



Proactive vs. Reactive; Why Architecture Matters



Did You Know....

That all our Identity Data has been stolen?

That all that ID data is for sale online?

Crooks buy our Identity data to forge fake Identity documents?

Crooks Use AI to make perfect images of ID documents?

What Would Make The Identity Data Trustworthy?

Known & Trusted Source

Fixed ID Data and Biometric Data Relationships (**BINDING!!**)

The Data is Immutable

This is this how we ID “Proof” Today...Upload a Driver License to the IDV Platform



A **Credential**....Binds a Human Being to an Identity and Associated Privileges



Transportation Security Administration - TSA ✓

about a month ago



TSA Intercepts Fraudulent Passport Cards at EWR

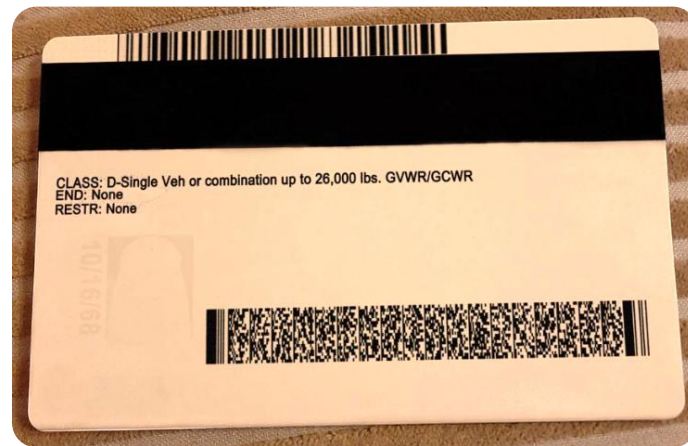
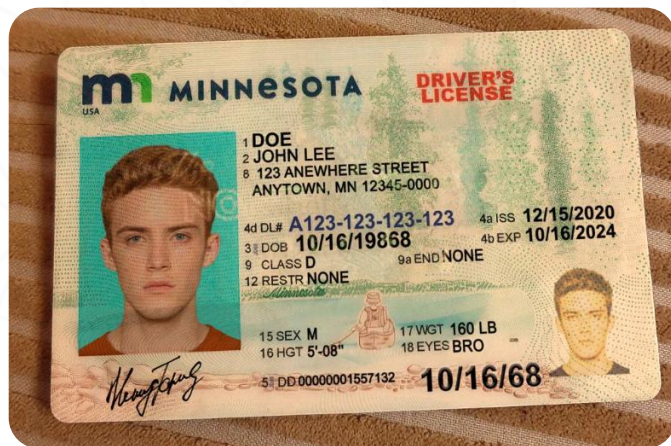
Incredible job by TSA officers at Newark Liberty International Airport (EWR) who spotted 34 fraudulent passport cards inside a passenger's carry-on bag last week. Each passport card (some are pictured below) contained one of the same two photos, but each passport card had different information such as name, address, date of birth. Talk about an identity crisis!

From John, to Jacob, to Jinglheimer and Schmidt, it looked like... [See more](#)



👍 326 💬 37 ➦ 66

Many ID GenAI Attack Vectors Are Undetectable



This is an uploaded AI Generated ID.

