Benefits from Biometric Standards to the European Banking Ecosystem

Christoph Busch

copy of slides available at:
https://christoph-busch.de/about-talks-slides.html

latest news at:
https://twitter.com/busch_christoph

EAB, April 23, 2021

ATHENE

European Association for Biometrics
eab
Human Identity in Europe

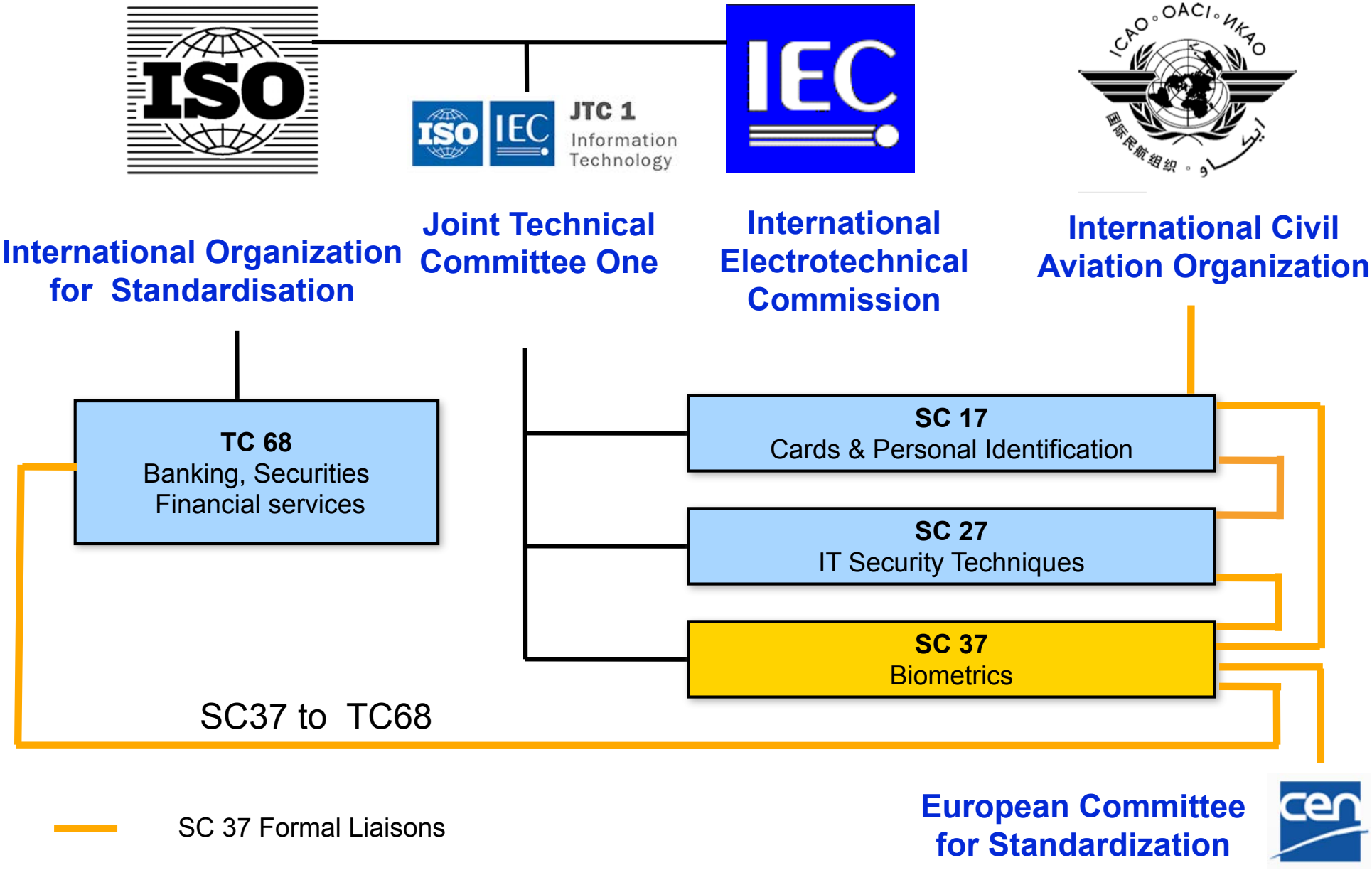
NTNU

Introduction to Standards

Biometric Standardisation

How does standardisation work?

