facetec

# Legal Identity Issuers: The New Digital Verifiers

# What Are We Going To Learn?

- Why Humans don’t always look the same in their 2D photos
- Why 2D Face Matching Accuracy has stalled out
- Why “3D Liveness Detection” is the key to remote ID Verification
- How to upgrade a 2D Photo Database to 3D FaceMaps over time
- Why Device Camera Feed must be secured for data to be trusted
- How to use FaceTec with existing Hardware / Infrastructure
- Why FaceTec powers US DHS, Canadian Parliament & 100s more

# What is True Digital Identity?

Digital Identity IS unique human biology recreated in 1s & 0s.

- It is not public details about a person
- It is not private details about a person
- It is not DOB or mother's maiden name
- It is not a social security number
- It is not your Fiat Identity

Your "Legal Identity" is your Government's official name & ID # for you.

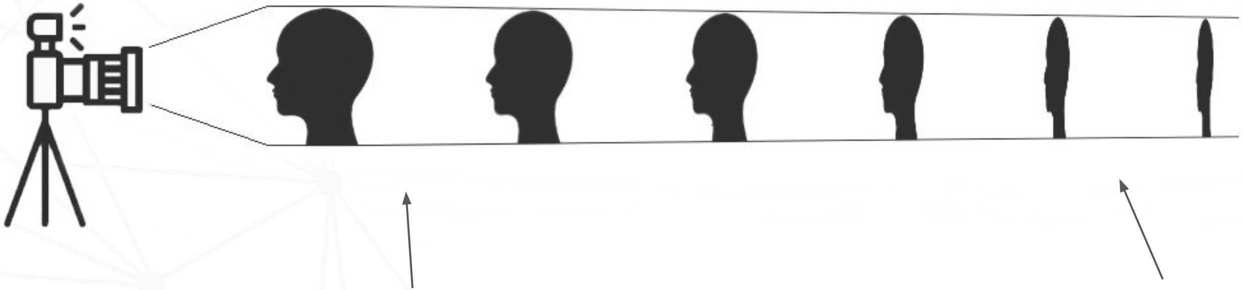
Humans visually recognize each other without a name or any additional information because we use an identity layer more foundational than Fiat.

# Layers of Human Identity

Your biology is more unique than your name

| | |
|---|---|
| Personal Preferences | Chosen by you, enforced by no one |
| Fiat/Govt Identity | Chosen by parents, issued & enforced by Govt |
| Biological Identity | Guided by DNA, influenced by environment |

# 2D Photos Connect Biometric & Fiat Layers



**Selfies Taken Here**

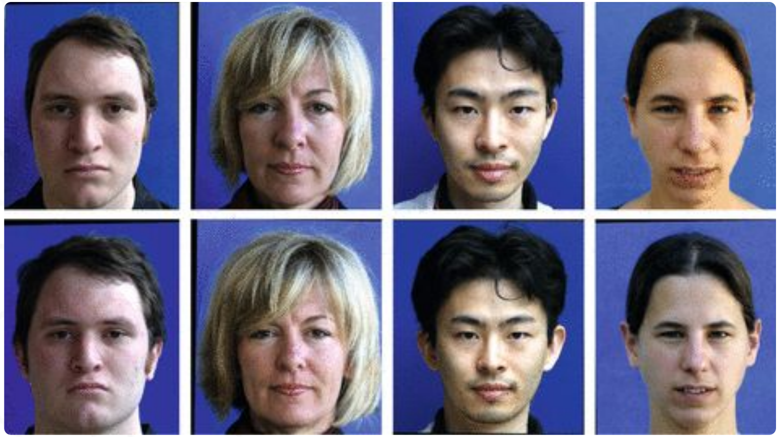
**Govt Photos Taken Here**

- Governments store at least 10 Billion Verified 2D photos globally
- Facial features “flatten” in 2D images as capture distance increases
- When a 3D face is flattened, much of the person’s unique data is lost

