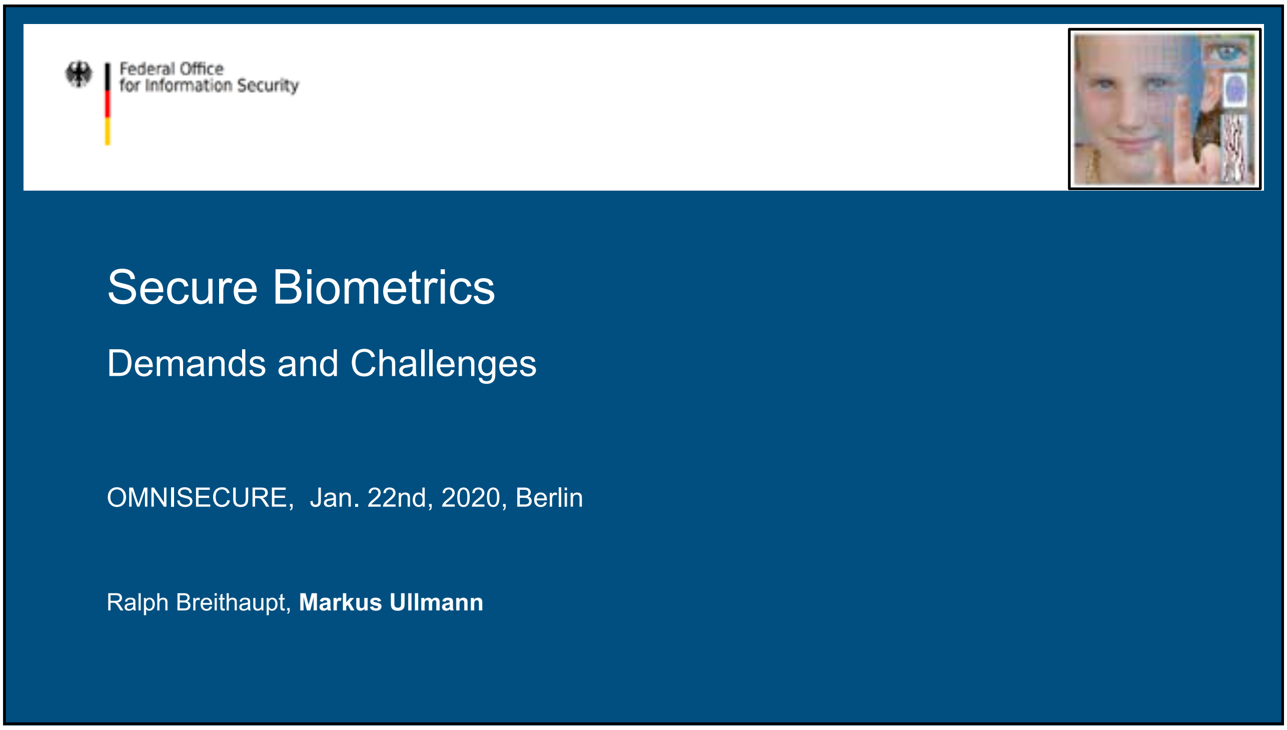


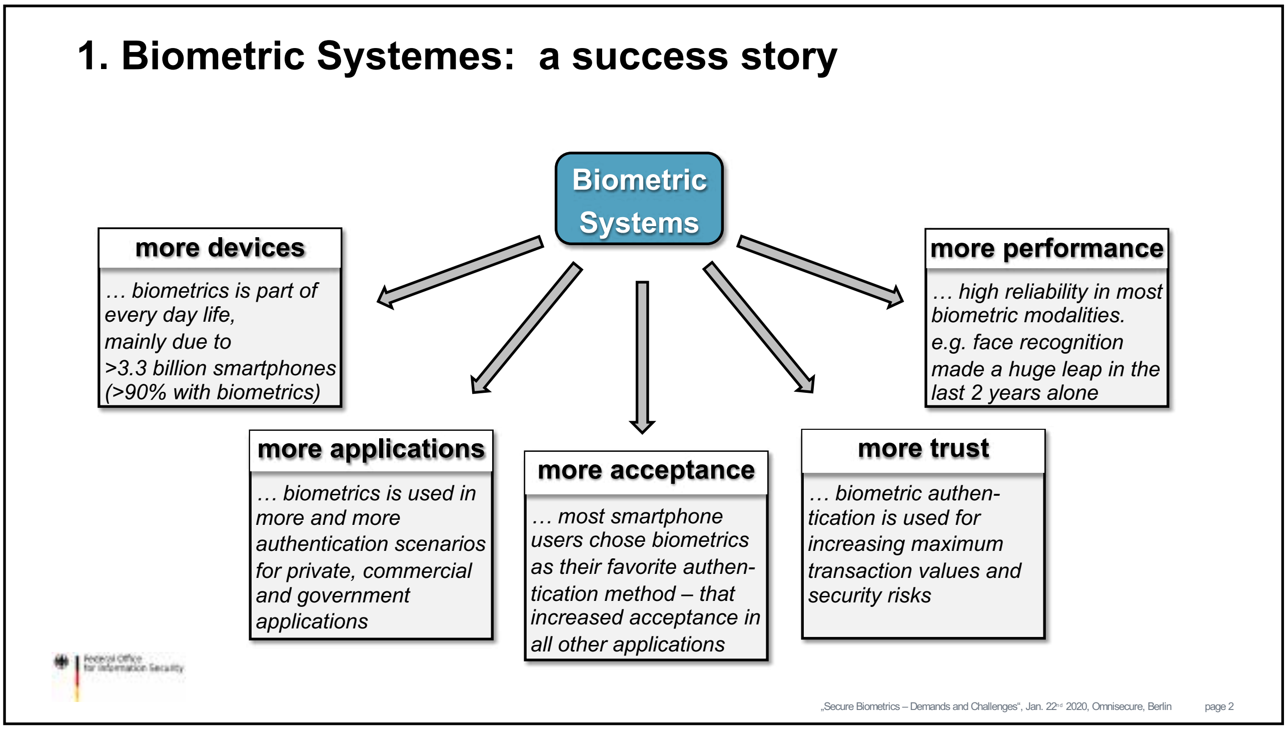
Federal Office for Information Security

Secure Biometrics

Demands and Challenges

OMNISECURE, Jan. 22nd, 2020, Berlin

Ralph Breithaupt, **Markus Ullmann**



1. Biometric Systemes: a success story

Biometric Systems

more devices

… biometrics is part of every day life, mainly due to >3.3 billion smartphones (>90% with biometrics)

more performance

