Digitalisation of Justice:
Face Biometric Verification for Secure Digital Presence

Joe Palmer, Chief Product & Innovations Officer, iProov

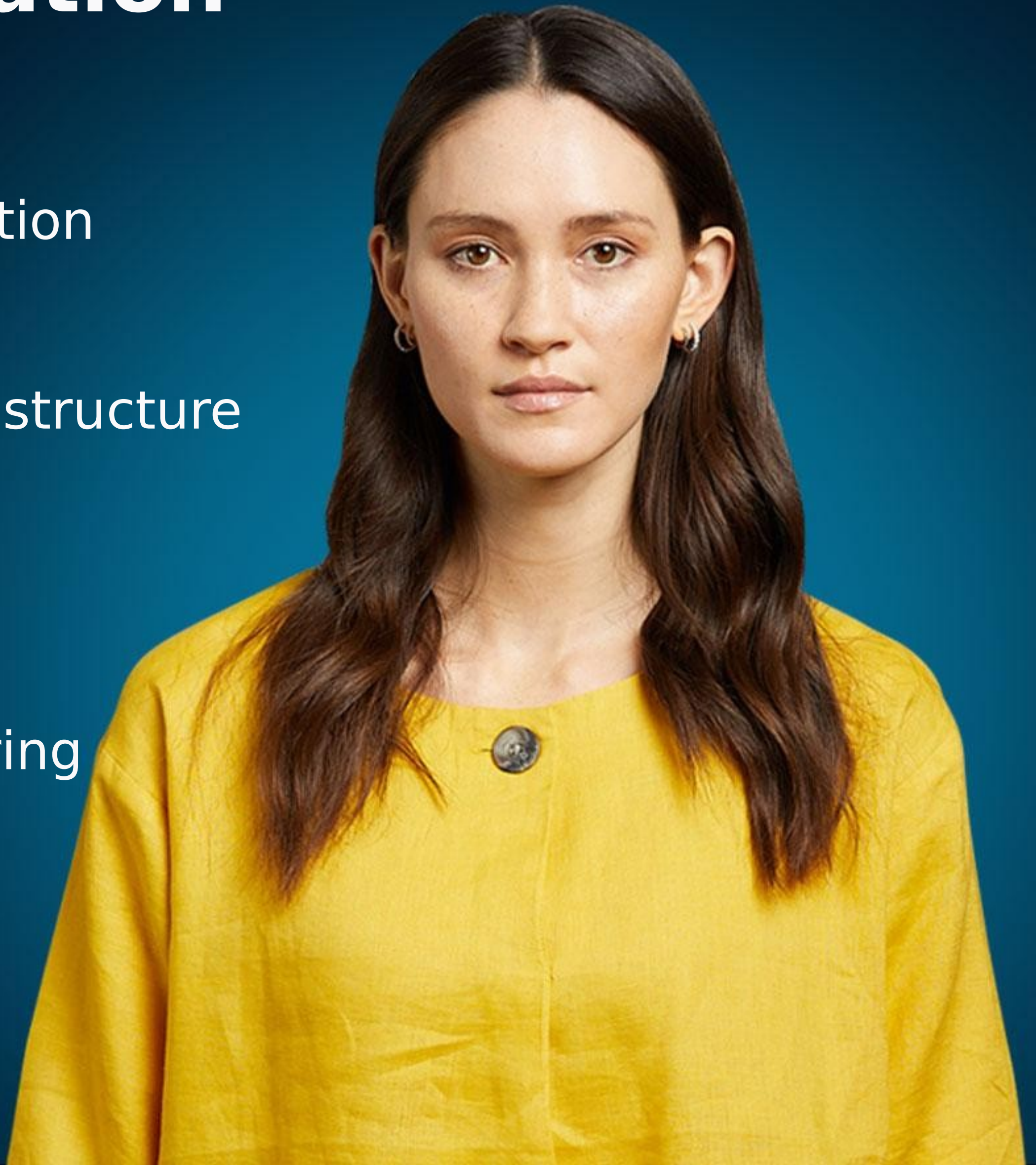
EU Justice System Challenges of Remote Identity Verification

Challenges

- Custom & Practice digital transformation
- Understanding National rules
- Member states architecture and infrastructure

Use Cases

- Secure evidence capture
- Secure cross-border intelligence sharing



© iProov 2023

EU Justice System Current Processes

Use Case: Attendee Court Participation

- Manual processes to verify an individual
- Low assurance in correct individual
- Operationally inefficient
- Privacy and confidentially concerns
- Vulnerable victim/witness drop out