The Bad Guys Want our Valid Privileges

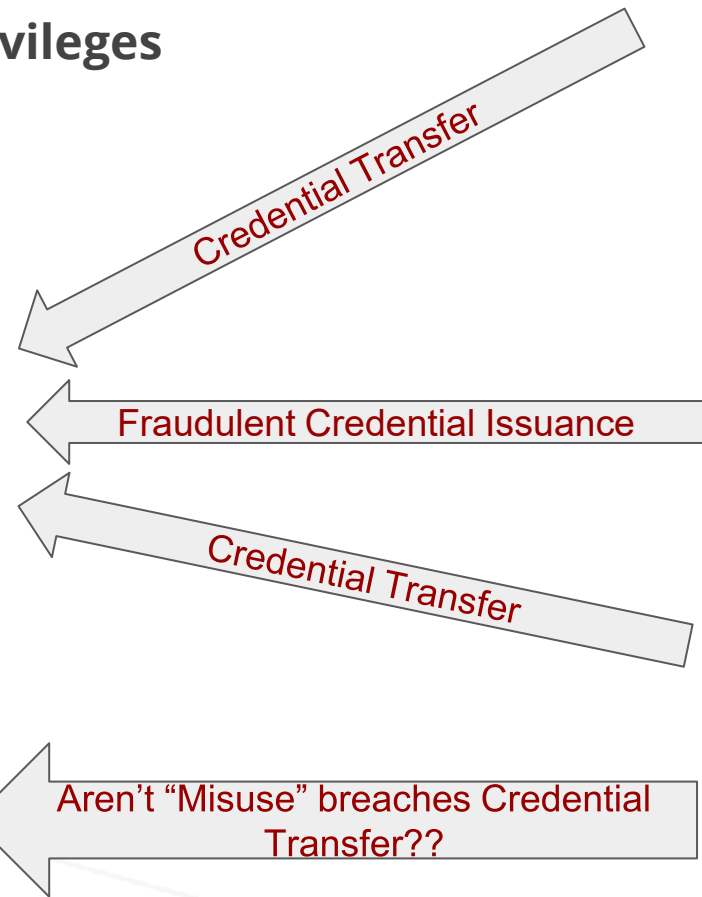
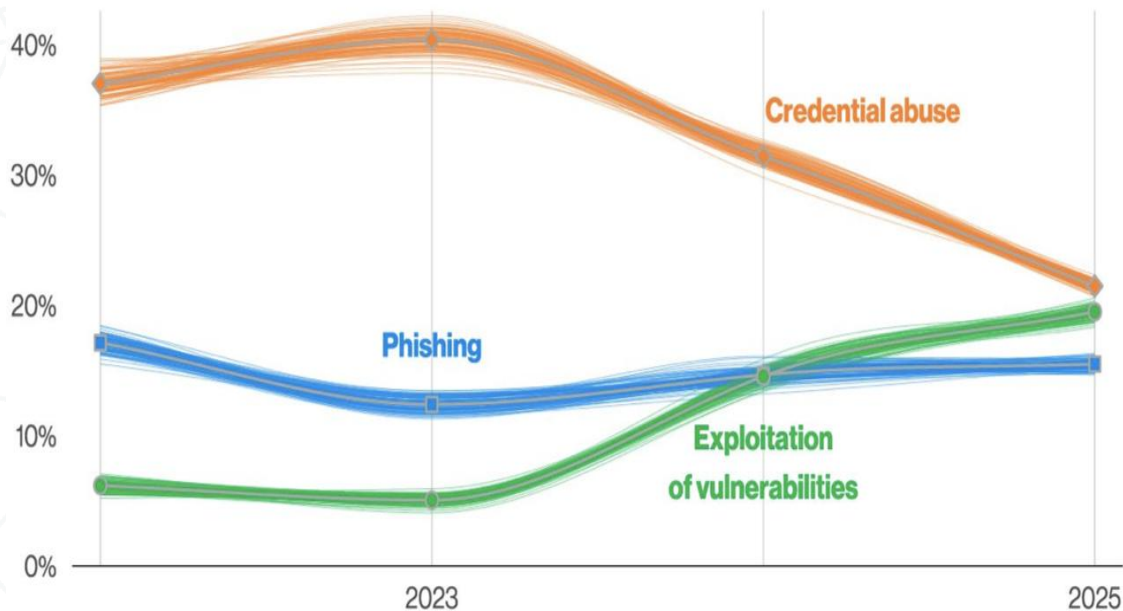
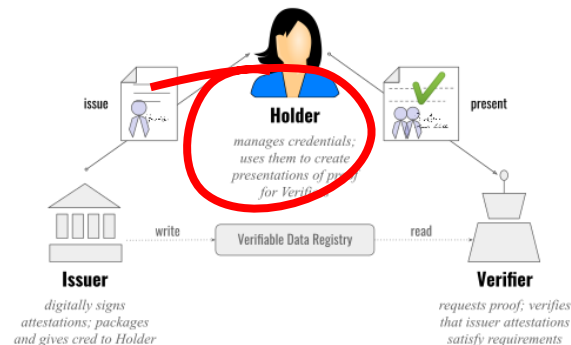


Figure 16. Known initial access vectors over time in non-Error, non-Misuse breaches (n in 2025 dataset=9,891)

How About Binding to the Identity Record AND Credential “Owner”?



