

# Liveness Detection and Robustness Against Fraud

May 2025

**Dr. Stephanie Schuckers**

Director, Center for Identification Technology Research (CITeR)

Professor, University of North Carolina - Charlotte

# Spoofting in the News

(Actual fraud, not just hacker demos)



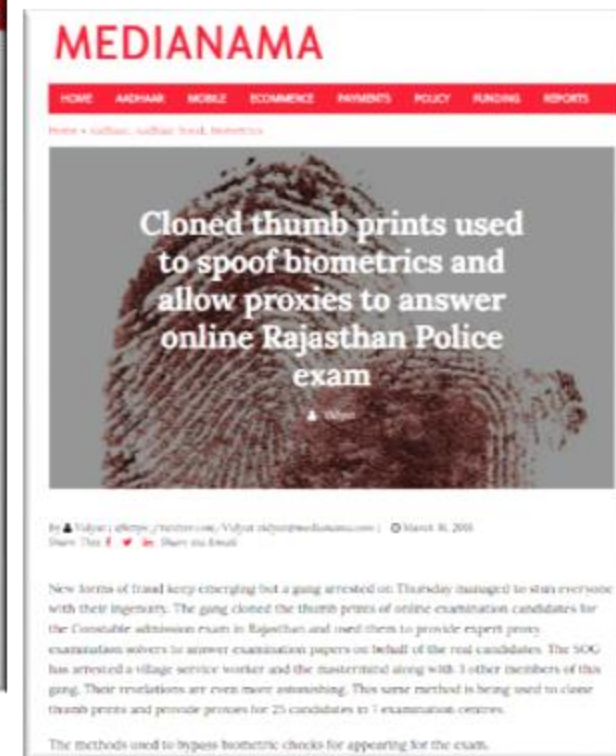
March 31, 2005



January 2, 2009



March 12, 2013



March 15, 2018

# Trust through Liveness

“It Is ‘Liveness’, Not Secrecy, That Counts.”  
Denning, Information Security Magazine, 2001