© iProov 2023

Remote Face Biometric Verification Enables Secure Digital Presence within Video Conferencing

Use Case: Attendee Court Participation

- Remotely verify an individual
  - tied to government identity documents
  - face biometrics with liveness detection
- High assurance in correct individual
- Reduce manual processing
- Privacy and confidentially assured
- Prevents drop out of attendees

Remote Automated Biometrics Are Fundamental for Identity Creation and Assertion

Human

- Expensive, slow
- Inherently biased
- False accept rate >10%*
- 57% of people believe they can spot deepfakes, only 24% can do so successfully**
- Generative AI makes video identity verification obsolete

Automated

- Accurate, fast
- Bias mitigation
- Low False Accept and Reject rates
- Continuous improvement
- Needs people to teach the right lessons
- People to manage the learning, not decisions

Solution: Human Intelligence + Decision Automation = Active Threat Management

[*] **Source: Passport Officers' Errors in Face Matching**
David White ,Richard I. Kemp,Rob Jenkins,Michael Matheson,A. Mike Burton Published: August 18, 2014 https://doi.org/10.1371/journal.pone.0103510

[**] ***Idiap Research 2022***

Not All Face Biometrics Are Created Equal

Right Person?
FACE MATCHING

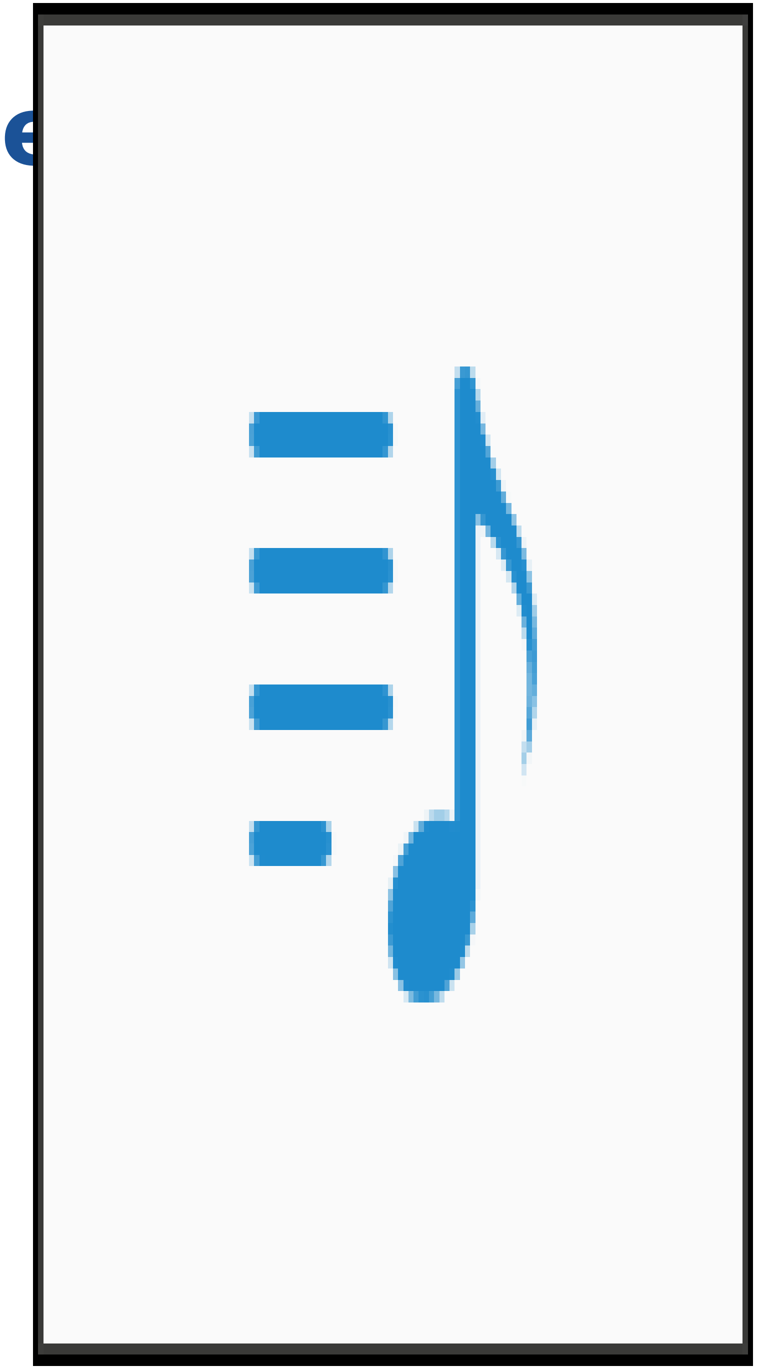
+

Real Person?
LIVENESS

+

Right Now?
REAL-TIME

Defences Against Generative

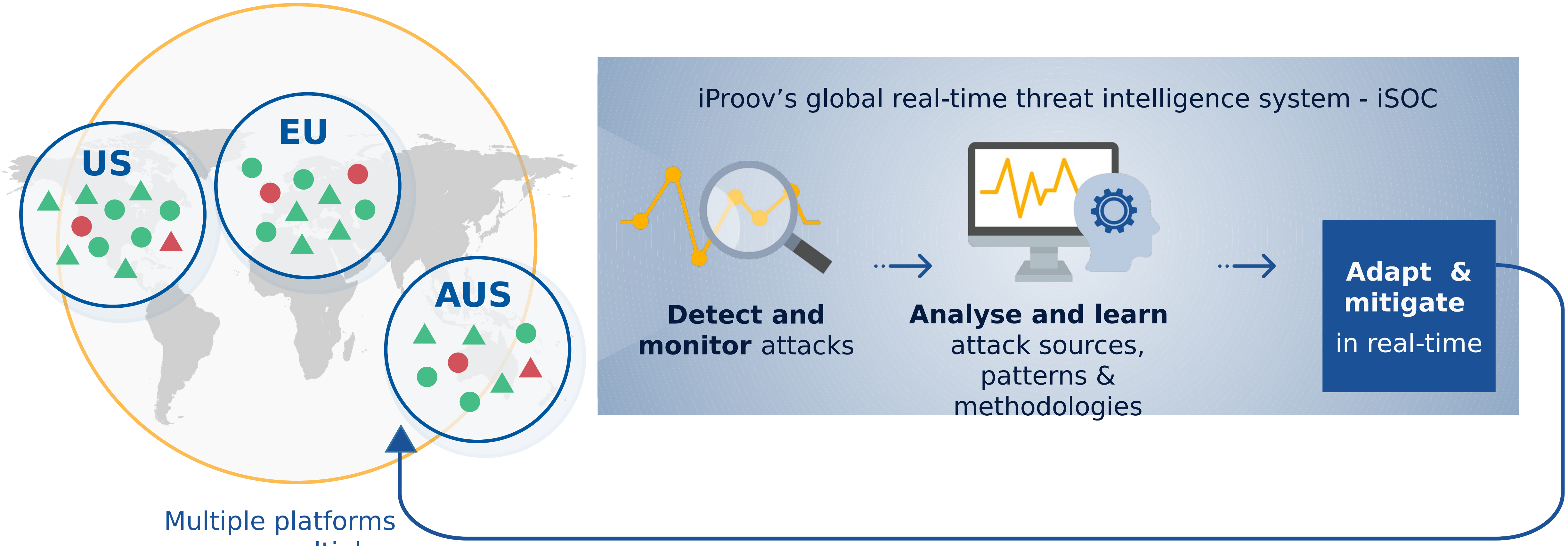


One-time biometrics with liveness detection

Defend against:

- Highly scalable digital injection attacks
- Synthetic media – such as Generative AI
- Reverse engineering

Active Biometric Threat Intelligence is Vital



iProov's global real-time threat intelligence system - iSOC

Detect and monitor attacks

Analyse and learn attack sources, patterns & methodologies

Adapt & mitigate in real-time

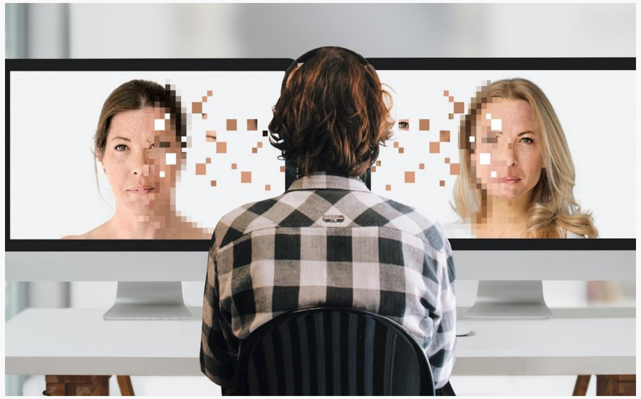
Multiple platforms across multiple geographies