# 2D Photos Will Never Provide Enough Accuracy

**Close Selfie =**

Captured at ~2 Feet



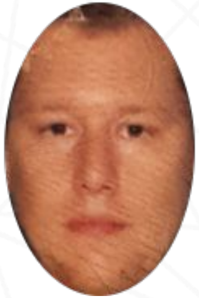
**= Govt. ID Photo**

Captured at ~6 Feet

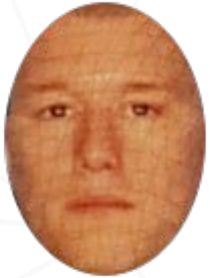
- Same person, same camera, same lens, different capture distance
- Lenses distort the subjects differently depending on the capture distance
- Capture inconsistency limits accuracy for 2D Face Matching algorithms

# Photos of the Same Person Can Look Very Different

FaceTec Bridges the gap between legacy 2D photo databases & new 3D technology

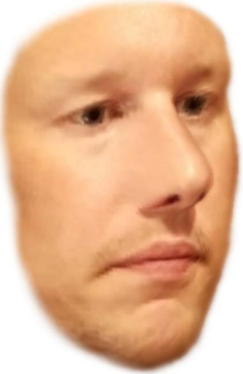


≈



**Low 2D:2D match**

[redacted]

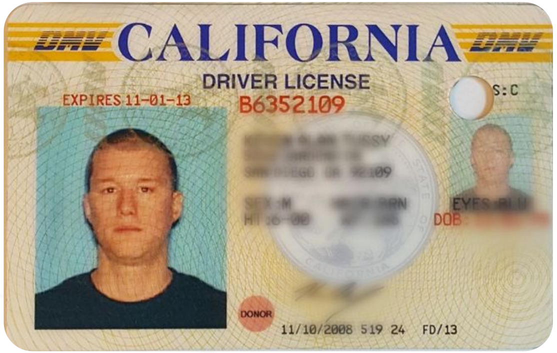


=

=

**3D FaceMap matches BOTH photos at 1/500,000 FAR**

@ <1% FRR



[redacted]

* For Illustrative Purposes

# A New Modality Designed For Digital Identity

FaceTec's patented Analog-to-Digital capture interface creates a topographic **3D FaceMap** from any smart device with a 2D camera.

* For Illustrative Purposes

- +10 Billion Devices Supported (.3mp cameras & up)
- iOS, Android, & PCs w/ Webcams (2.5 & 3.9mb SDKs)
- Strong, Concurrent 3D Liveness Detection
- Excellent Performance in All Lighting
- +98.1% First-Time User Success Rate
- No Observable Racial or Gender Bias (Like Apple's Face ID)
- Can't Be Captured at a Distance, or Surreptitiously

# How 3D FaceMaps Are Created

During the 2-sec session, a real user's face bends because of perspective distortion

Distortion *does not* occur with 2D spoof attempts

Proprietary AI processes up 120 video frames & proves user Liveness

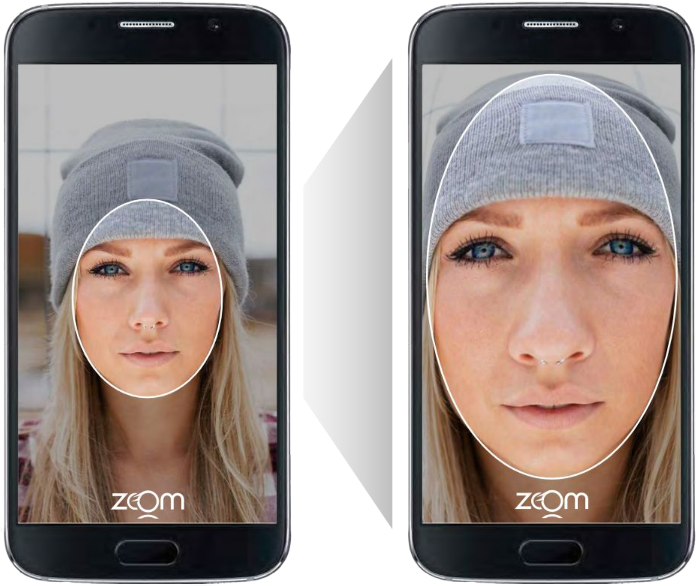
3D FaceMaps store ~100x more data than photos, allowing for glasses, beards & makeup

Liveness data expires to block replay attacks, and/or can be deleted to prevent honeypots