Biometric Standardisation



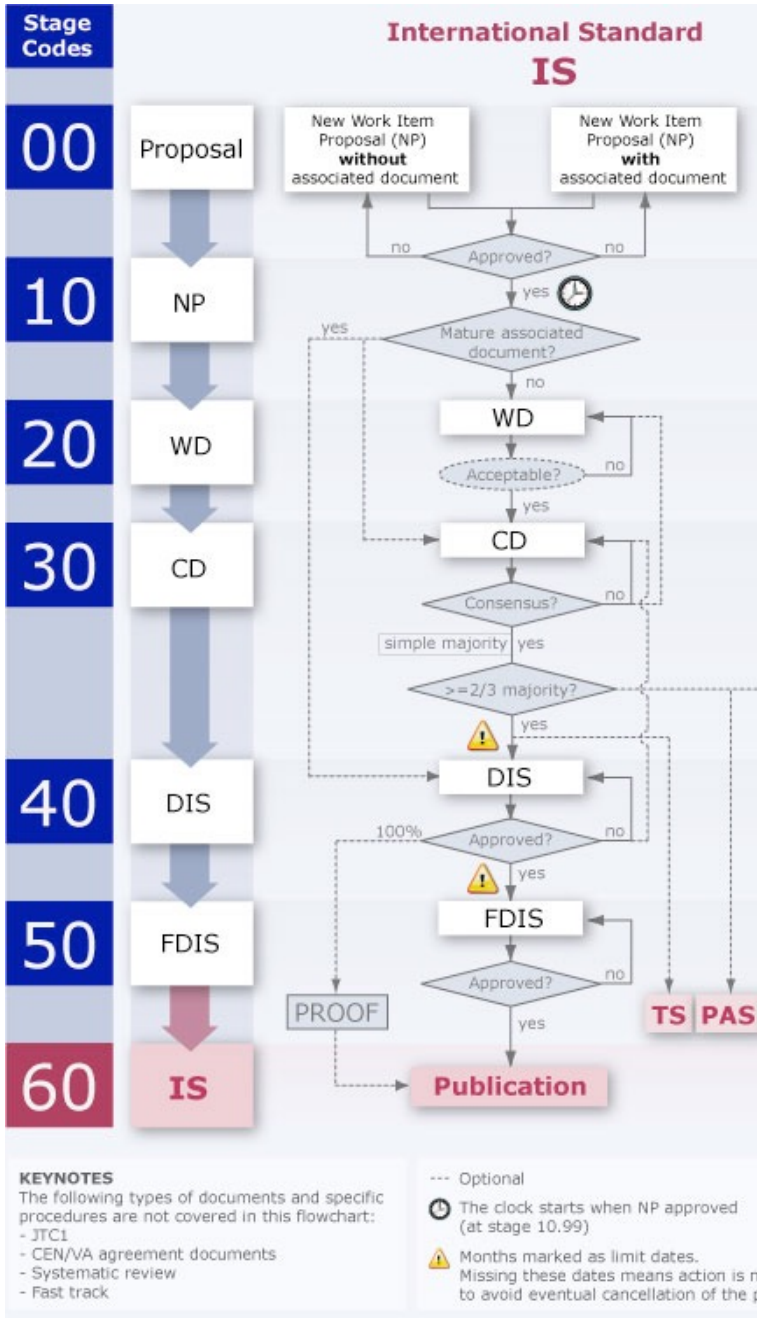
Levels of Development - Standards

Progression levels

- Working Draft (WD)
- Committee Draft (CD)
- Draft International Standard (DIS)
- Final Draft International Standard (FDIS)
- International Standard (IS)

Issues to consider:

- Need for mature technology
- Decisions are made on consensus
- Commenting periods
- Potentially multiple loops at one level
- Need to progress
- Five year revision cycle



Expressions in International Standards

In order to make clear what the user must do,

the following verbal forms are used in standards:

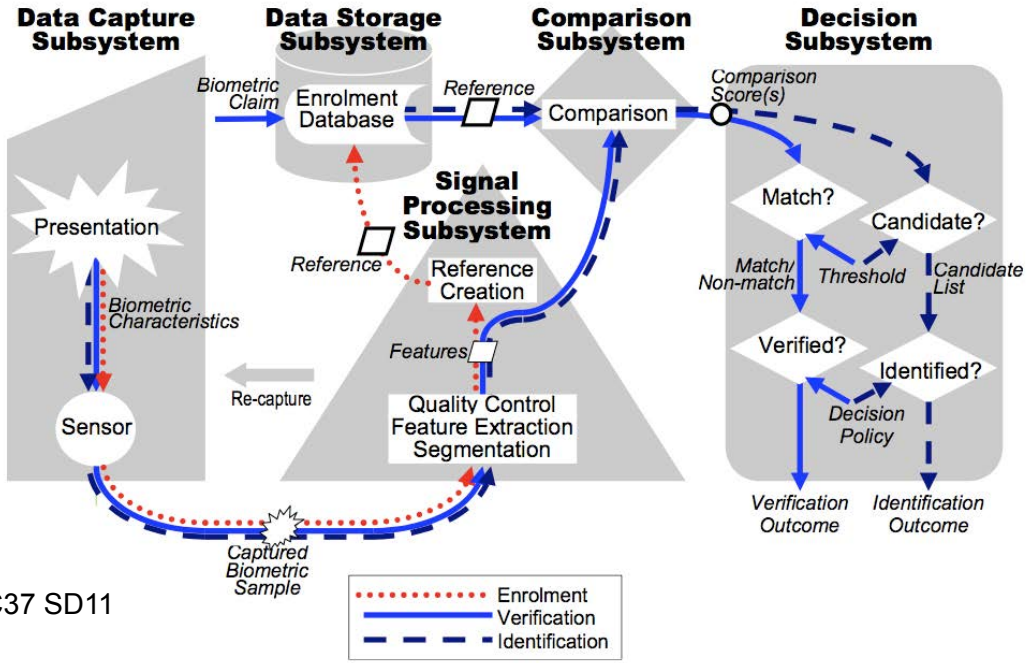
- Requirements – shall, shall not
- Recommendations – should, should not
- Permission – may, need not
- Possibility and capability – can, cannot