*(i.e. a stolen biometric is not useful)*



Laptop Display

High-quality photo mask

Low-quality photo paper



Low-quality 3D mask

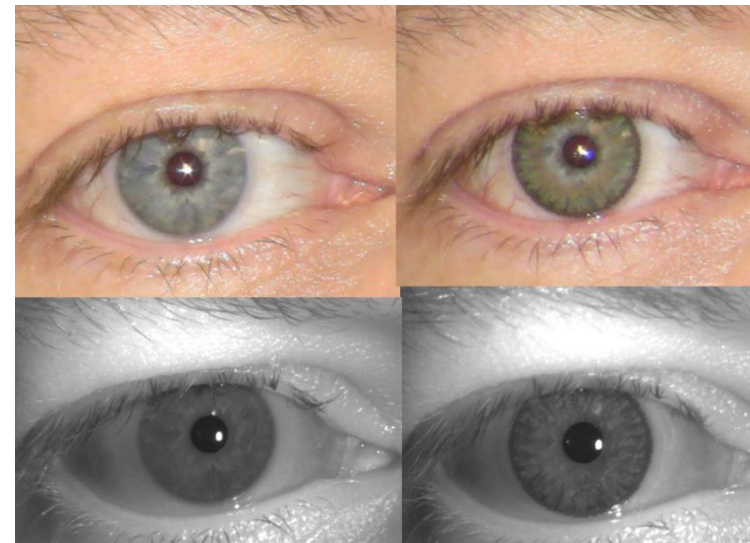
Medium-quality 3D mask

High-quality 3D mask

**Face Spoofs**



**Fingerprint Spoofs**



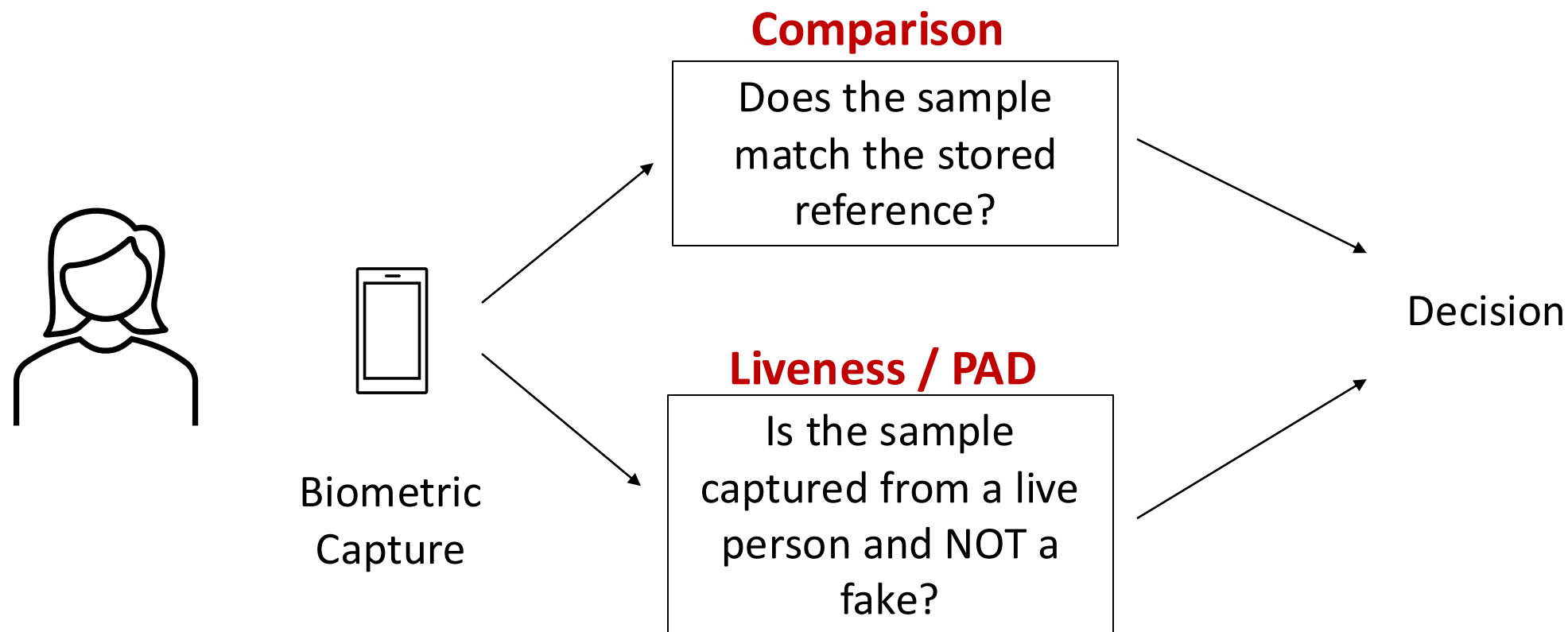
**Iris Spoofs**

# Vocabulary

- Presentation Attacks
  - Presentation of an artefact or human characteristic to the biometric capture subsystem in a fashion that could interfere with the intended policy of the biometric system\*
  - Spoofs, artefacts, altered biometrics, non-conformance, obfuscation
- Presentation Attack Detection (PAD)
  - Examples: **liveness detection**, altered fingerprint detection, anti-spoofing

\*from: ISO/IEC CD 30107-1, Information Technology — Biometrics --  
Presentation Attack Detection

# Biometrics - Comparison + Liveness



*Both critical components for effective biometric recognition*

# Biometric Security—Attack Examples

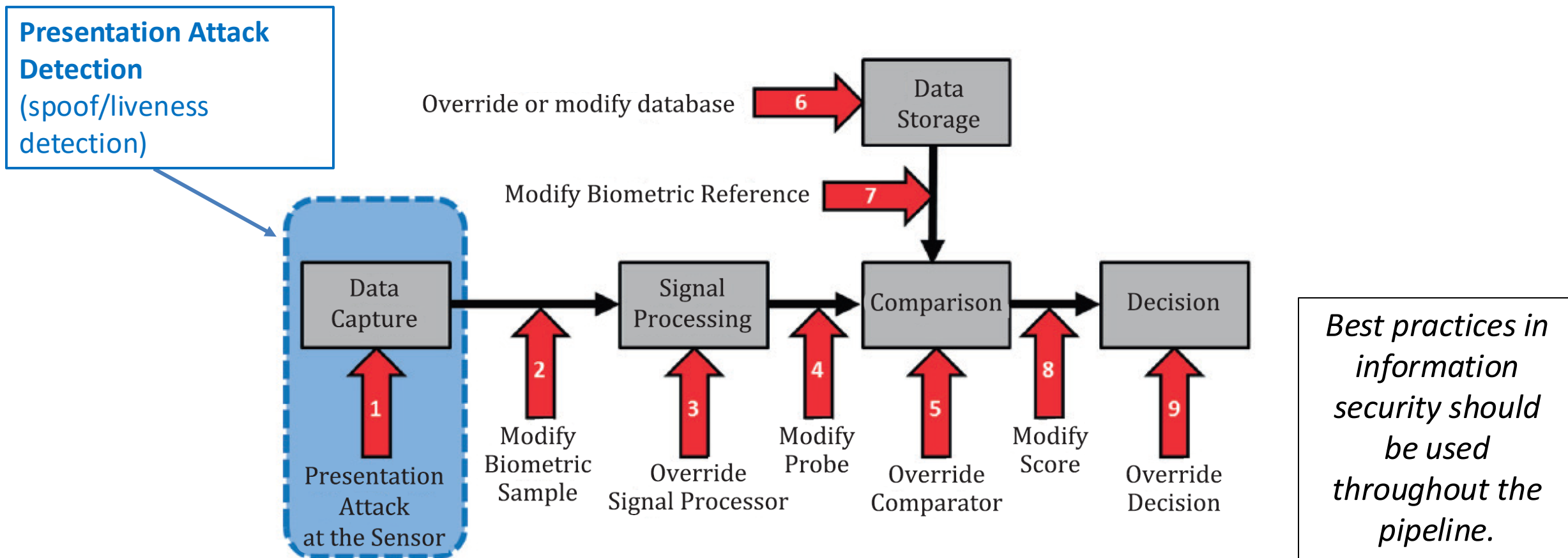


Figure 2 — Examples of points of attack in a biometric system (from ISO/IEC 30107-1)

# PAD Categories defined in ISO 30107

1. Liveness not related to challenge-response (“passive”)\*
2. Involuntary Challenge Response  
e.g. random colors of light; change in pupil dilation due to random input
3. Voluntary Challenge Response  
e.g. blinking/smiling at a specific time; saying specific words that are randomly given

\*Active PAD not defined in ISO

From: ISO/IEC 30107-1, Information  
Technology — Biometrics -- Presentation  
Attack Detection

# Iphone X - Face

- “To counter both digital and physical spoofs, the TrueDepth camera **randomizes** the sequence of 2D images and depth map captures, and projects a **device-specific random pattern.**” \*

## WIRED



ANDY GREENBERG SECURITY 11.12.17 06:44 PM  
**HACKERS SAY THEY'VE BROKEN FACE ID A WEEK AFTER IPHONE X RELEASE**



*This article has been updated below with another, more convincing video demonstration of Bkav's Face ID spoofing, which the firm revealed two weeks after the original.*

When Apple released the iPhone X on November 3, it touched off an immediate race among hackers around the world to be the first to fool the company's futuristic new

# Challenge

Evaluation of PAD needed to ensure usable, effective performance in the face of evolving attacks

# Lab Controlled Spoofing

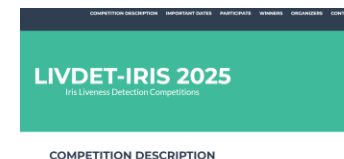


# Benchmarking – Liveness Detection (LivDet)

- Liveness Detection Competitions 2009, 2011, 2013, 2015, 2017, 2019, 2020, 2021, 2023, 2024, 2025
  - Sense of the State of the Art in the Field
  - Part I: Algorithms & Part II: Systems
  - Publically available databases to support R&D (even after competitions)
  - Fingerprint—U of Cagliari, Clarkson U
  - Iris—Clarkson U, Notre Dame University & Warsaw U, WVU, I
  - Face—Clarkson U, IDIAP, University of Georgia



<http://livdet.org>



The Department of Electrical and Electronic Engineering of the University of Cagliari, the Italian Group of the International Biometric and the Department of Electrical and Computer Engineering of the Clarkson University are proud to announce the sixth edition of the Fingerprint Liveness Detection Competition.