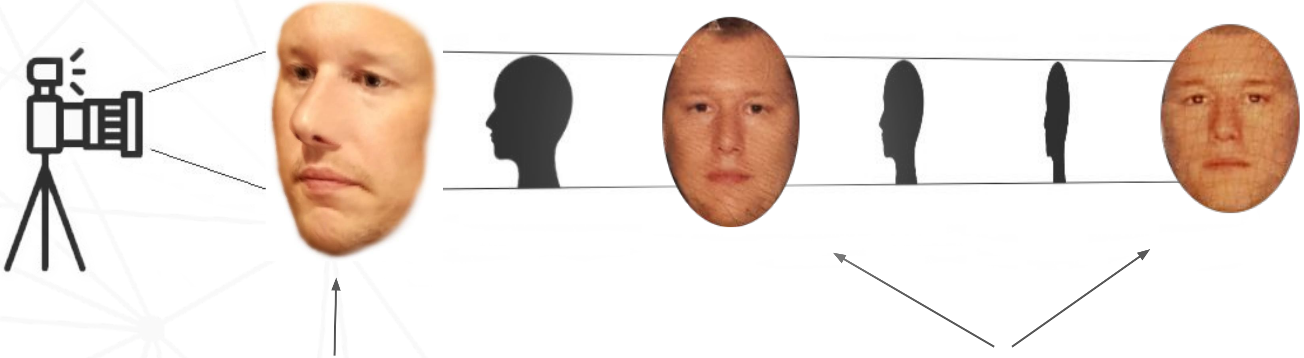
3D FaceScans = 350KB with Liveness Data, 3D FaceMaps contain only Matching Data = ~170KB

UnZoOmed Perspective
at 10 inches away

ZoOmed Perspective
at 6 inches away



# 3D FaceMaps Highly Match Any 2D Photo



**3D FaceMap Created Here** **=** **3D FaceMap Matches Both Highly**

- 3D FaceMaps are created by measuring “Perspective Distortion”
- Using 3D FaceMaps, FaceTec AI predicts how a person will appear at 2-12ft
- FaceTec AI determines IF the 2D photo was derived from that 3D Face

# 3D FaceMaps Match Very Highly to 2D Photos

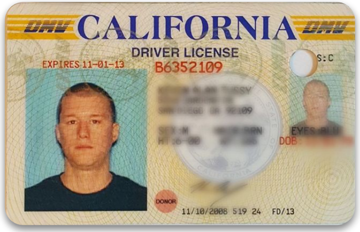
* For Illustrative Purposes

=

2D Face Portrait

=

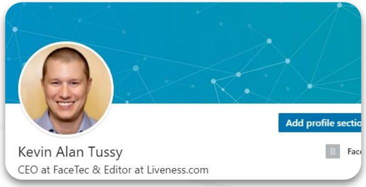
Photo ID Document



DMV CALIFORNIA DMV
DRIVER LICENSE
EXPIRES 11-01-13
B6352109
S:C
[redacted]
EYES
DOB
DONOR
11/10/2008 519 24 FD/13

=

Profile Pic



Add profile sectio

Kevin Alan Tussy
CEO at FaceTec & Editor at Liveness.com

# FaceTec’s 3D FaceMap Match Levels

* For Illustrative Purposes

=

**3D FaceMap to 3D FaceMap -** 1/125,000,000 FAR @ <1% FRR

- 1st Generation Topographical Depth & Texture Maps created by AI, not human viewable

=

**3D FaceMap to 2D Face Portrait -** 1/2,000,000 FAR @ <1% FRR

- 1st Generation Digital Photo, constrained Mugshot style

=

**3D FaceMap to Photo ID Document -** 1/500,000 FAR @ <1% FRR

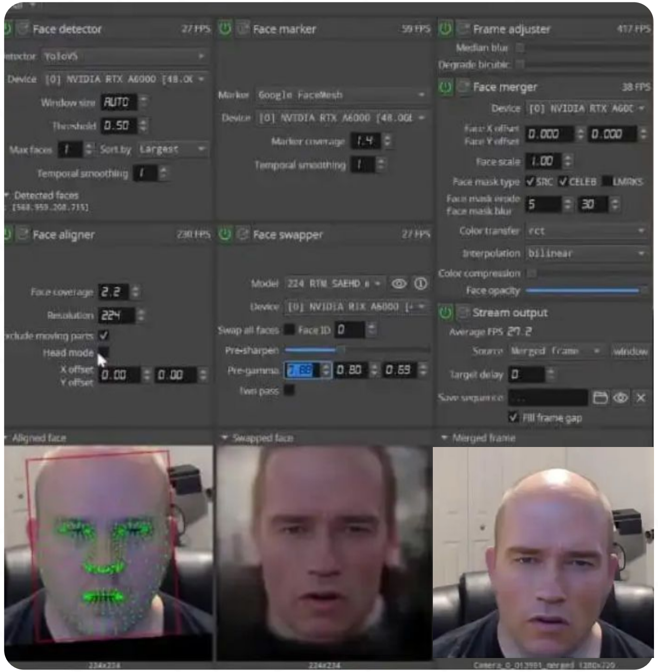
- 2nd Generation Photo of a Photo, holograms & anti-Tamper Lines OK, ends Passport Morphing