Biometric Application Programming Interface

Application Programming Interface - API

Biometric systems maintenance requires

- flexibility (plug-in of components)
- avoiding vendor lock-in,
  - rather allow transparency and exchangeability
- supports scalability and expandable platform
- upgrade partial components (sensors, algorithms) with little/no impact on the entire system



Source: ISO/IEC JTC1 SC37 SD11

Application Programming Interface - API

BioAPI (Biometric API)

- supports biometric enrolment and recognition
- defines interfaces between subsystems that enables software or sensors from multiple vendors to be integrated
- communication between (sub-) systems using the Biometric Interworking Protocol (BIP)
- support for applications, which observe multiple biometric characteristics (for example fingerprint, iris, and face)

ISO/IEC 19784-1: BioAPI specification, 2006

- Framework architecture and interfaces
- High-level C programming language specifications
- currently in revision process

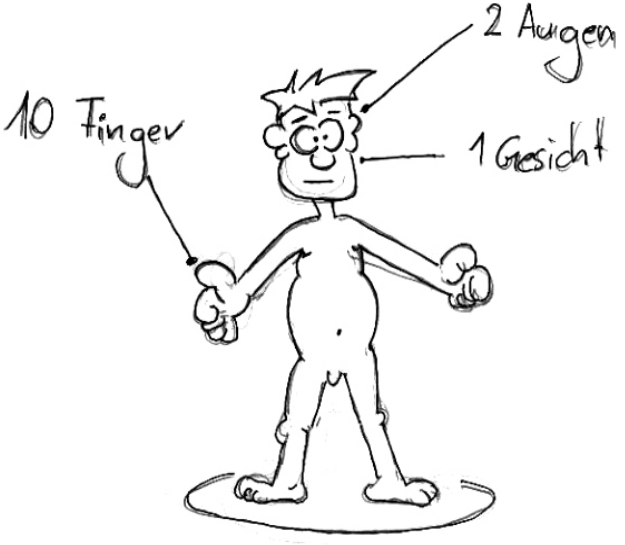
- also standards for embedded BioAPI and object oriented BioAPI (Java, C#)

Common Concerns

Revocability ?

Data subjects may think:

„*The number of biometric characteristics is limited (e.g. we have only 10 fingers) - we can not revoke the biometric reference*“



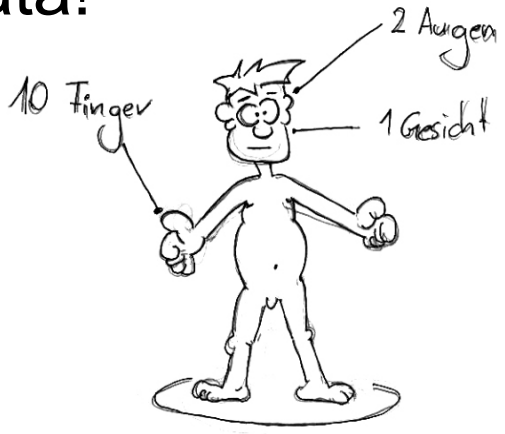
Data Privacy and Data Protection ?

Operators may think:

„Biometric systems are not compliant to data privacy principles“

Biometric Template Protection

We need to protect biometric reference data!
but …



- how to revoke biometric references?

- how to protect sensitive information in biometric data?
  - and align with the General Data Protection Regulation (GDPR)