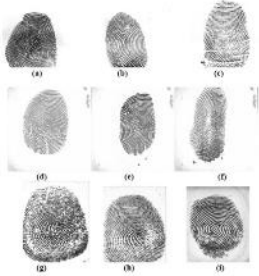
**Synopsis** – The widespread use of personal verification systems based on fingerprints has shown some weaknesses related to the problem of security. Among the others, it is well-known that a fingerprint verification system can be deceived by submitting artificial reproductions of fingerprints made up of silicon or gelatin in the electronic system (silicon fingers, etc.). These replicas are then processed as “real” fingerprints.

**Liveness Detection** – Therefore, a major issue in the field of security in fingerprint verification (conspicuously known as “liveness detection” or “presentation attack detection” (PAD)). The standard verification system is coupled with additional hardware or software modules aimed to certify the authenticity of the submitted fingerprints. Whilst hardware-based solutions are the most expensive, software-based ones attempt to measure liveness by the characteristics of image perception by image analysis image processing algorithms.

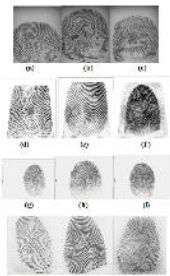
# Benchmark Datasets from LivDet

- Over 100,000 spoof and lives images shared
- Over 400 requests from over 40 countries

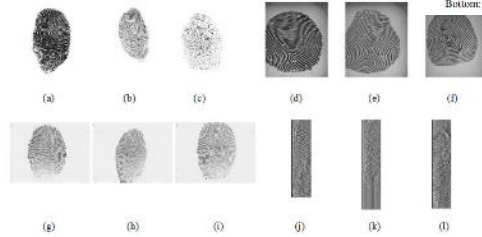
## LivDet 2009



## LivDet 2011



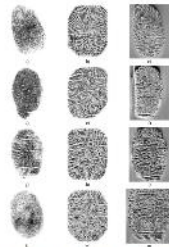
## LivDet 2013



## LivDet 2015



## LivDet 2019



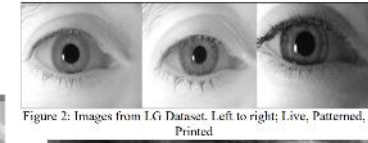
## LivDet 2021 to 2025



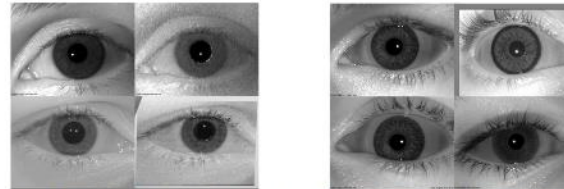
## LivDet 2025



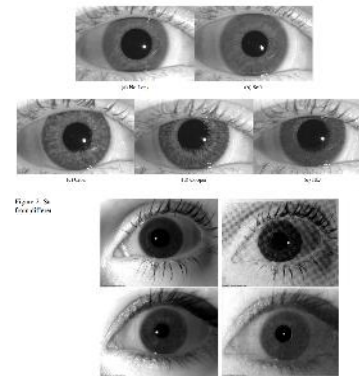
## LivDet-Iris 2015



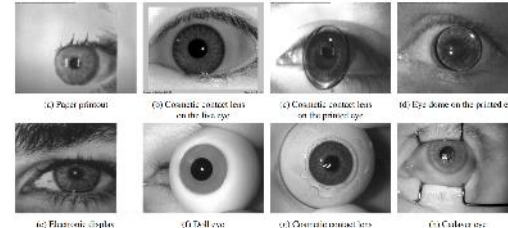
## LivDet-Iris 2017



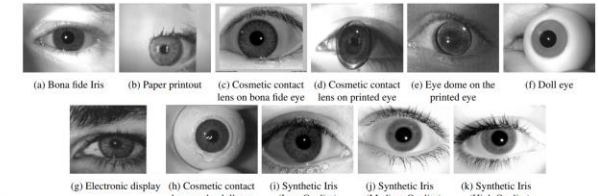
## LivDet-Iris 2013



## LivDet-Iris 2020



## LivDet-Iris 2023



## LivDet-Face 2021



## LivDet-Face 2025



Figure 4: Examples of spoof images of the LivDet 2009 dataset. Crossmatch (top): (a) Lay Doh, (b) gelatin, (c) silicone. Ekanis (middle): (d) Play-Doh, (e) gelatin, (f) silicone. Biometrica (top): (g) Play-Doh, (h) gelatin, (i) silicone.

Figure 5: Examples of spoof images of the LivDet 2011 dataset. From Crossmatch: (a) body double, (b) latex, (c) wood glue, from Biometrica: (d) gelatin, (e) latex, (f) wood glue, from Ikalda: (g) gelatin, (h) latex, (i) wood glue, from Swipe: (j) body double, (k) latex, (l) wood glue.

Figure 6: Examples of fake fingerprint images of the LivDet 2013. From Crossmatch: (a) body double, (b) latex, (c) wood glue, from Biometrica: (d) gelatin, (e) latex, (f) wood glue, from Ikalda: (g) gelatin, (h) latex, (i) wood glue, from Swipe: (j) body double, (k) latex, (l) wood glue.