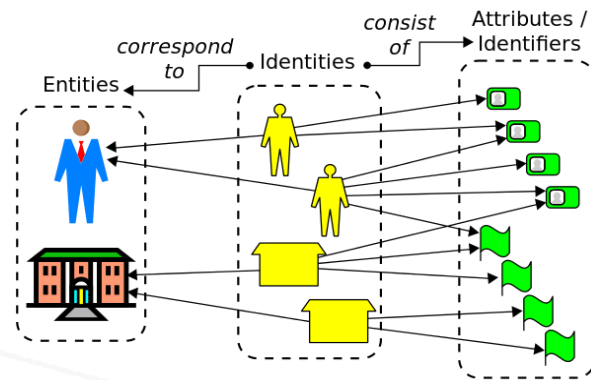
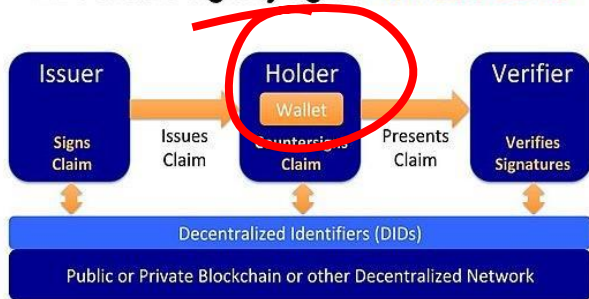
1. How does the ISSUER “know” who the HOLDER is, when they provision the “verifiable credential”? (Is this really the person who was issued the credential?)



2. How does the VERIFIER (or anybody) “know” who the HOLDER is when they present the “verifiable credential”? (Who is holding the phone or ID or Passport?)

3. How does the HOLDER get a reissued credential after losing the device that holds the wallet? (See 1 & 2)

DIDs enable digitally signed verifiable claims



(Deterministic)(Probabilistic) = Probabilistic

- Device & Data Authentication (Cryptography: PKI & Tokens) is Deterministic
 - Binary: one or zero, yes or no
- Remote User Identity Verification is always Probabilistic
 - Statistical probabilities, percentages

If you can't Guarantee who controls a device (and bound credentials), Device-based User Verification or Authentication is Probabilistic

$$\underline{(100\%)(99.9\%) = 99.9\%}$$

(Deterministic)(Probabilistic) = Probabilistic

What Would Make The Identity Data Trustworthy?

Known & Trusted Source

Fixed ID Data and Biometric Data Relationships (**BINDING!!**)

The Data is Immutable

Basically...We Have Two Problems to Solve...

1) We Cannot Trust the Physical Identity Data in Circulation

2) We Cannot Trust We Know Who Holds the Devices the Credentials are Bound to

Basically...We Have Two Solutions...

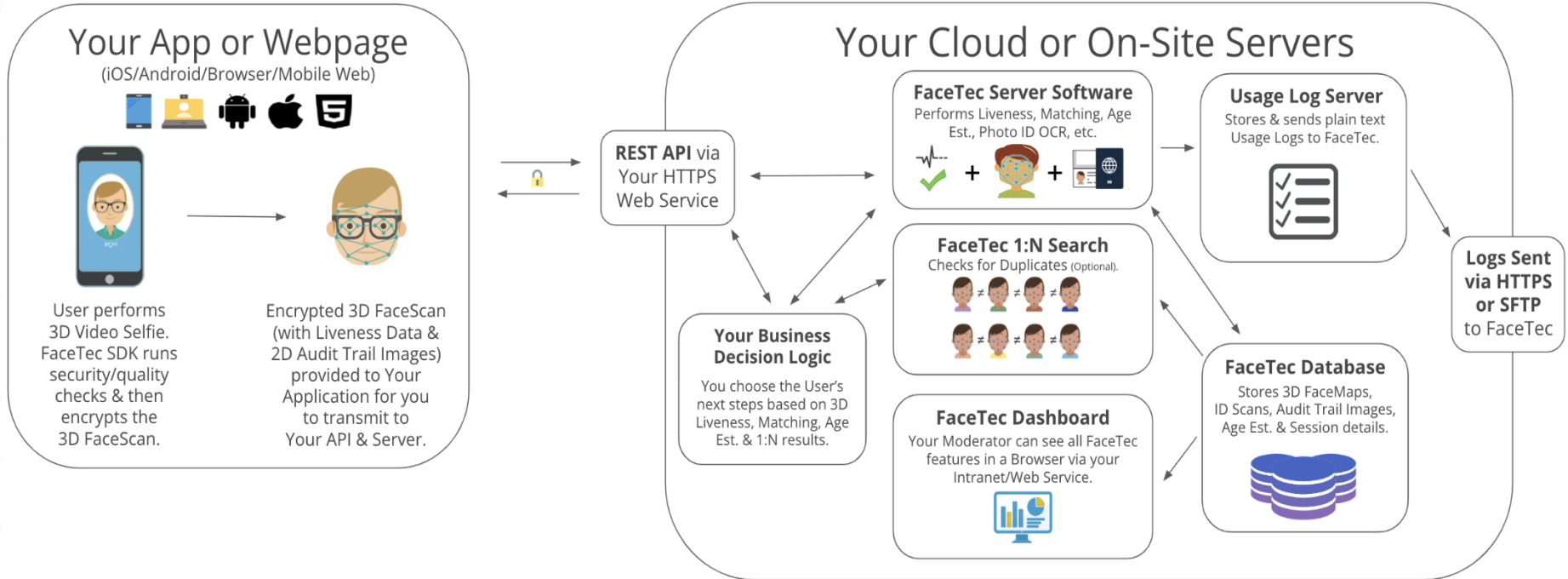
- 1) Move Biometric and ID Data from the Identity Owner to the Issuing Authority for comparison, or**
- 2) Move Biometric and ID Data from the Issuing Authority to the Identity Owner for comparison**