=

**3D FaceMap to Profile Pic ~** 1/100,000 FAR @ <1% FRR

- 1st Generation Digital Photo, no sunglasses, unconstrained w/ less than 15°of pose angle

# Next-Gen Attack Vectors Are Here



Face detector 27 FPS
Detector YoloV5
Device [0] NVIDIA RTX A6000 [48.0G
Window size AUTO
Threshold 0.50
Max faces 1 Sort by Largest
Temporal smoothing 1
Detected faces
[568,959,208,715]

Face marker 59 FPS
Marker Google FaceMesh
Device [0] NVIDIA RTX A6000 [48.0GB
Marker coverage 1.4
Temporal smoothing 1

Frame adjuster 417 FPS
Median blur
Degrade bicubic

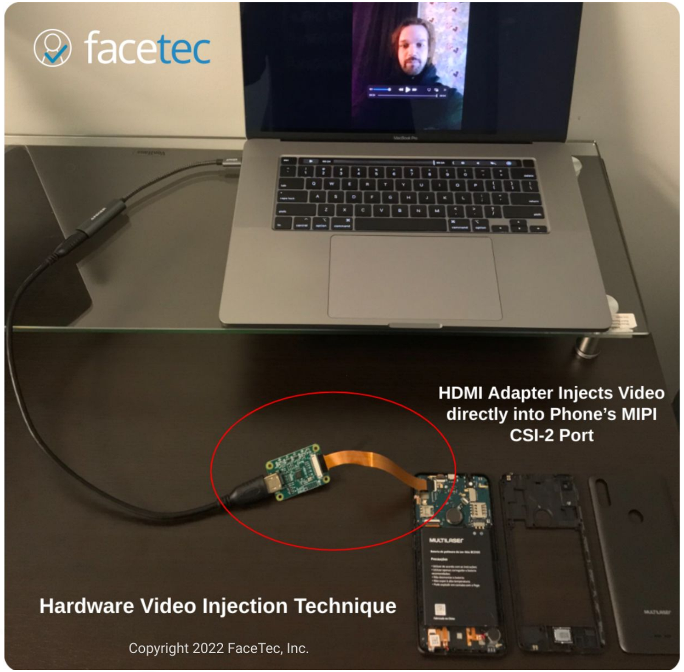
Face merger 38 FPS
Device [0] NVIDIA RTX A60C
Face X offset 0.000
Face Y offset 0.000
Face scale 1.00
Face mask type ✓ SRC ✓ CELEB □ LMRKS
Face mask erode 5
Face mask blur 30
Color transfer rct
Interpolation bilinear
Color compression
Face opacity

Face aligner 230 FPS
Face coverage 2.2
Resolution 224
Exclude moving parts ✓
Head mode □
X offset 0.00
Y offset 0.00

Face swapper 27 FPS
Model 224 RTM SAEHD
Device [0] NVIDIA RTX A6000
Swap all faces □ Face ID 0
Pre-sharpen
Pre-gamma 0.88 0.80 0.59
Two pass □

Stream output
Average FPS 27.2
Source Merged frame window
Target delay 0
Save sequence ...
✓ Fill frame gap

From 'DeepFace Live - Arnold Schwarzenegger 224 3.03M Iterations | RTX A6000'



HDMI Adapter Injects Video directly into Phone's MIPI CSI-2 Port

Hardware Video Injection Technique

See 2022 Liveness Security Report

# FaceTec’s 3D Liveness Detection

The Strongest in the Lab. The Strongest in the Real World.