Figure 7: Examples of samples LivDet fingerprint dataset. In the first row: live fingerprints for a Chinese Biometric Passport and a Canadian Scanner. In the second row: there is Min 2 spoof images for the Green Eye, the Digital Recognition and a Canadian scanner. In the third row: there is a Digital Recognition and a Canadian scanner. In the last row: the samples of Min 1 spoof materials with the same order as the first row. We can appreciate in the three columns the variety of the scanner, the quality of the face, the liveness as a thermal source, and the material used to create the spoofing. The last image is a synthetic fingerprint.

Purnapatra, et al 2023. Liveness Detection Competition-Noncontact-based Fingerprint Algorithms and Systems (LivDet-2023 Noncontact Fingerprint). In 2023 IEEE International Joint Conference on Biometrics (IJCB) (pp. 1-10). IEEE.

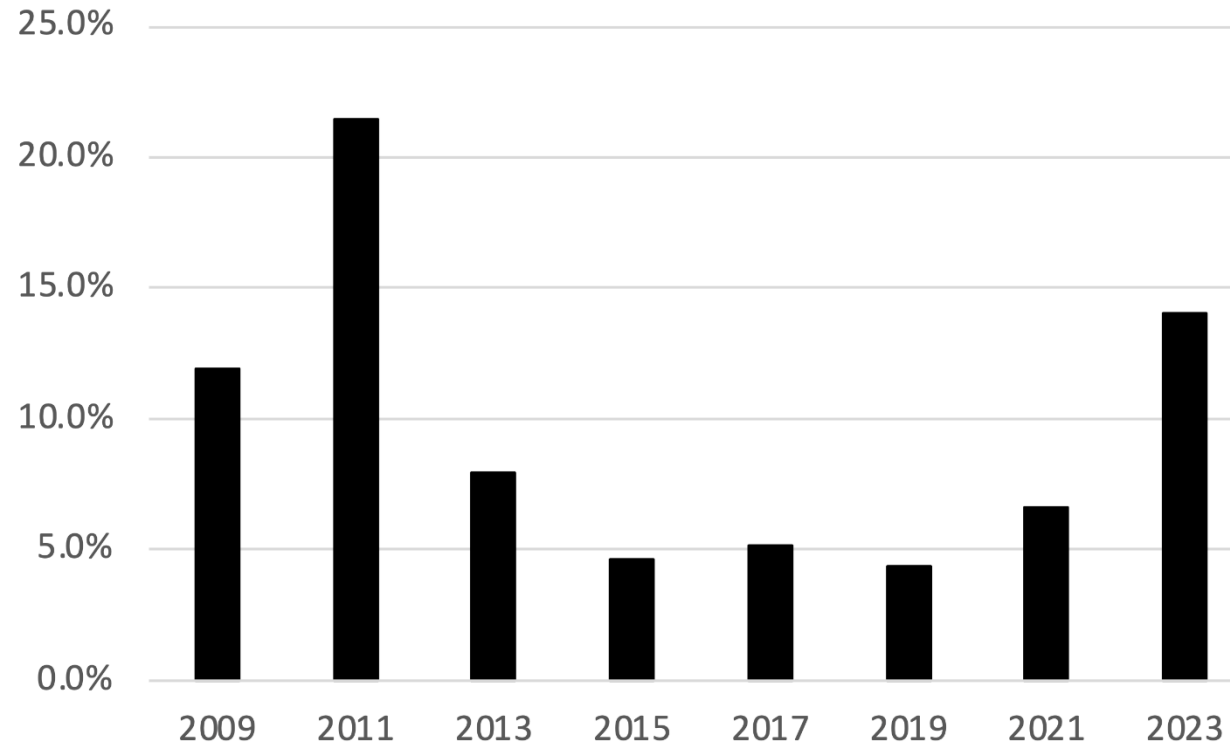
Micheletto, M., Orrù, G., Casula, R., Yambay, D., Marcialis, G.L. and Schuckers, S.C., 2022. Review of the Fingerprint Liveness Detection (LivDet) competition series: from 2009 to 2021. arXiv preprint arXiv:2202.07259.

Igene, L. et al, 2024, September. Face Liveness Detection Competition (LivDet-Face)-2024. In 2024 IEEE International Joint Conference on Biometrics (IJCB) (pp. 1-9). IEEE.

Tinsley, P., et al, 2023, September. Iris liveness detection competition (livdet-iris)-the 2023 edition. In 2023 IEEE International Joint Conference on Biometrics (IJCB) (pp. 1-10). IEEE.

Purnapatra, S, et al., 2023, September. Liveness detection competition-noncontact-based fingerprint algorithms and systems (livdet-2023 noncontact fingerprint). 2023

# LivDet over the years (Fingerprint)



Average of APCER and BPCER for top two performers across all databases tested in LivDet competitions hosted 2009 to 2023

Micheletto, M., Orrù, G., Casula, R., Yambay, D., Marcialis, G.L. and Schuckers, S.C., 2022. Review of the Fingerprint Liveness Detection (LivDet) competition series: from 2009 to 2021. arXiv preprint arXiv:2202.07259.

Ghiani, L., Yambay, D.A., Mura, V., Marcialis, G.L., Roli, F. and Schuckers, S.A., 2017. Review of the Fingerprint Liveness Detection (LivDet) competition series: 2009 to 2015. *Image and Vision Computing*, 58, pp.110-128.

\*Crossmatch removed

# Challenge

Trust in technology—Securing Against the Use of Deepfakes that Interfere with Biometric Recognition

# Challenge: Deepfakes and Biometric Recognition

## Problem:

- May interfere with biometric recognition
  - E.g. can impart “liveness” characteristics to a stolen image



James Vincent, Tom Cruise deepfake creator says public shouldn't be worried about 'one-click fakes', The Verge, Mar 5, 2021.

