

- **Second Factor**
  - ID: Strong Password
  - Token/phone
  - Biometric

- **Multi-Factor**
  - Crypto
  - MultiFactor Authentication

© 2016 MorphoTrust USA, LLC. All rights reserved. No reproduction or republication without written permission.
A growing concern...

Balancing Authentication & Proofing

PROVEN IDENTITY

Top Secret
In-Person Proofing
Multi-Factor (Remote Proof)
Validated
Corroborated
Friend Attested
Self-Attested

DMV, IdentoGO
etID
Comparator, NetVerify,
Data checks, Authenticity
KBA, Linkedin
Facebook, Google+
Yahoo, Hotmail

Sponsored
Employee, Academic

Single Factor
Second Factor
Multi-Factor

ID: Weak Password
ID: Strong Password
Token/phone
Biometric
Crypto
Multi-Factor Authentication

AUTHENTICATION STRENGTH
Biometrics value is unleashed when they are present a proofing time

High trust digital identities are rooted in strong in-person identity proofing
Real world example: *DMV in-person ID proofing enable online eID trust*

**Physical World**
- **Driver License Applicants**
- **State DMV Examiner**
- **Physical DL/IDs issued**

**In-Person ID Proofing**
- **Secure Credential Issuance**
- **In-Person Uses**
  - "offline credential"

**Online eID**
- **eID Registration**
  - 1. DL authenticated
  - 2. 2D code decoded
  - 3. Self-Photo (biometric match)

**eID Issuance & Ready for Online Use**
- **Biometric & Demographic Authentication at DMV**
- **eID issued & ready for online use**
  - High LOA eID Issued
  - QR Code login
  - out of band biometric auth

**"Cert-based & Interoperable"**

MorphoTrust eID Applicant (person with their driver license)
Our example of biometrics in action

MorphoTrust® eID is an online ID, issued by MorphoTrust and authenticated by state MVAs to simplify and protect online transactions. The eID delivers a trusted digital credential that consumers can use to facilitate trusted transactions.
Our example of biometrics in action

The eID is the 1\textsuperscript{st} and only service allowing consumers to create a personal online credential by authenticating themselves against their MVA record.

**It’s Personal:**
- A highly trustworthy online identity credential
- Resides on an individual’s smartphone
- Puts full control of PII in the hands of the individual

**It’s The Future:**
- Accepted in lieu of traditional Usernames/Passwords
- Enables the future of identity in which users choose which credentials they want to use
- Minimizes the number of times an individual’s PII is copied and stored across the internet… reducing breach risk

Simplify. Protect. Secure.
Leveraging Strong Identity Proofing

1. Bind Phone
   - SMS Verify

2. Scan Front of License/ID
   - Doc Auth (Cloud)

3. Scan Back of License/ID
   - (SOR) Authentication

4. Take a Selfie

“Something I have”

“Something I am”

Phone
Doc Auth
Data
Biometric

Simplify. Protect. Secure.
Biometric Unlock ensures the person holding the phone is the same that registered for the eID.

1. Open with selfie
2. Go to relying party login screen on computer
3. Click on eID button
4. Scan QR code to gain access on mobile phone
Real-time or Transaction-time value

Multiple Means of Delivering Value:

1. **Active Web Navigation**
   - Securely login to a state portal (i.e. DHHS, DOR, DOT...)
   - Complete online forms without extra steps identity verification steps
   - Step-up trust level for highly sensitive actions (i.e. biometric)

2. **Securing specific transactions that may happen at any time**
   - Restrict a transaction from happening without consent
   - Authorize an action or transaction
   - No timing restrictions
eID Use Cases

- Make secure online purchases
- Apply for a benefits
- Approve your state tax refund filing
- Make High Trust Banking Transactions

Simplify. Protect. Secure.
eID Tax Use Case - Program Spotlight

GA & AL DOR in partnership with GA DDS & ALEA (their driver license issuing agencies)

Problem: Fraudsters are stealing tax refunds (>20B per year)

- Up to this point, there’s been no true way for the taxpayer to prove their identity online and/or lock down their tax account
- Fraudsters file fake tax returns in advance of the actual taxpayer
- Federal & state governments pay within 30 days but take months to match financial data
- Governments lose money to fraudsters and still have to pay taxpayers after the identity theft is remedied
- Agency’s fraud detection tools are outdated or insufficient

Our Solution: Authenticate taxpayers against their trusted MVA Record

- Taxpayers download the eID app, scan their DL/ID and take a selfie to register for their MorphoTrust® eID
- MorphoTrust uses the DL/ID and selfie to authenticate against the MVA (in this case GA DDS or ALEA)
- Upon registration, taxpayers visit their DOR’s website to opt-in and lock their account with their eID
- Once a tax refund is filed, the DOR sends a notification to the taxpayers eID app on their phone, asking them to approve or deny the claim filed.

The Contract: In the case of Alabama - ALEA pays $250K per year per agency

- FREE to taxpayers
- AL agencies sign-up for $250K/year or go statewide for $1.25M/year (15% share)
- MorphoTrust can use AL user base for other commercial transactions
- Piloted by AL DOR employees | Release scheduled for Q1 (active through this tax season)

Simplify. Protect. Secure.
**eID Tax High Level Workflow**

**Download App**
- Register for eID
- Enroll into Tax Protection Program

**Opening App**
- Using the eID
  - Click on Icon
  - Take a Selfie

**For Tax Authorization Request**
- Accept (or Deny)

**Additional Steps:**
- Download
- Scan Front & Back of License
- Take a Selfie
- Scan the QR code/Enroll

---

*Simplify. Protect. Secure.*

MorphoTrust USA, Inc. Company Confidential
Companies are betting on a new way to protect your identity: the selfie.

The selfie is about to get serious.

Already ubiquitous at parties and for capturing Instagram-worthy landscapes, the act of raising a phone to your face and finding the perfect photo angle could take on a whole new role in people’s finances. Some banks, tax agencies and tech companies are making the selfie an integral step for people checking their bank accounts, shopping online and filing tax returns. Read More

Tax refunds have turned into a gold mine for cybercriminals, who each tax season unleash a slew of scams and phishing expeditions aimed at claiming billions in phony refunds.

In 2013 alone, the Internal Revenue Service estimated that it paid out $5.8 billion in fraudulent refunds, even as it prevented $24.2 billion in payments from going to criminals.

Could a selfie be the answer to curbing this multibillion-dollar fraud problem? Read More

Identity theft tax refund fraud is an expensive problem in America. Last year, the Internal Revenue Service (IRS) received more than 1 million fraudulent tax returns and managed to stop nearly $7 billion in fraudulent tax refunds - and that's just the feds.

The IRS and state tax authorities have been looking at ways to combat tax fraud while still ensuring that honest taxpayers have their tax returns processed (and refunds issued) in a timely manner. With that in mind, the Alabama Department of Revenue is hoping that new technology will help them stay ahead of scammers and thieves. All it takes is a cell phone. Read More

Selfies, long derided as a symbol of narcissism and oversharing, have found a more serious purpose.

Companies and government agencies—ranging from the ride-hailing service Uber Technologies Inc. and credit-card giant MasterCard Inc. to the Alabama Department of Revenue—are asking people to snap self-portraits on their smartphones as proof of identity. Read More
Adding new ROI to DHHS Operations

Remote Self Service

In-Person Service

Instances of Identity Verification

Front Office

Back Office

Low Complexity – low or no-touch transactions

Mid-High Complexity – high-touch transactions

Approve – Deny – Pend – Recertify