- $200,000 Spoof Bounty Program, 24/7 since October 2019
- Bounty Program = Attack Vector Levels 1, 2, 3, 4 & 5
- Rebuffed >110,000 Attacks - 2 Bounties Paid & Patches Created
- Strong Web Browser Video Injection & Virtual Camera Detection
- iBeta Level 1 & 2 Certified, the First and Only
- Concurrent 3D Liveness on the Same Data as the 3D Matching
- Liveness Data expires & can be deleted preventing replays
- 3D FaceScan/Map & Device/Server SDK Pen Testing by Praetorian

PRAETORIAN

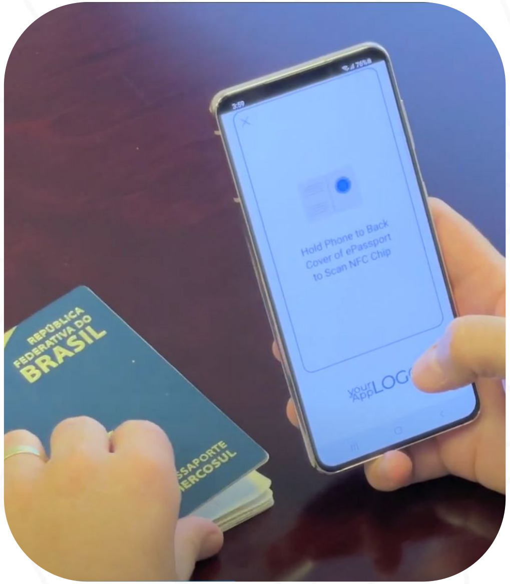
iBeta QUALITY ASSURANCE TESTED LEVEL 1 ISO 30107-3 Presentation Attack Detection CERTIFIED

iBeta QUALITY ASSURANCE TESTED LEVEL 2 ISO 30107-3 Presentation Attack Detection CERTIFIED

SpoofBounty.com
Crowd-Sourced Biometric Security Testing Explained

# FaceTec's Remote Identity Verification

Until Identity Issuers Verify Identity, We Must Use ID Documents


REPÚBLICA FEDERATIVA DO BRASIL
PASSAPORTE MERCOSUL
Hold Phone to Back Cover of ePassport to Scan NFC Chip
yourAppLOGO