Wart Fingerprint

Source: TU Brno, 2013

Biometric Template Protection

We do NOT store fingerprint, iris or face images

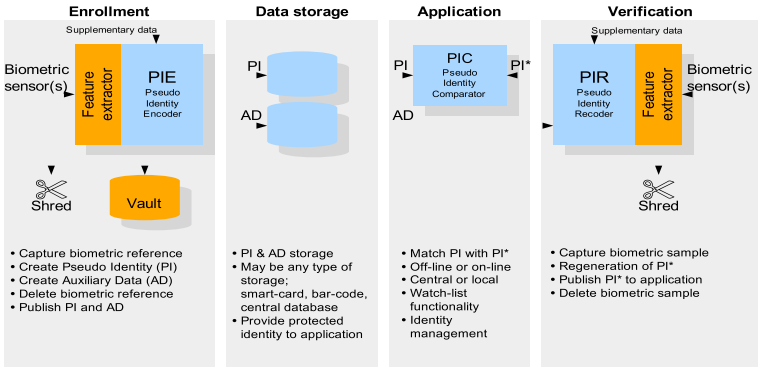
- we transform templates to pseudonymous identifiers (PI)
- we reach
  - Secrecy: biometric references (PI) can be compared without decryption.
  - Unlinkability: Unique pseudonymous identifier can be created for each application to prevent database cross-comparison
  - Renewability: we can revoke and renew template data.
  - Non-invertibility:Original biometric sample can not be reconstructed

- [Br2008] J. Breebaart, C. Busch, J. Grave, E. Kindt: "A Reference Architecture for Biometric Template Protection based on Pseudo Identities", in BIOSIG-2008, GI-LNI, (2008) http://www.christoph-busch.de/files/Breebaart-BTPReferenceArchitecture-BIOSIG-2008.pdf
- [RaBBB2013] C. Rathgeb, F. Breitinger, C. Busch, H. Baier: "On the Application of Bloom Filters to Iris Biometrics", in IET Journal on Biometrics 3(1), (2014) http://www.christoph-busch.de/files/Rathgeb-BloomFilter-IET-2014.pdf

Data Protection Requirements

A technical guideline, how to implement requirements for data privacy and data protection is formulated in:

- ISO/IEC 24745: Biometric Information Protection
  https://www.iso.org/standard/52946.html



ISO/IEC 24745
Biometric Information Protection !

Standards ?

Operators may think:

„There are no standards to evaluate biometric technology“

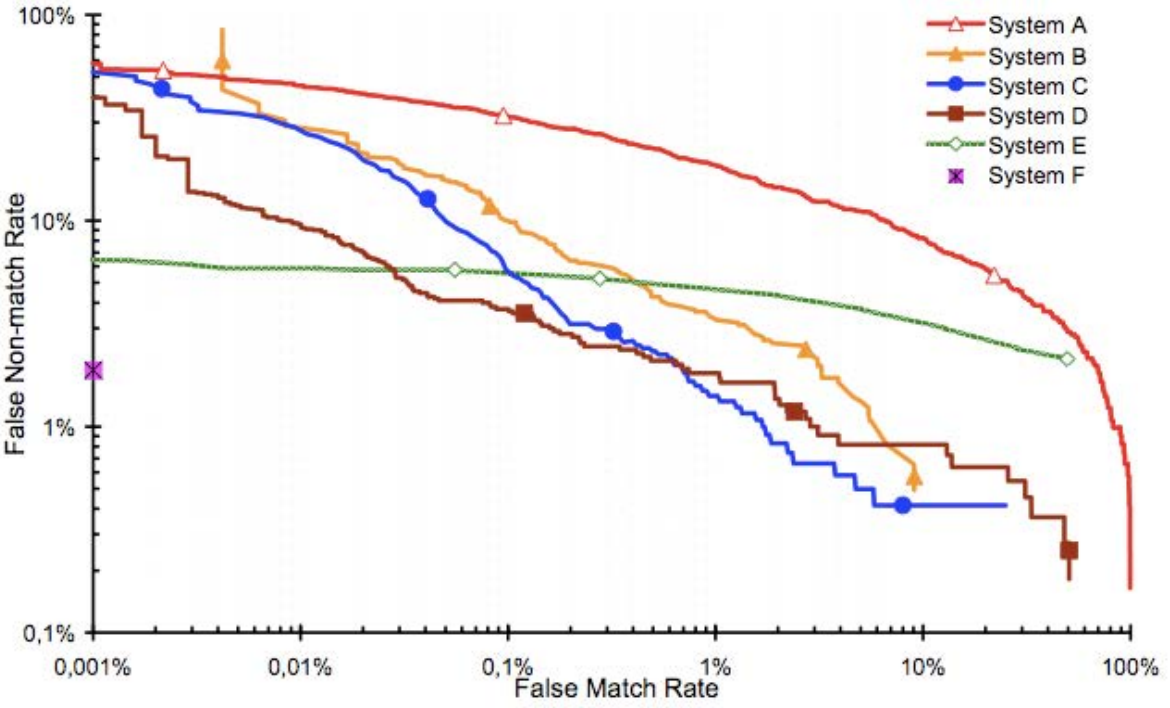
Biometric Performance Testing Standard

- ISO/IEC 19795-x, Information technology - Biometric performance testing and reporting
  - Part 1: Principles & Framework (revision to be published in 2021)
    - Guidance applicable to the broad range of tests
  - Part 2: Testing Methodologies for Technology and Scenario Evaluation
  - Part 3: Modality-Specific Testing
  - Part 4: Interoperability Performance Testing
  - Part 5: Framework for biometric device performance evaluation for access control
  - Part 6: Testing methodologies for operational evaluation
  - Part 7: Testing of on-card biometric comparison algorithms
  - Part 9: Testing on mobile devices
  - Part 10: Quantifying biometric system performance variation across demographic groups (under development)

Biometric Performance Testing - Report

DET curve (detection error trade-off curve)

- which plots error rates on both axes (false positives on the x-axis and false negatives on the y-axis)



Extensive test results:
https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

Standards ?