<https://www.theverge.com/2021/3/5/22314980/tom-cruise-deepfake-tiktok-videos-ai-impersonator-chris-ume-miles-fisher>

# Original



# Example Deepfake



## (a) Homepage

### DEEPPFAKE-O-METER

An Open Platform Integrating State-Of-The-Art Algorithms for DeepFake Image, Video, and Audio Detection

## (b) Result Page

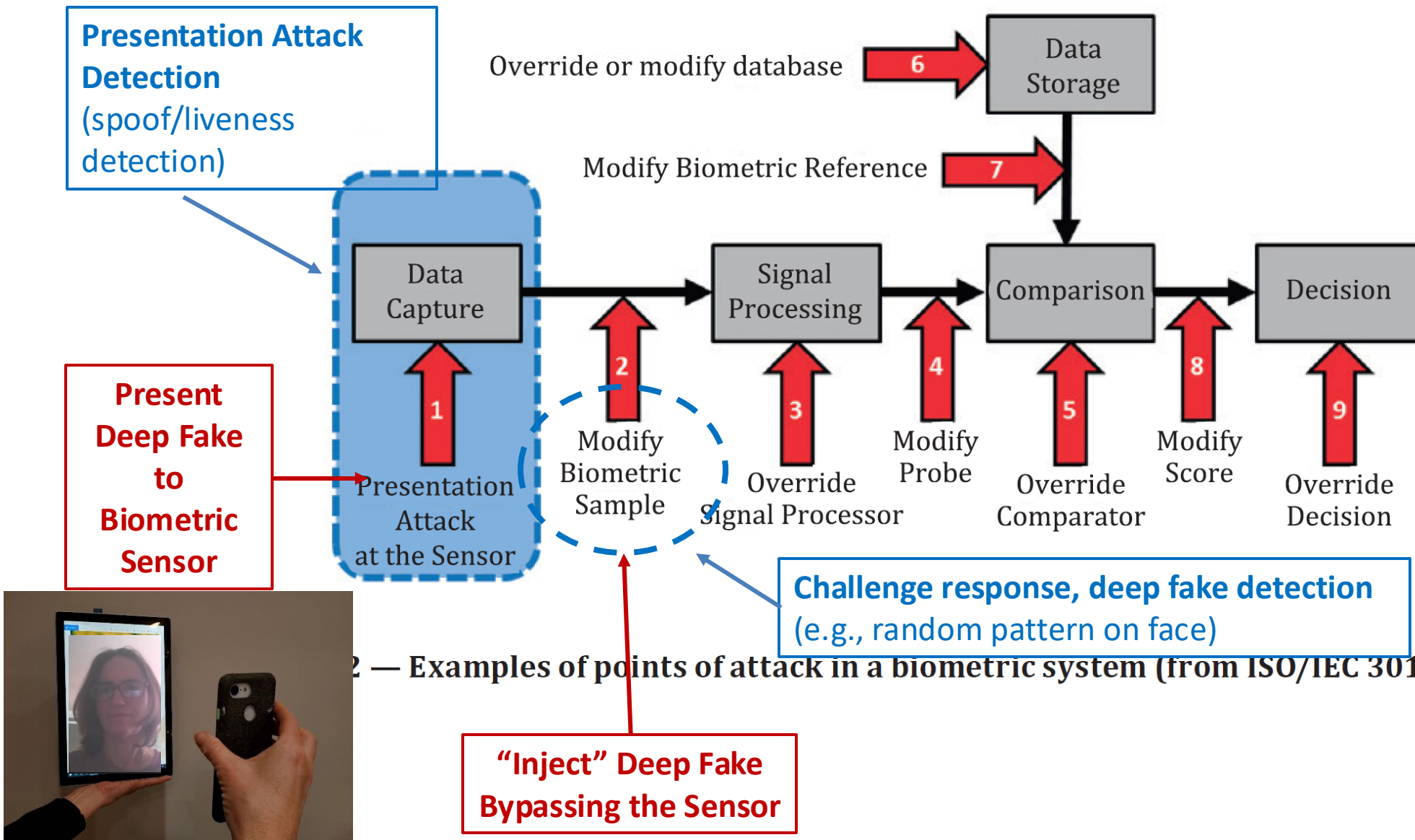
The likelihood score derived from the method indicates the probability of the input being fake. This score reflects the extent to which the input shares characteristics with the real or fake data labeled in the training set of the method, as reported in the original study, supported by correlation statistics. However, it is important to note that this score should not be considered as providing deterministic result.

Detector	Result	Details
NoDown	0.0% AI-Generated Likelihood	Completed
GLFF	2.8% AI-Generated Likelihood	Completed
CLIP-VIT	0.1% AI-Generated Likelihood	Completed
NPR	Processing..... (estimated time: 30s)	

Try it!

[https://zinc.cse.buffalo.edu/ubmdfl/deep-o-meter/home\\_login](https://zinc.cse.buffalo.edu/ubmdfl/deep-o-meter/home_login)

# Biometric Security—Attack Examples



# PAD and Injection Attacks

## Presentation Attack Detection\*

- ISO/IEC 30107
- Categories
  - **Liveness** not related to challenge-response (“passive”)
  - Involuntary Challenge Response
    - e.g. random colors of light; change in pupil dilation due to random input
  - Voluntary Challenge Response
    - e.g. blinking/smiling at a specific time; saying specific words that are randomly given

\*Active PAD not defined in ISO

## Injection Attack Detection

- ISO/IEC 25456 (under development)
- Possible similar solutions:
  - **Deepfake detection** not related to challenge-response (“passive”)
  - Involuntary Challenge Response
    - e.g. random colors of light; change in pupil dilation due to random input
  - Voluntary Challenge Response
    - e.g. blinking/smiling at a specific time; saying specific words that are randomly given
  - **Best practices in IT security**

*Based on ISO standards*

*Independent network of laboratories*

## Challenge

Lack of an ecosystem of  
certified biometrics products

*Requirements defined by subject matter experts*

# What is the FIDO Alliance?



The FIDO Alliance is an open industry association with a focused mission: **reduce the world's reliance on passwords.**

