ICAO

TRIP 2022

SEAMLESS AND CONTACTLESS

Sharing data to accelerate the recovery

13 - 15 SEPTEMBER 2022

Bernhard Strobl

Novel Technologies for seamless Traveler Authentication

AIT – Austrian Institute of Technology

Content

Quick Intro

- New upcoming biometric possibilities
- Contactless capturing
- Compare flats vs. contactless
- How about accuracy ?
- Presentation Attack Detection (PAD)

The Holy Grail ?

- Privacy preserving checks
- Distributed ledgers
- Homomorphic Encryption

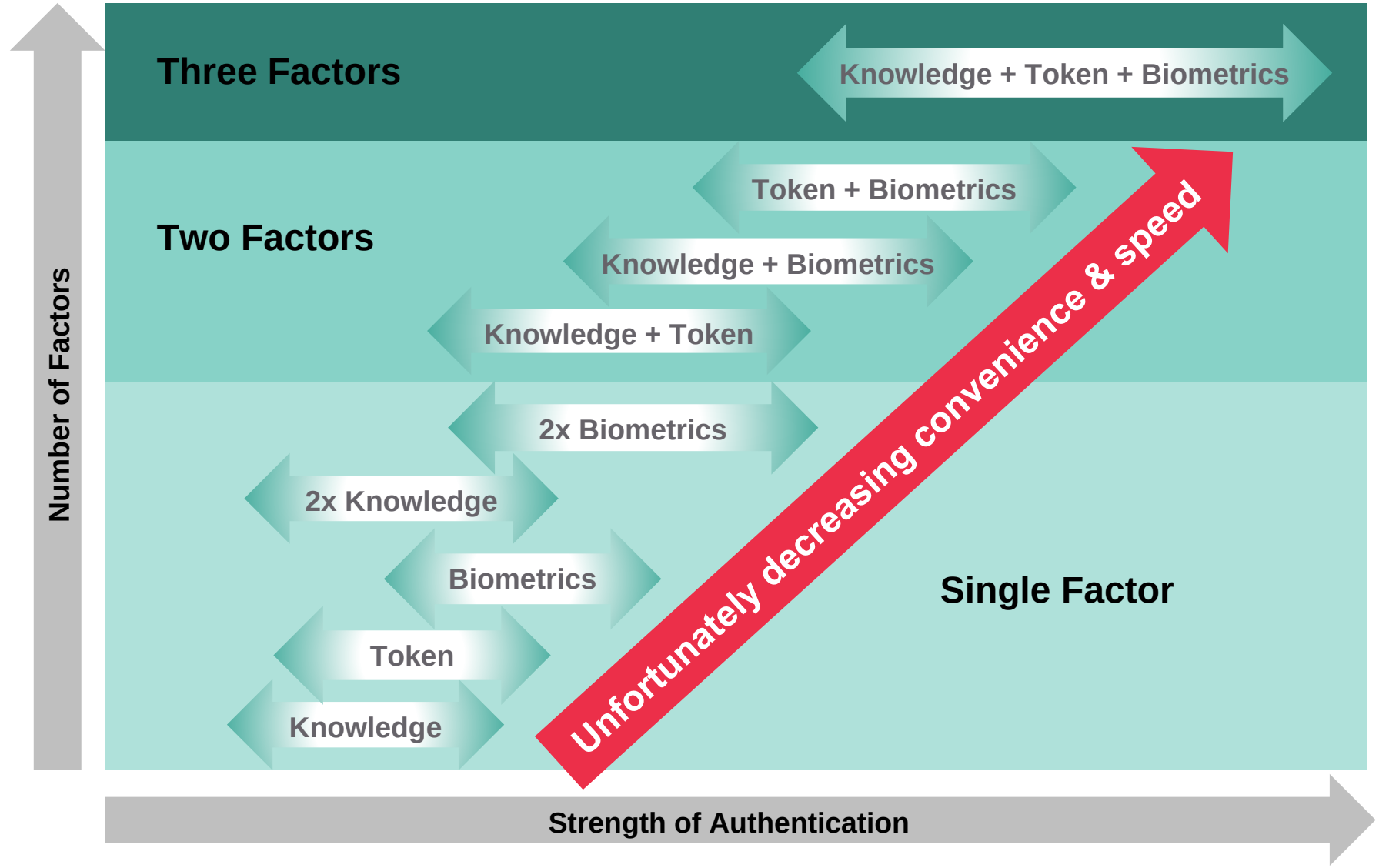
Border crossing is simple: Justification by several means

Are you the eligible holder of your document ?