… high reliability in most biometric modalities. e.g. face recognition made a huge leap in the last 2 years alone

more applications

… biometrics is used in more and more authentication scenarios for private, commercial and government applications

more acceptance

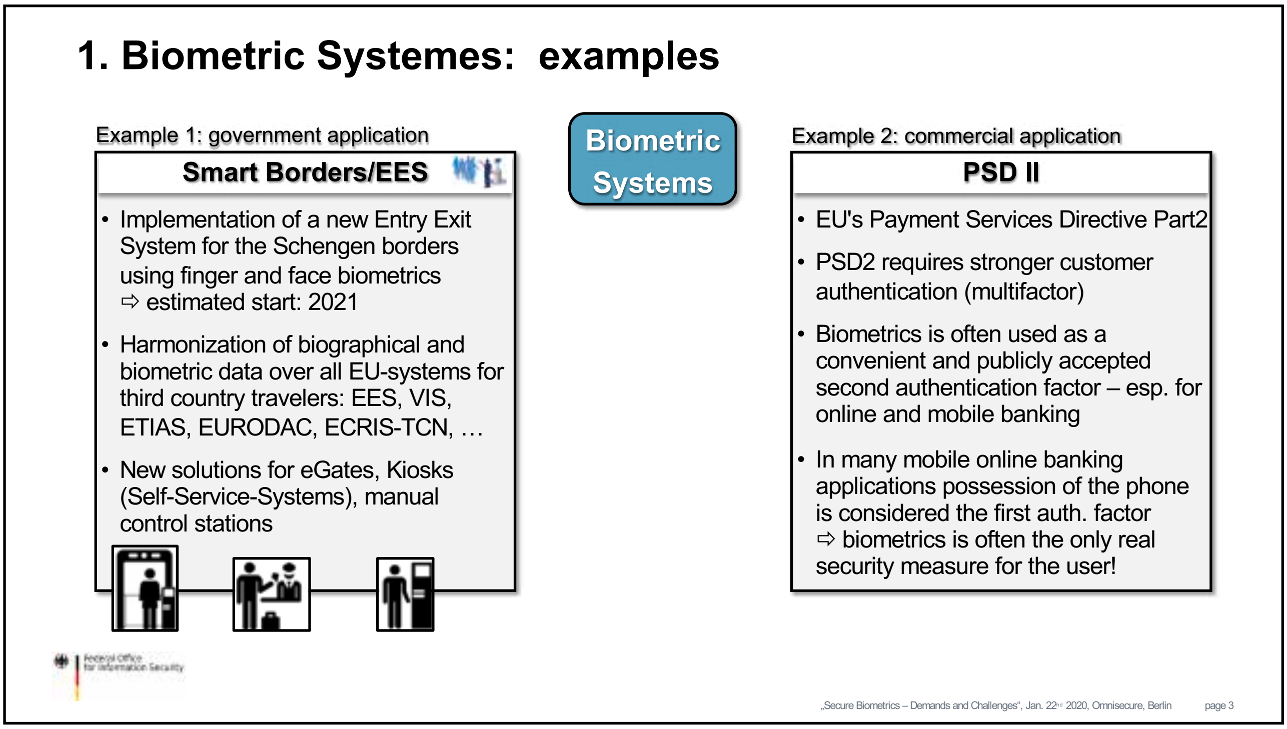
… most smartphone users chose biometrics as their favorite authentication method – that increased acceptance in all other applications

more trust

… biometric authentication is used for increasing maximum transaction values and security risks