# Backed by 300+ global tech leaders



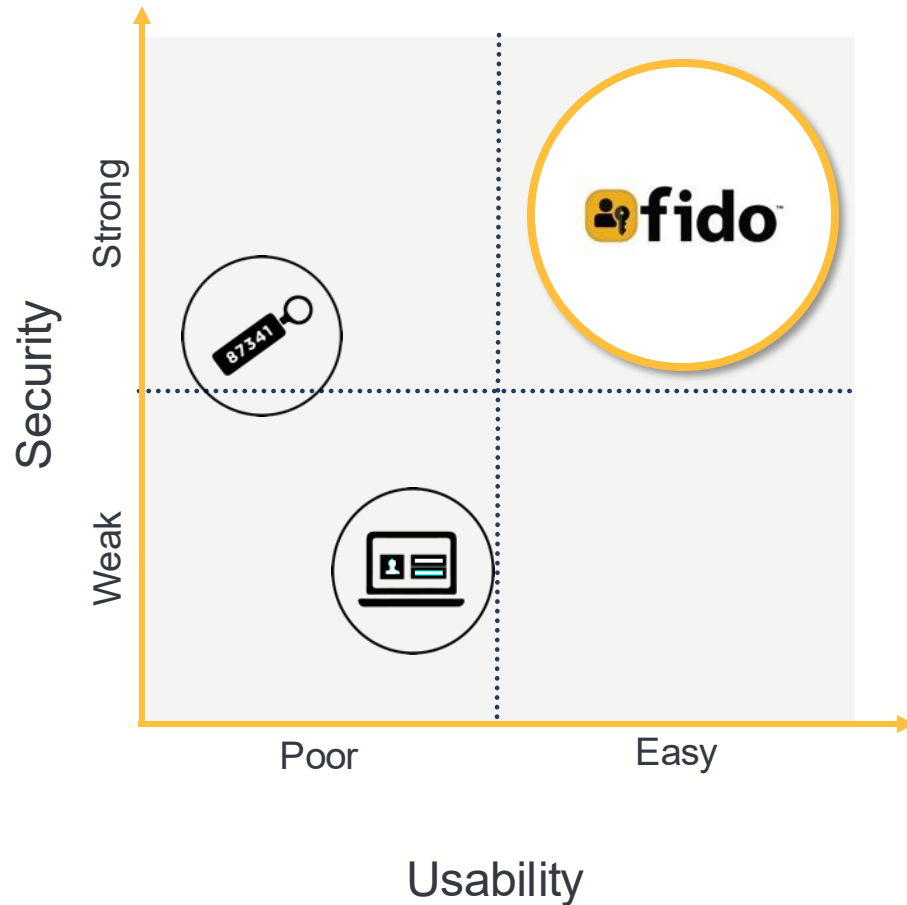
+ Sponsor members

+ Associate members

+ Liaison members

+ Government members

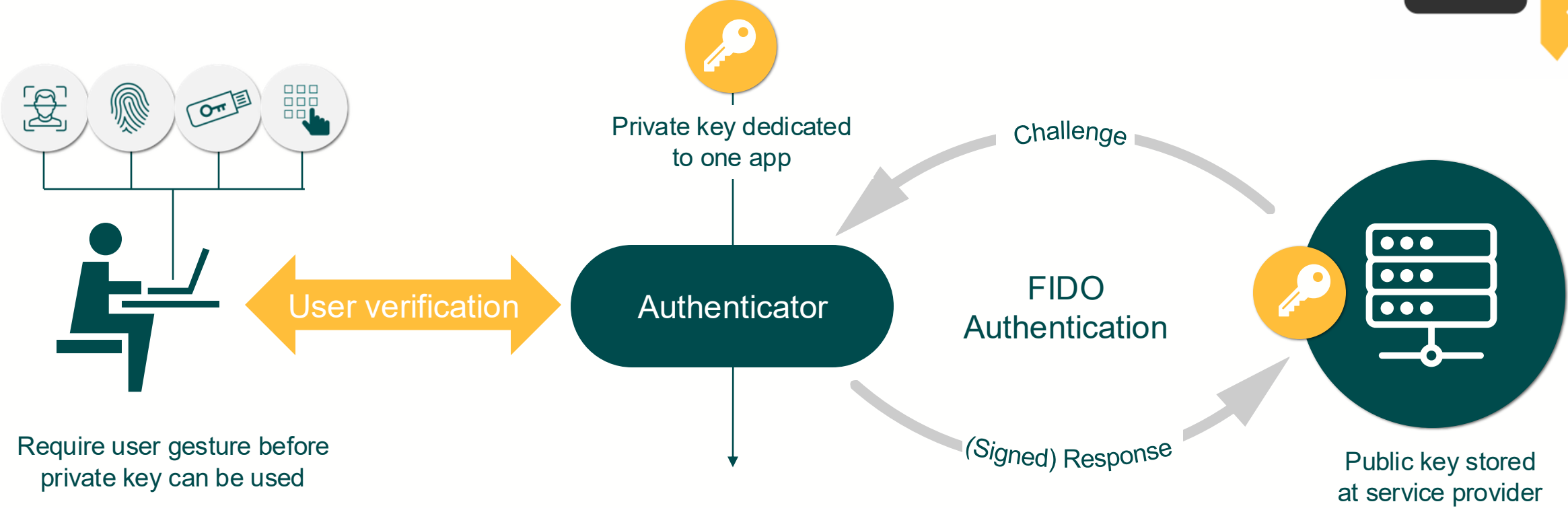
# FIDO since 2013: Simpler and stronger



Open standards for simpler, stronger authentication using **public key cryptography**