3 Basic-Factors of Authentication

Knowledge (What you know)	**Hardware Token** (What you have)	**Biometrics** (What you are)
		
Password Passphrase PIN Pattern	Key USB Stick Smart Card QR-Code Passport	Face Fingerprint Iris Voice Signature Gait DNA

Convenience – Authentication Strength - Dilemma



Covenient, accurate, fast, secure, hygienic biometric data aquisition

- Iris – very good, acquisition more complicated, small industry
- Veins – only very few manufacturers, little is known about accuracy
- Voice – not really privacy preserving, not the best accuracy
- Gait - not practical in “wild environment”
- Ears – not so bad, but very unpractical
- Multifactor – yes, but takes time
- DNA …

- Face - tremendous progress, still morphing problem, liveness check
- Finger - very accurate, acquisition procedure lengthy, touch based

➢ Can we capture fingerprints faster, more hygienic ?

Covenient, accurate, fast, secure, hygienic biometric data aquisition

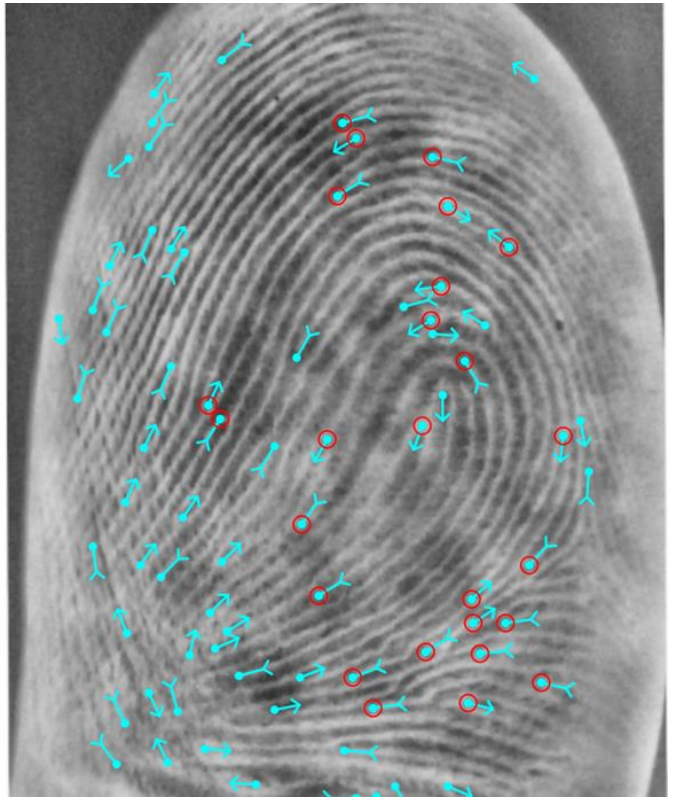
- ✓ Contactless
- ✓ 4 fingers
- ✓ No latent traces
- ✓ Hygienic
- ✓ Fast

Covenient, accurate, fast, secure, hygienic biometric data aquisition

- ✓ Contactless
- ✓ 4 fingers
- ✓ No latent traces
- ✓ Hygienic
- ✓ Fast

Flat - Contactless Comparison ?

Contact Sample



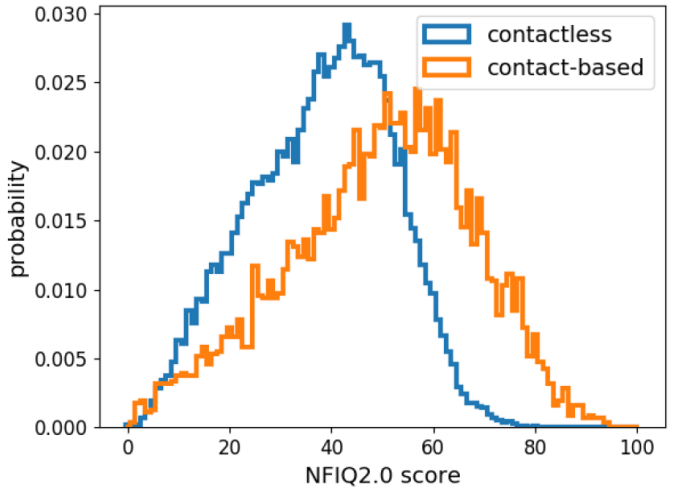
Contact-less Sample

Tests

- NIST (IR-8307) Interoperability Assessment shows very acceptable results for verification
- AIT test at the premises of the Austrian police comparing contact-less vs contact-based:

~600 pax, 50 samples = 300.000 fingerprints
good ethnic, gender and age distribution

- EER of 2.7×10^{-4}
- Ø capture time: <10s
- Ø NFIQ 2.2 score:
- 38.1 contact-less
- 49.4 contact-based



Ethnic group	Male	Female	Unknown
Africa	75	18	1
Asia	273	153	0
Europe	59	13	0
Central America	2	1	0
South America	4	3	0
Unknown	7	4	0
Total	420	192	1

Tab. 2: Gender distribution of the participants.

Age group	Male	Female	Unknown
< 20	49	24	1
[20, 30)	167	64	0
[30, 40)	119	59	0
[40, 50)	52	24	0
[50, 60)	25	15	0
> 60	8	6	0
Total	420	192	1

Tab. 3: Age distribution of the participants.

Utilisation

- Very few manufacturers worldwide
- No certification procedures available for very high-quality capturing (enrollment) (appendix F)
- Uncertainty of end-users

- Call to action:
  - Start worldwide efforts with new certification procedures
  - Ask authorities to have medium scale proof-of-concepts installations

Presentation Attack Detection

(Micro)-movements (+eyes)
Challenge response systems
3D capturing (hardware needed)
Infrared capturing (hardware needed)

Trained AI systems
Easy to avoid: live enrollment

Trained AI systems
Pore detection
Different wavelength responses
Optical Coherence Tomography
Difficult on smartphones

Presentation Attack Detection

Differentiate:

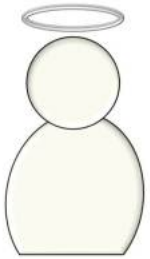
Attended by policeman/officer
smartphone fingerprint capture on the street

Un-attended (hardware provided)
Kiosk, e-Gate, Door-controller, luggage service, check-in

Un-attended (self-enrollment/registration):
Link fingerprint image to facial image (one-take)

Some Metrics:

NIST does a Face Recognition Vendor Test (FRVT):

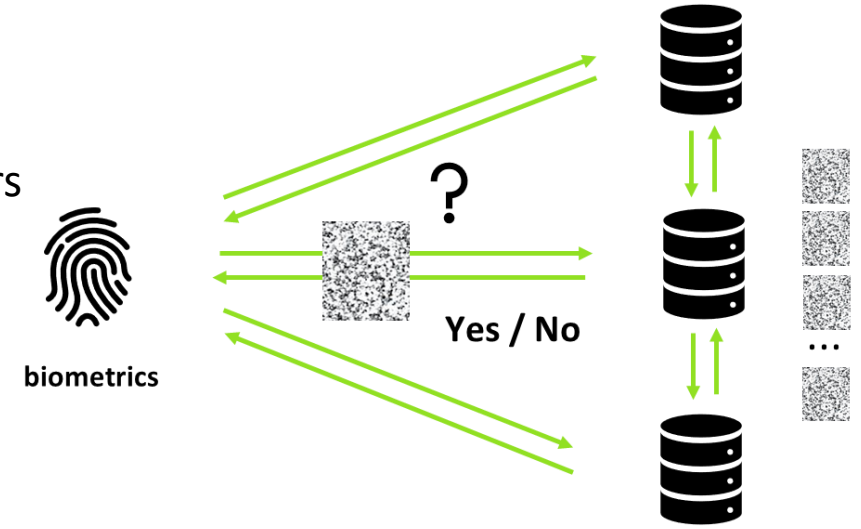


Bona Fide Presentation Classification Error Rate (BPCER)
The proportion of bona fide samples
incorrectly classified as presentation attack samples

Attack Presentation Classification Error Rate (APCER)
The proportion of presentation attack samples
incorrectly classified as bona fide presentation

The Holy Grail ?

- A distributed ledger system
  - builds trust by using several computational nodes/ledgers verifying a “transaction” located at different premises
- Secret sharing by MPC – Multi Party Computation
  - different players who jointly compute the output but no party learns anything about the input of other players
- Homomorphic encryption:
  - The server DOES NOT KNOW WHAT he is comparing
  - Original data is never revealed
- Touchless fingerprint capture
  - Convenient, hygienic, fast, accurate, secure



Thank You

ICAO