Move Biometric and ID Data from the Identity Owner to the Issuing Authority for comparison....

- 1) Liveness-proven Biometric Collection at the Edge**
 - A. Enrollment**
 - B. Access Control Verification or Authentication**

- 2) One-to-Many (1:N) Comparisons in the Database**
 - A. Duplicate Legitimate Entries**
 - B. Fraudulent Duplicative Entries**

Querying Verified Record Behind the Issuing Authority's Firewall



Move Biometric and ID Data from the Issuing Authority to the Identity Owner for comparison

- 1) Liveness-proven Biometric Collection at the Edge**
 - A. Enrollment**
 - B. Access Control Verification or Authentication**

- 2) Identity “Owner” Control of their Verified Identity**
 - A. Privacy**
 - B. Decentralized Data**
 - C. Portability**

Digitally Signed Biometric QR Barcode



Face Data
from
Issuing
Authority
ID Profile

+



Identity
Data from
Issuing
Authority
ID Profile

+



Digitally
Signed by
the Issuing
Authority

=



Add to ANY
Physical or
Digital
Credential,
Document, or
stand alone

72 Bytes of Face Data = zAAAD5fIALMkzIAABVlgAAC4SoAyqk0u4AG5AAAEj5ogAXKYHEFAF4AAVsgA/CFABIQoArOU



UR Codes to Validate Data & Binding Verify & Re-verify User Identity Remotely



**UR Code Scanned
by Codeholder**
w/ Smart Device or
Webcam



**Relying Party
Receives Data**
of Codeholder w/
Digital Signature



**Data Validated w/
Digital Sig & Public Key**
of UR Issuing Authority



**Codeholder Takes
Liveness-proven Selfie**
for Relying Party



**Face Data Match +
Digital Sig Validated =
PII Real & IDV Complete**



UR Codes Validate Physical & Digital Documents and Prove Binding



For optimal real-world scanning UR Codes should be printed at least:

3/4" x 3/4" or 2cm x 2cm @ 300 DPI





Scan + Match

FaceTec, Inc.

10+ Downloads | Everyone

Install | Share | Add to wishlist

You don't have any devices



App support

About this app

Free Scanner for UR Codes (Special biometric barcodes) that can contain data from Driver Licenses, Passports, Credit Cards, and many other documents. This App allows you to Match the encoded face data in the UR Code to another face and provides a Face Match Level and validates the Digital Signature that proves the immutability of the personal info stored in the barcode.

For more information on UR Codes, their capabilities and for the ability to encode them visit: <http://URCodes.com>.

Updated on

Jan 3, 2025

Tools

Data safety

Safety starts with understanding how developers collect and share your data. Data privacy and security practices may vary based on your use, region, and age. The developer provided this information and may update it over time.

No data shared with third parties
[Learn more](#) about how developers declare sharing

No data collected





Jay Meier

Chief Identity Technology Strategist, FaceTec, Inc.

Subject matter expert in biometrics & IAM, author, tech executive, and award-winning Securities Analyst.

FaceTec, Inc., the leading, global provider of 3D Liveness and 3D Face Matching software for remote identity platforms.

+1-612-978-3687 - Jay@FaceTec.com



facetec

FaceTec.com

Liveness.com

Biometric liveness detection explained

URCodes.com