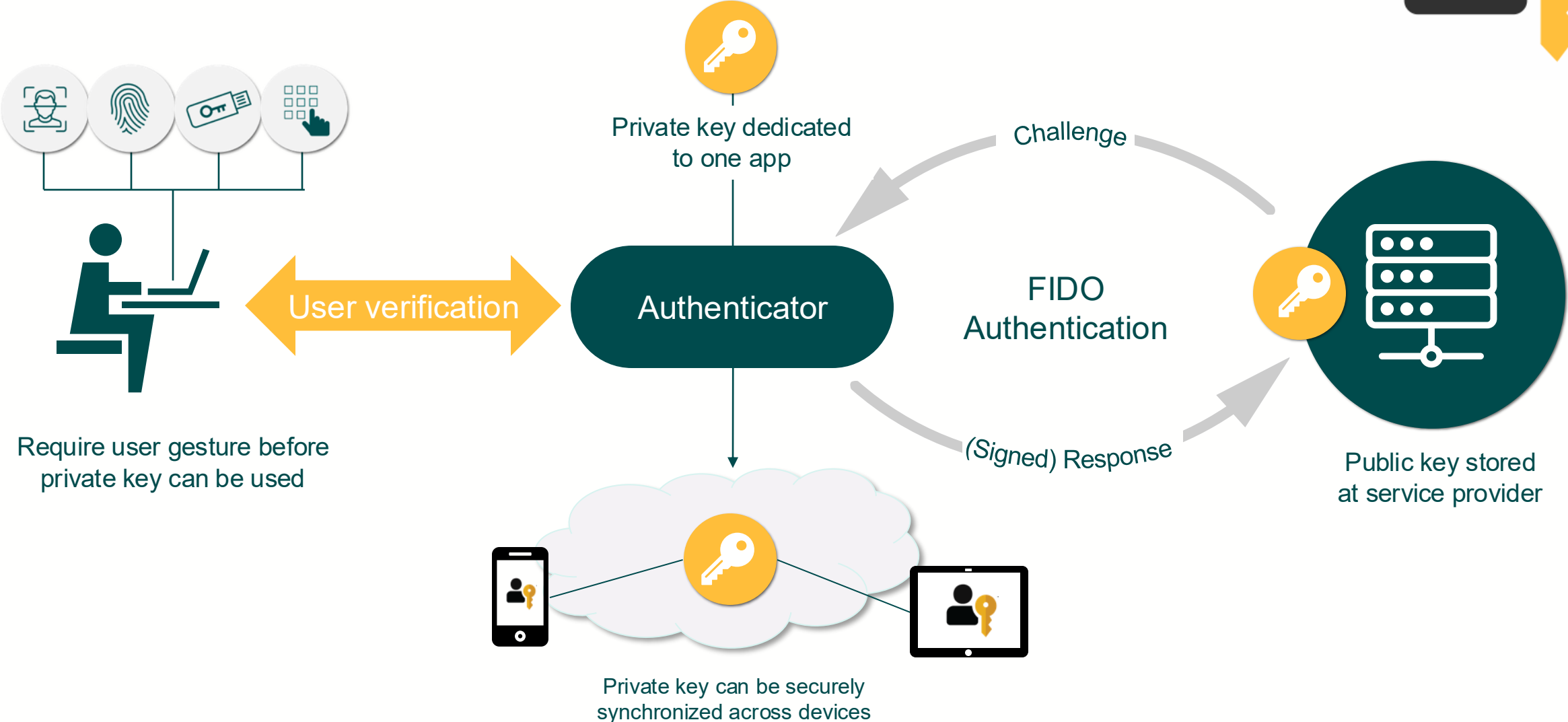
- Single Gesture –
- Possession-based –
- Phishing-resistant –

# FIDO Authentication “Passkey”: How it works



Require user gesture before private key can be used

# Newer syncing capabilities (introduced in 2022)



Require user gesture before private key can be used

Private key can be securely synchronized across devices

# Operating Systems offering Passkeys

Chrome on Windows



Firefox on Windows

Chrome on Android

Edge on Android

Apps on iOS



Safari on iOS

Chrome on Mac

Edge on Mac

Edge on Ubuntu



Chrome on iOS

Edge on iOS

Apps on Mac

**Available Today!**

Apps on Android

Chrome on Ubuntu



Safari on Mac

Edge on Windows

# Account Lifecycle: **Risks today**



## Account Enrollment & Identity Verification

Knowledge-based authentication  
Synthetic IDs  
Fabricated biometrics  
Injection attacks  
Presentation attacks  
Biased face verification results



## User Authentication

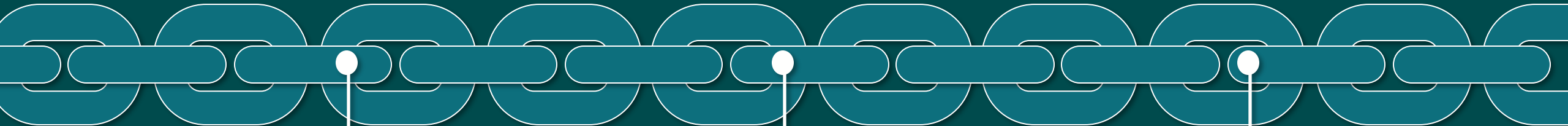
Phishing  
Credential stuffing  
Man in the Middle  
Spear-phishing  
SIM swapping  
Social engineering



## Account Recovery & Identity Re-verification

Account take over  
Consumer and business fraud  
Stolen identities  
Business Email Compromise

# Securing the Account Lifecycle: **The FIDO Approach**



**Secure Account Enrollment**

Certified Remote Identity Verification



**Phishing-resistant User Authentication**

Passkeys



**Secure Account Recovery**



# FIDO IDV and Biometric Certification



## Document Authenticity

- Tests for authenticity of government-issued ID documents
- Verifies the authenticity of government-issued documents during initial account set up and account recovery (i.e., employees, citizens)
- Complements the FIDO IDV Face Verification program



## Face Verification

- Tests for security, bias, accuracy, and liveness of facial biometrics
- Verifies identities using “selfie-match” technology matched to the user’s government-issued ID (i.e., employee onboarding with I-9 and passport)
- Complements the IDV Document Authenticity program