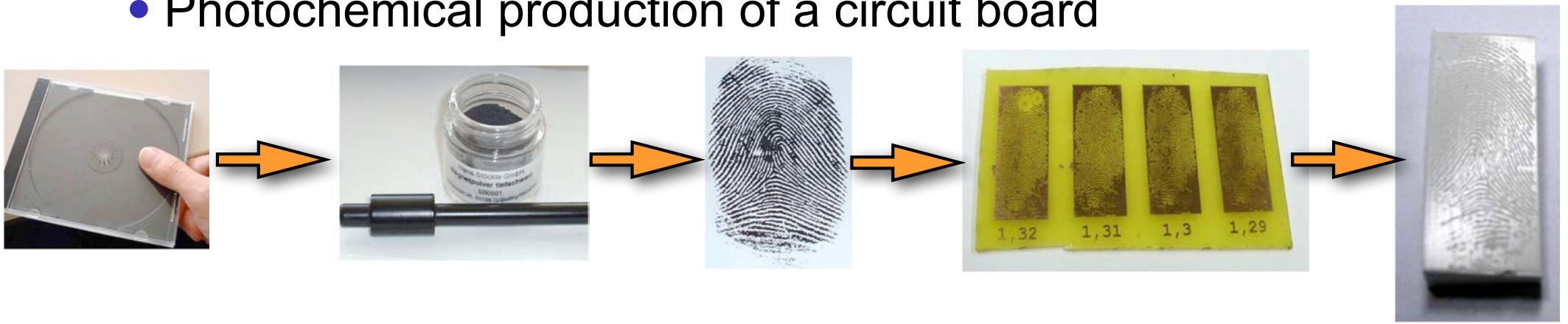
Operators may think:

„*The sensors can be fooled*“

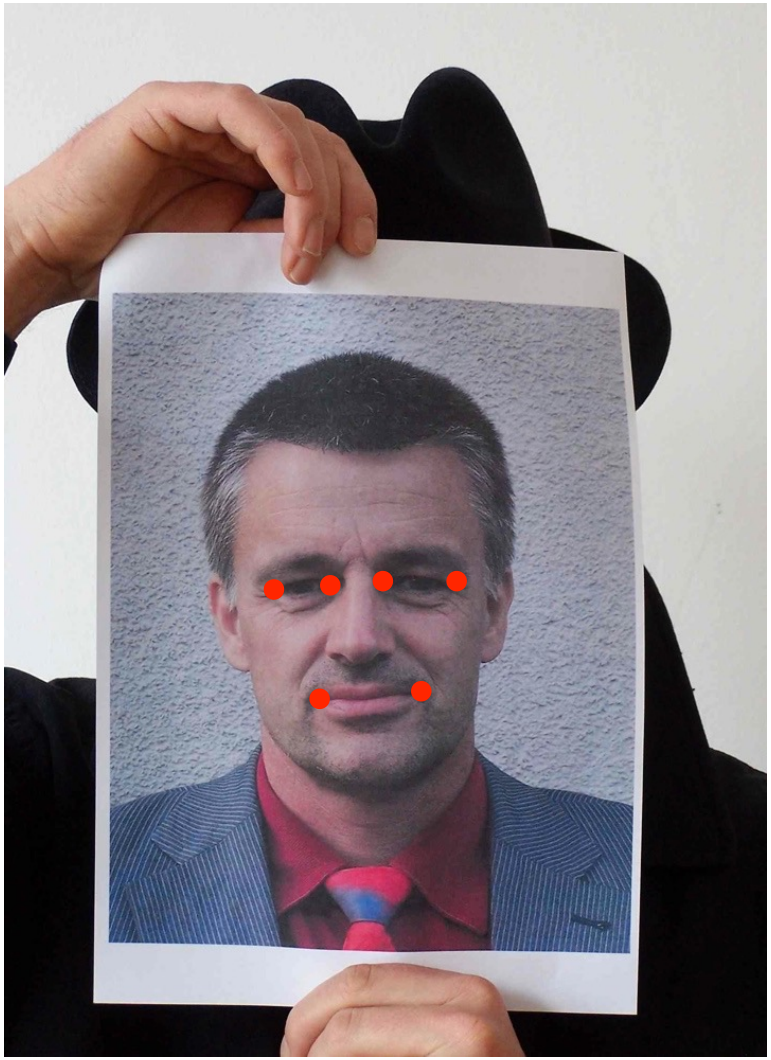
Security Fingerprint Sensor - Attack 2

Attack without support of an enrolled individual

- Recording of an analog fingerprint from flat surface material
  - z.B. glass, CD-cover, etc.
    with iron powder and tape
- Scanning and post processing:
  - Correction of scanning errors
  - Closing of ridge lines (as needed)
  - Image inversion
- Print on transparent slide
- Photochemical production of a circuit board