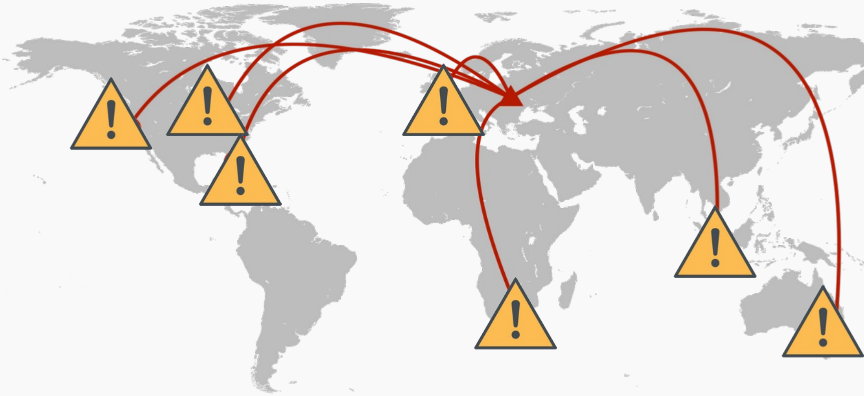
Key Threat Trends

1 Evolution of Digital Injection Attacks

2 Emergence of Novel Face Swap Attacks

3 Global, Indiscriminat Attacks at Scale





149% Increase ⬆

Injection attacks appearing as mobile web, android and iOS native H2 vs. H1 2022

295% Increase ⬆

H2 vs. H1 2022

100-200 within 24hrs

Simultaneously Launched Automated DIA Verification Attempts 3 X Per Week Worldwide

iProov Proven Global Deployments at Scale

Government Services

Government Digital Service

ID.me
For the IRS

Home Office

GOVTECH SINGAPORE

Australian Government
Australian Taxation Office

Borders & Travel

U.S. Department of Homeland Security

eurostar

Digital ID for Citizens

NHS

itsme

STATE OF CALIFORNIA DMV
Department of Motor Vehicles

Financial Services

UBS

bradesco

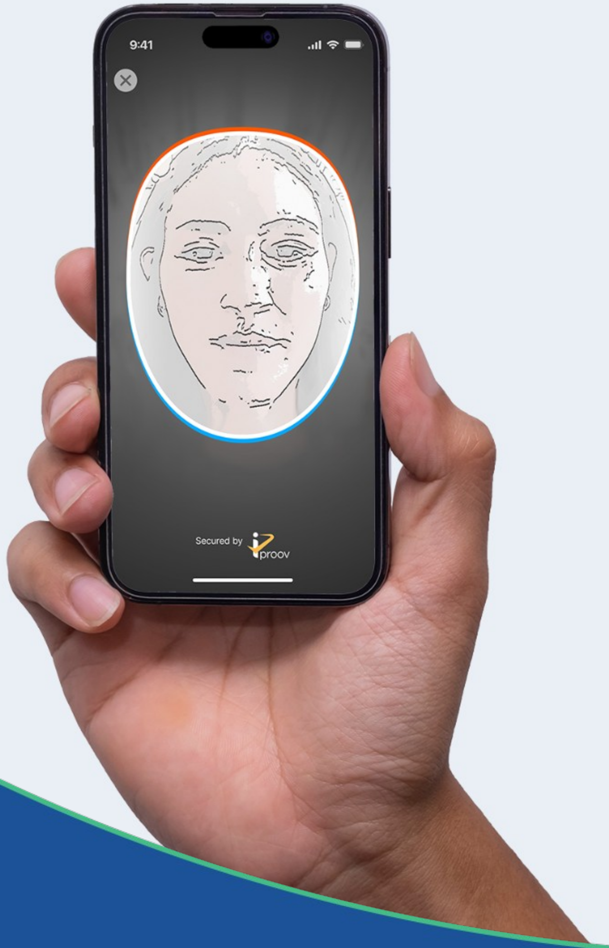
ING BANK

Standard Bank

absa

bank axept
Norway's national Bank ID

Thank you



Genuine Presence Assurance

Right person, Real person, Right now

Joe Palmer, Chief Product & Innovations Officer
contact@iproov.com

© iProov 2023