## Biometric Components

- Tests for security, bias, and accuracy of biometric performance during FIDO authentication
- Assures performance, interoperability, and security of biometric components used in FIDO authentication
- Complements the FIDO Certified Authenticator program

# FIDO Certification Programs



## ISO based evaluations

Evaluations based  
ISO standards



## Proven Trusted Authority

Requirements defined by  
leading industry stakeholders



## Independent Accredited Testing

International Network of  
Accredited Laboratories

# Biometric Component Certification

**Certifies the efficacy of biometric subsystems, including:**

- End-to-end performance (scenario testing)
  - FAR / FRR
- Differential assessment of demographic groups
- Presentation attack detection (PAD)

**Independent validation of biometric performance.**

- No need to maintain own program for evaluating biometric products.
- Requirements developed by a diverse, international group of stakeholders from industry, government, and subject matter experts.
- Evaluation conforms to ISO standards around biometric evaluation.

**Complements FIDO Authenticator Certification at Level 2 Security and is mandatory at Level 3/L3+ Security Certification.**

FIDO® Certified Biometric  
Component Solutions



# Sample PAI Species for Fingerprint

Species	Level
Fingerprint image printed on inkjet or laser printer	A
Fingerprint image converted to a mold which is used to make a cast with materials such as gelatin or silicon	B
Same as previous with graphite or other material placed on surface of mold	B
3D printed fingerprints	C
Fingerprint models which capture sweating, veins, blood flow or more sophisticated finger information	C

# Performance Differentials - Optional Certification

🔗 Address significant concern around bias and fairness in biometric recognition

🔗 Available for:

- ✦ Biometric Component: Levels 1+ and 2+
- ✦ Face verification for rIDV: Level 2 increased to 245 subjects

🔗 Performance requirements for each demographic subgroup

- ✦ Age - 3 groups (18-30; 31-50; >50)
- ✦ Gender - 2 groups (Male, Female, Other)
  - Other is an option, but will not be analyzed due to low sample size
- ✦ Monk Skin Tone – Combined to 3 groups



<https://skintone.google/the-scale>



**USE PASSKEYS!**

**THANK YOU**

# Good practice for biometrics

## Biometric vulnerabilities



### Top 10 Vulnerability Questions

A guiding document that provides clarification around some of the frequently asked questions about the spoofing of biometrics.



### Biometrics Vulnerability Assessment Checklist

A checklist which complements the Top 10 Vulnerability Questions, prepared to help guide members in addressing vulnerability assessments in biometrics.



### Presentation attack detection (PAD) and liveness guiding document

This document explaining what PAD and liveness is and suggests some general considerations and questions users may want to ask when choosing a biometric product.

# Conclusions

- Presentation Attack Detection (PAD)
  - Attacks at the biometric sensor – Physical attacks
  - Biometrics + Liveness/PAD = Success!
- Injection Attack Detection (IAD)
  - Attacks which “bypass” the biometric sensor – Digital attacks
  - IAD can use similar approaches to PAD, but with a different purpose
  - Biometrics + Liveness/PAD/IAD = Success!
- FIDO Biometric Certification
  - Incorporates both live subject testing + PAD testing + fairness evaluation
  - Value Proposition
    - Requirements developed by biometrics experts
    - Independent, international network of laboratories
    - Based on ISO standards
  - Future work – IAD evaluation

# Special Thanks to CITeR Current Affiliates—2025

- ACV Auctions
- Athena Sciences
- Aware
- DRDC—Defence Research and Development Canada (DRDC)
- DoD—Defense Forensics and Biometrics Agency
- DoD – Defense Forensic Science Center
- DHS—Office of Biometric Identity Management
- DHS—Science & Technology
- Federal Bureau of Investigation
- General Services Administration (GSA)
- Home Team Science and Technology Agency (HTX) – Singapore

- Idemia
- Ingenium
- Israel National Cyber Directorate (INCD)
- iProov
- Metalenz
- National Security Agency (NSA)
- Oak Ridge National Labs (ORNL)
- Precise Biometrics
- PrivateID
- Public Safety Canada
- Qualcomm
- Synolo
- Thales
- Tools for Humanity



Public Safety  
Canada

Sécurité publique  
Canada



Defence Research and  
Development Canada

Recherche et développement  
pour la défense Canada





# Good practice for biometrics

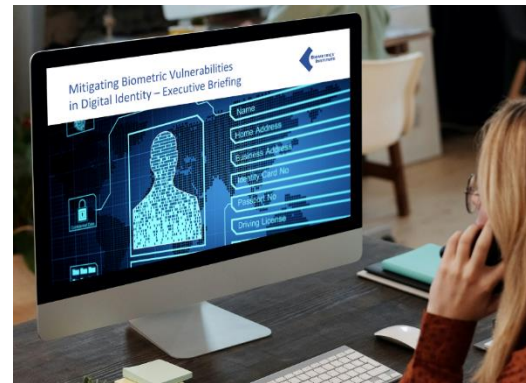
## Privacy and digital identity



### Privacy Guidelines

Guidelines for biometrics and privacy, lawfulness, fairness, transparency, and trust.

This updated guide features 18 principles and now incorporates advice on AI, guidance on brainwave biometrics, test use cases for each principle, and actionable insights with key questions.



### Mitigating Biometric Vulnerabilities in Digital Identity – Executive Briefing

A clear and high-level overview of biometric vulnerability risks associated with digital identity and how adversaries might exploit these vulnerabilities in your biometric systems.



### Digital Onboarding and Biometrics

An overview of how biometrics intersects with digital identity onboarding to help improve performance of biometric digital onboarding services and increase confidence in the identity of those being onboarded.



### Digital Identity and Biometric Authentication

Recommended good practices for implementing biometric authentication in a secure and effective manner. With guidance to develop new authentication processes or enhance existing ones.