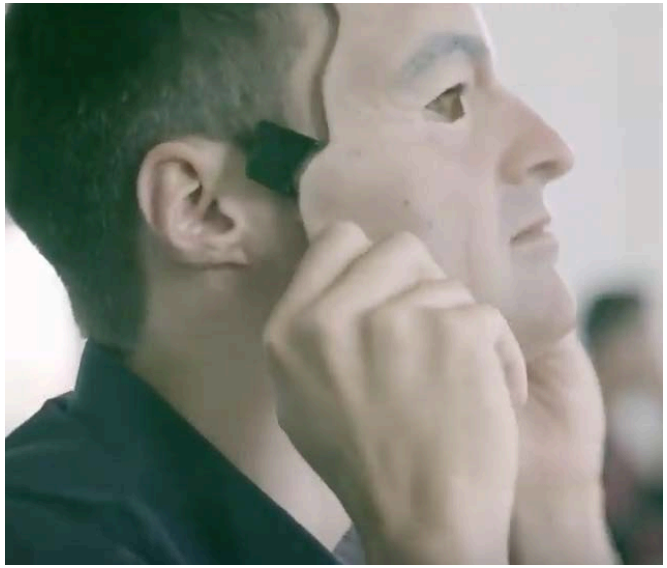
Face Presentation Attacks



Impostor Presentation Attack

3D silicone mask

- Targeted attack with 3D silicone custom mask
- Cost more than 3000 USD

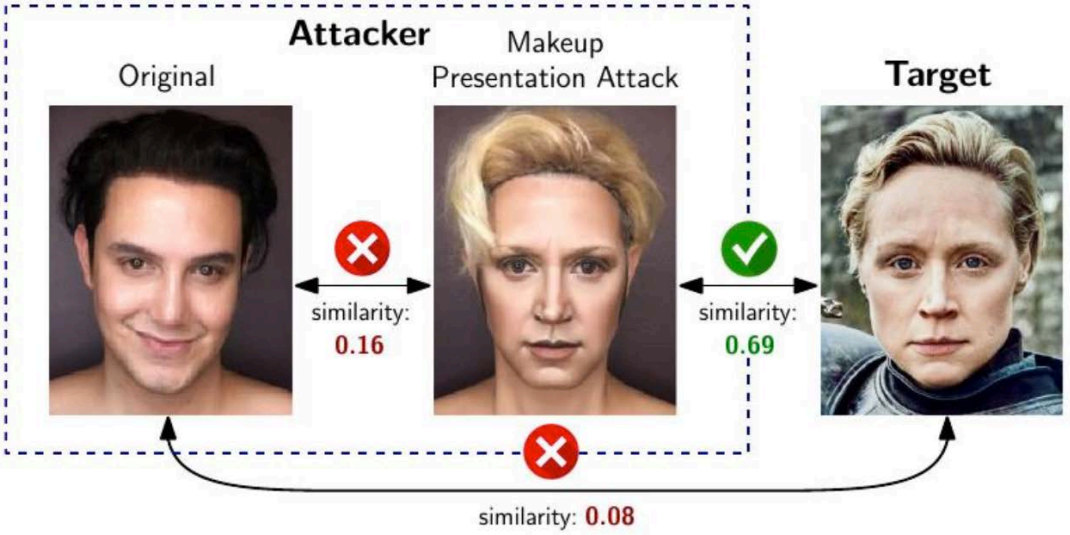


Makeup Presentation Attacks

Severe alterations

- Makeup for impersonation
- Liveness detection is not sufficient
- Detection difficult since bona fide users may also apply

(a) Before (b) After (c) Target



[RDB2020] C. Rathgeb, P. Drozdowski, C. Busch: "Detection of Makeup Presentation Attacks based on Deep Face Representations“, in Proceedings of 25th International Conference on Pattern Recognition (ICPR), (2020)

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- Testing the PAD subsystem with false-negative and false-positive errors:

- **Attack presentation classification error rate (APCER)**
  proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario

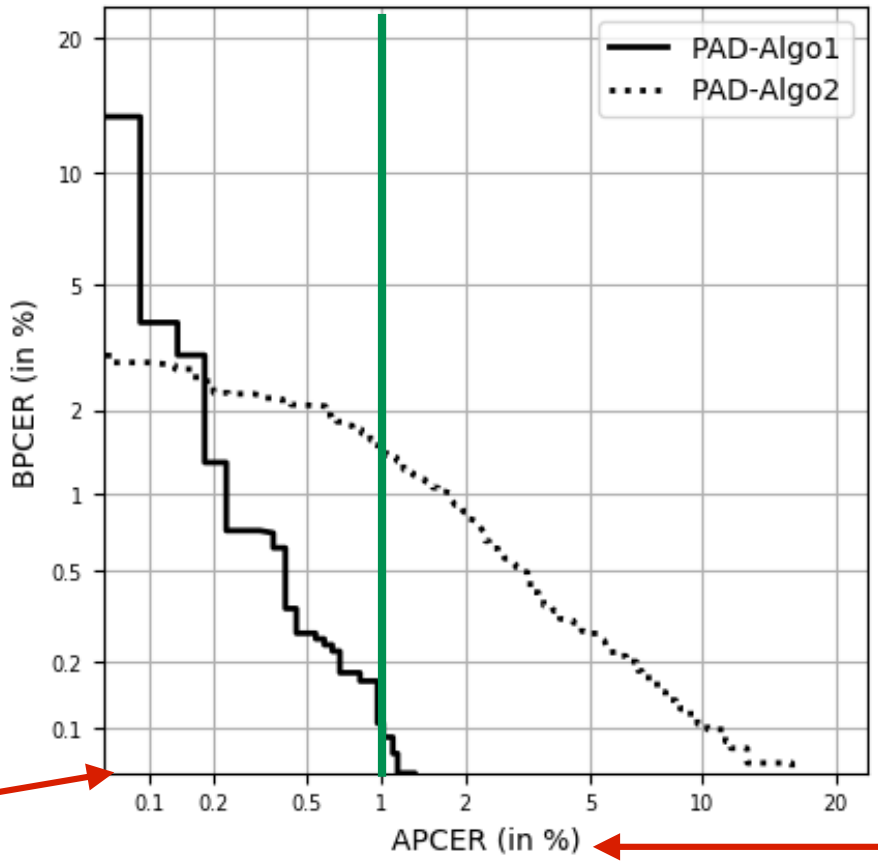
- **Bona fide presentation classification error rate (BPCER)**
  proportion of bona fide presentations incorrectly classified as attack presentations in a specific scenario

Source: ISO/IEC 30107-3

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- DET curve reports operating points for various thresholds showing security measures versus convenience measures
- Example:



convenience measure

Ideal:
APCER - low
BPCER - low

security measure (strength of function)

Your Operator Reality Check

Operators should ask the vendors

- Is the sensor replaceable and robust for presentation attacks?

I want the biometric capture device to be operated via BioAPI interface according ISO/IEC 19784 and tested for PAD according ISO/IEC 30107-3

- Is the accuracy of the algorithm good?

I want to see the technology performance test report with a DET curve according ISO/IEC 19795!

- Is there data protection of stored biometric reference data?

I want the design of the systems to be compliant to ISO/IEC 24745

Smartphone Access Control

Foreground authentication (user interaction)

- Deliberate decision to capture (willful act)
- Camera-Sensor
  - Fingerprint recognition
    - Apples iPhone 5S / Samsung Galaxy 5
    - Fingerphoto analysis
  - Face recognition
  - Iris recognition
- Touchpad: allows signature recognition

Image Source: Apple 2013

Background authentication (observation of the user)

- Microphone
  - Speaker recognition
- Accelerometer
  - Gait recognition
  - concurrent - unobtrusive