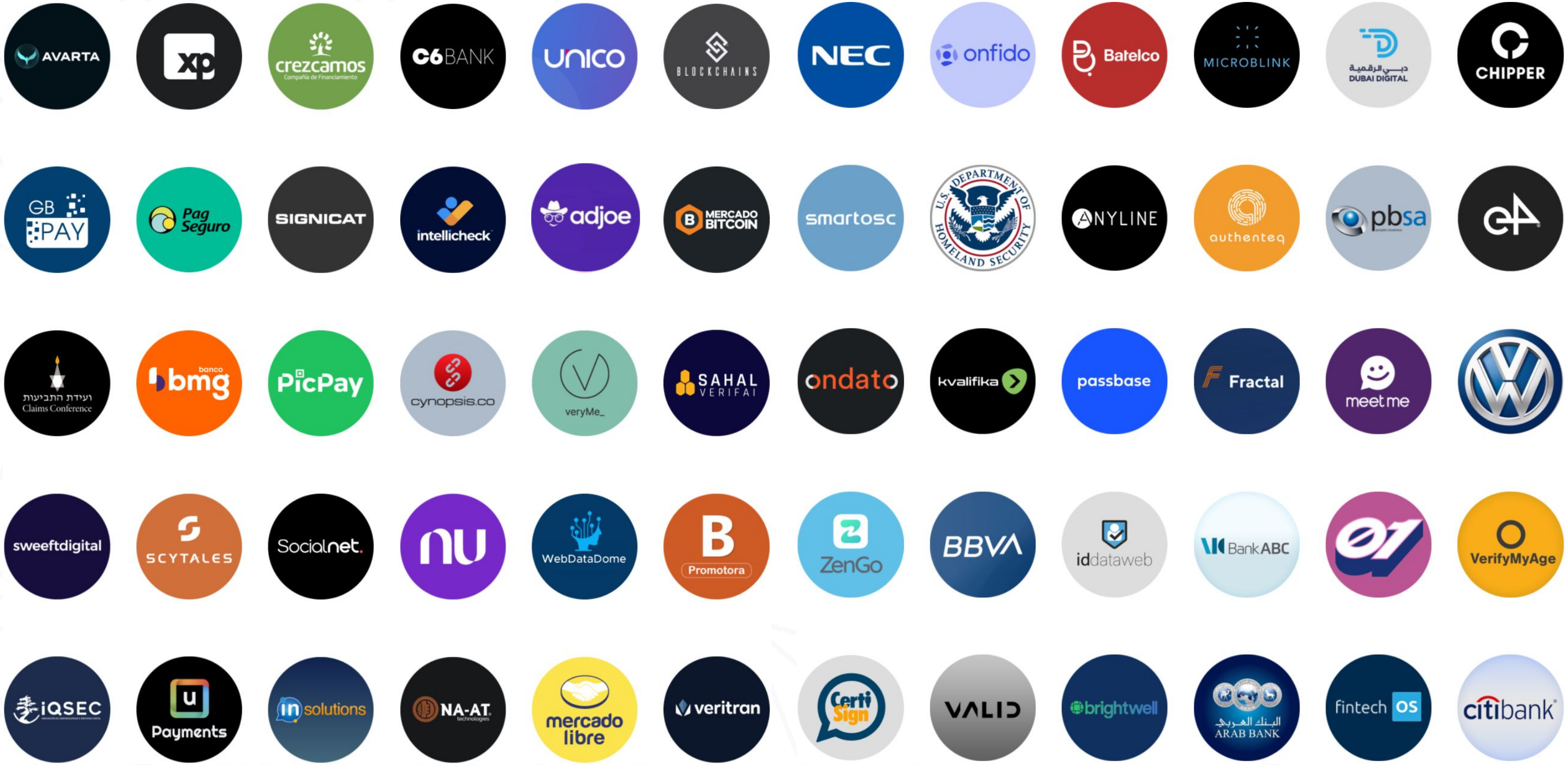
- Free OCR for Photo IDs & Passports
- Free Barcode/NFC Chip Scanning with Face Match
- Free Moderator Dashboard for Onboarding
- Over 700 Official ID Templates Included
- Use OCR Template Creator to Add ANY ID Document
- Auto-Captures High-Quality Images of the ID
- Anti-Photo Swap & Anti-Text Tamper Checks