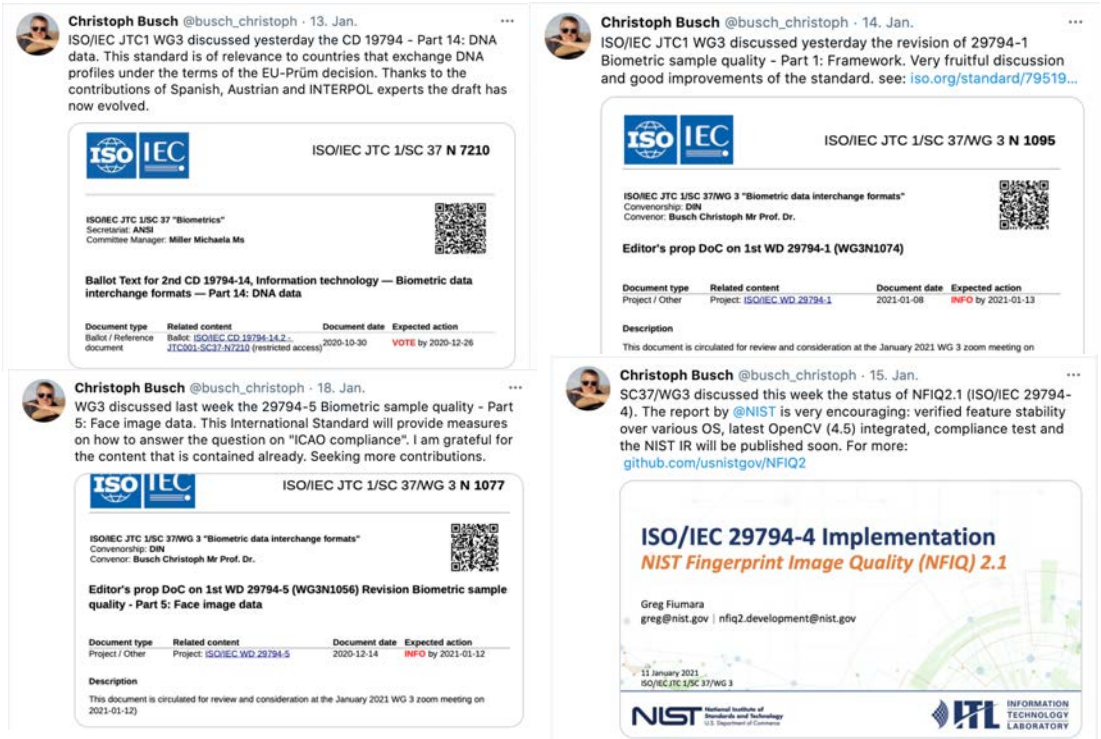
Follow Standards

Register with your national body

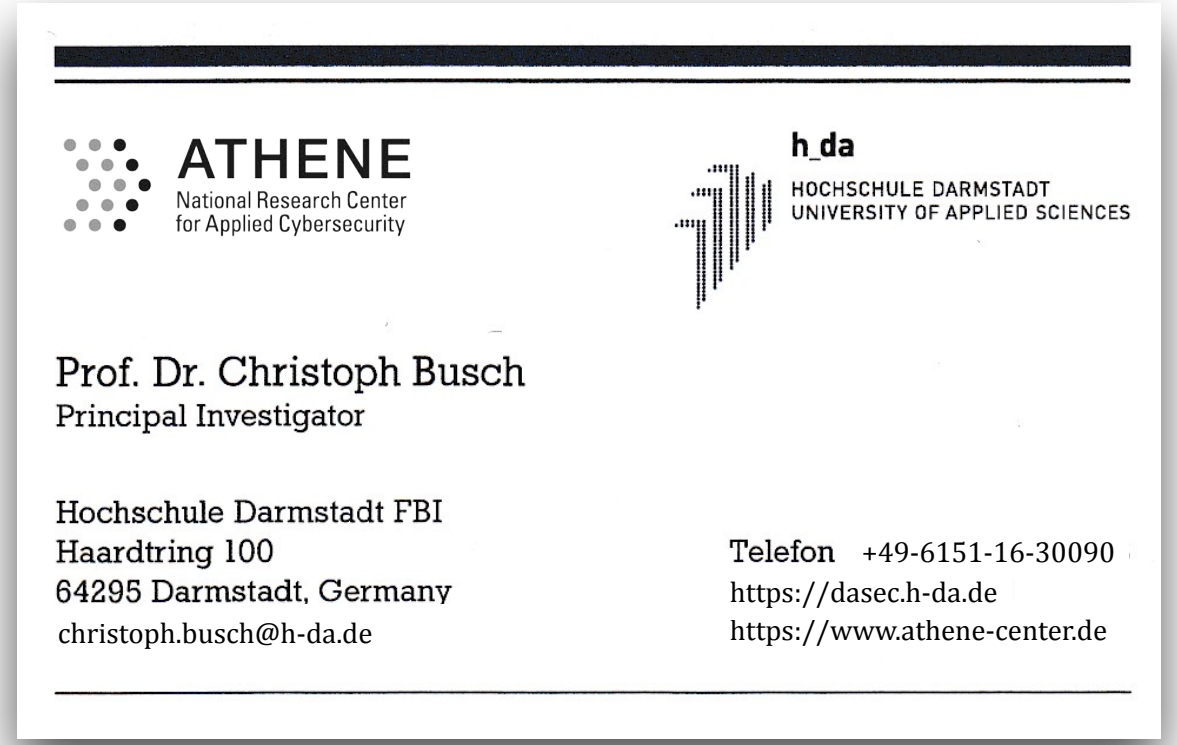
- Any organization can participate in the development of a standard https://www.iso.org/members.html

Follow the news on standards

- https://twitter.com/busch_christoph



Contact


ATHENE
National Research Center
for Applied Cybersecurity
h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
Prof. Dr. Christoph Busch
Principal Investigator
Hochschule Darmstadt FBI
Haardtring 100
64295 Darmstadt, Germany
christoph.busch@h-da.de
Telefon +49-6151-16-30090
https://dasec.h-da.de
https://www.athene-center.de

Contact

Contact:

NTNU

Prof. Dr. Christoph Busch

Norwegian University of Science and Technology
Department of Information Security and Communication Technology
Teknologiveien 22
2802 Gjøvik, Norway
Email: christoph.busch@ntnu.no
Phone: +47-611-35-194