# 3D FaceMaps & Broken Records

2D:2D is for surveillance; 3D:3D & 3D:2D is for Verifying Identity

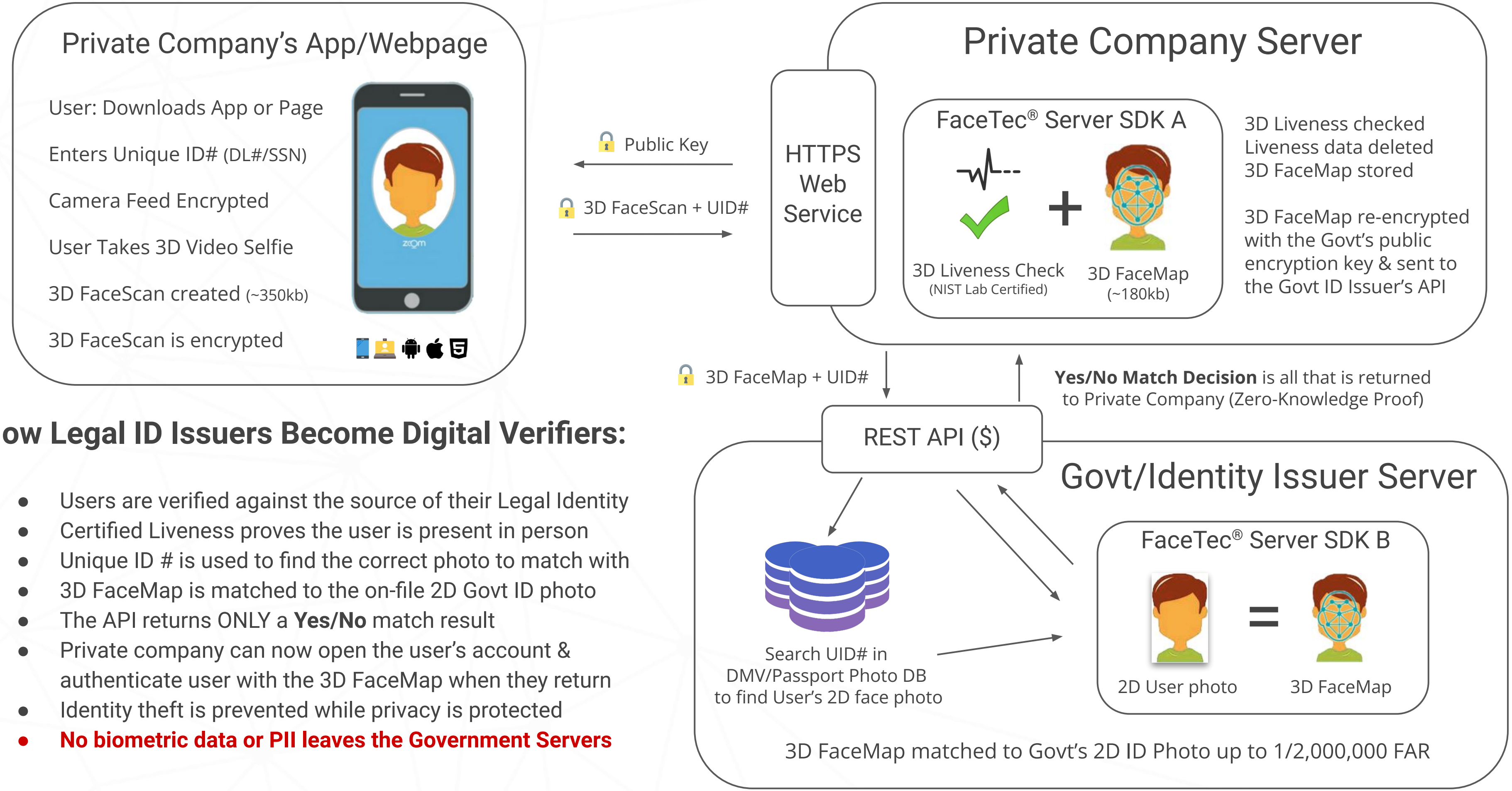
- 2D & 3D data captures appear similar, but accuracy is not
- 3D FaceMaps make Remote Identity Verification secure
- Apple knew 3D was required & uses 3D IR Cameras in Face ID
- NIST can’t test FaceTec’s OR Apple’s 3D Matching in FRVT
- 3D FaceMaps match very highly against 2D ID photos
- FaceTec has numerous US & Intl. patents on 3D FaceMaps
- FaceTec’s 3D Liveness Detection vastly superior to 2D
- FaceTec Encrypts the Camera Feed using its Device SDK

# FaceTec's Customers & Partners



& hundreds more...

facetec



Private Company's App/Webpage

User: Downloads App or Page

Enters Unique ID# (DL#/SSN)

Camera Feed Encrypted

User Takes 3D Video Selfie

3D FaceScan created (~350kb)

3D FaceScan is encrypted

Public Key

3D FaceScan + UID#

HTTPS Web Service

Private Company Server

FaceTec® Server SDK A

3D Liveness Check (NIST Lab Certified)

3D FaceMap (~180kb)

3D Liveness checked
Liveness data deleted
3D FaceMap stored

3D FaceMap re-encrypted with the Govt's public encryption key & sent to the Govt ID Issuer's API

3D FaceMap + UID#

**Yes/No Match Decision** is all that is returned to Private Company (Zero-Knowledge Proof)

REST API ($)

Govt/Identity Issuer Server

Search UID# in DMV/Passport Photo DB to find User's 2D face photo

FaceTec® Server SDK B

2D User photo = 3D FaceMap

3D FaceMap matched to Govt's 2D ID Photo up to 1/2,000,000 FAR

## How Legal ID Issuers Become Digital Verifiers:

- Users are verified against the source of their Legal Identity
- Certified Liveness proves the user is present in person
- Unique ID # is used to find the correct photo to match with
- 3D FaceMap is matched to the on-file 2D Govt ID photo
- The API returns ONLY a **Yes/No** match result
- Private company can now open the user's account & authenticate user with the 3D FaceMap when they return
- Identity theft is prevented while privacy is protected
- **No biometric data or PII leaves the Government Servers**

facetec

facetec

for more information, please visit

FaceTec.com

Liveness.com
Biometric Liveness Detection Explained