Federal Office for Information Security

„Secure Biometrics – Demands and Challenges", Jan. 22nd 2020, Omnisecure, Berlin   page 2



1. Biometric Systemes: examples

Biometric Systems

Example 1: government application

Smart Borders/EES

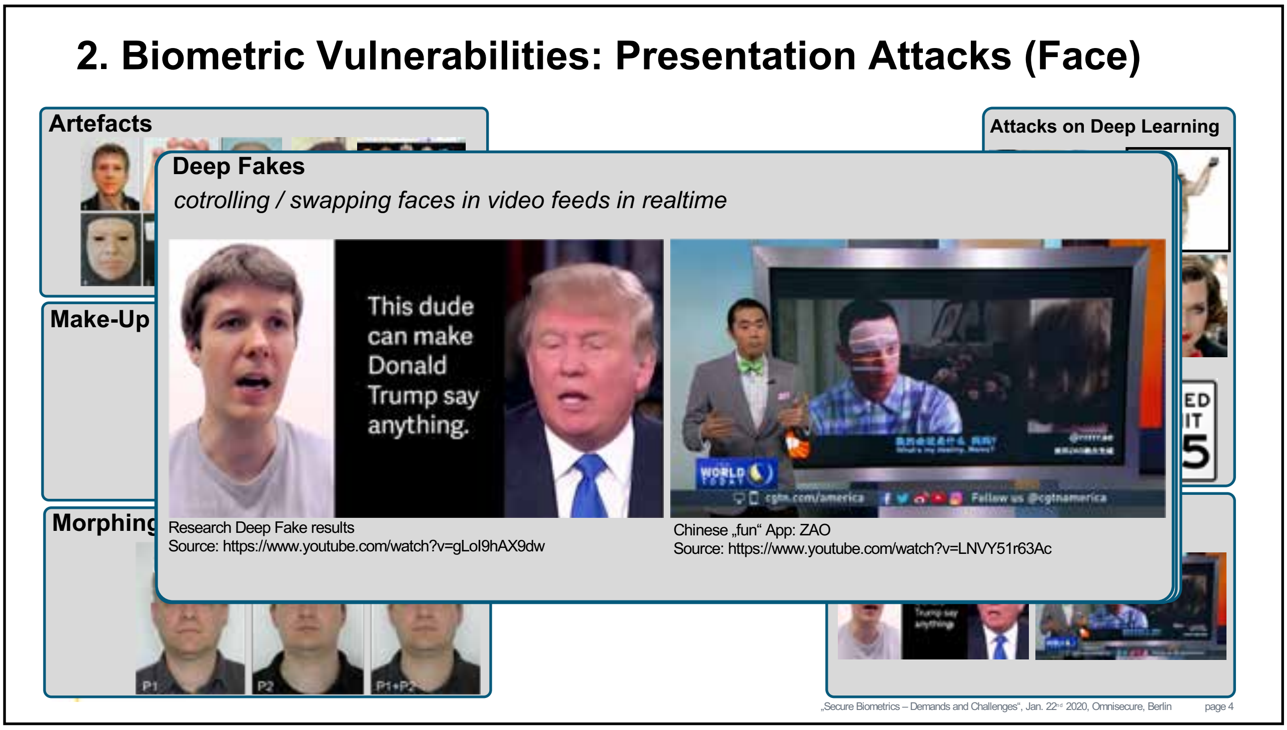
- Implementation of a new Entry Exit System for the Schengen borders using finger and face biometrics ⇨ estimated start: 2021
- Harmonization of biographical and biometric data over all EU-systems for third country travelers: EES, VIS, ETIAS, EURODAC, ECRIS-TCN, …
- New solutions for eGates, Kiosks (Self-Service-Systems), manual control stations

Example 2: commercial application

PSD II

- EU's Payment Services Directive Part2
- PSD2 requires stronger customer authentication (multifactor)
- Biometrics is often used as a convenient and publicly accepted second authentication factor – esp. for online and mobile banking
- In many mobile online banking applications possession of the phone is considered the first auth. factor ⇨ biometrics is often the only real security measure for the user!

Federal Office for Information Security



2. Biometric Vulnerabilities: Presentation Attacks (Face)

Artefacts

Make-Up

Morphing

P1
P2
P1+P2

Attacks on Deep Learning

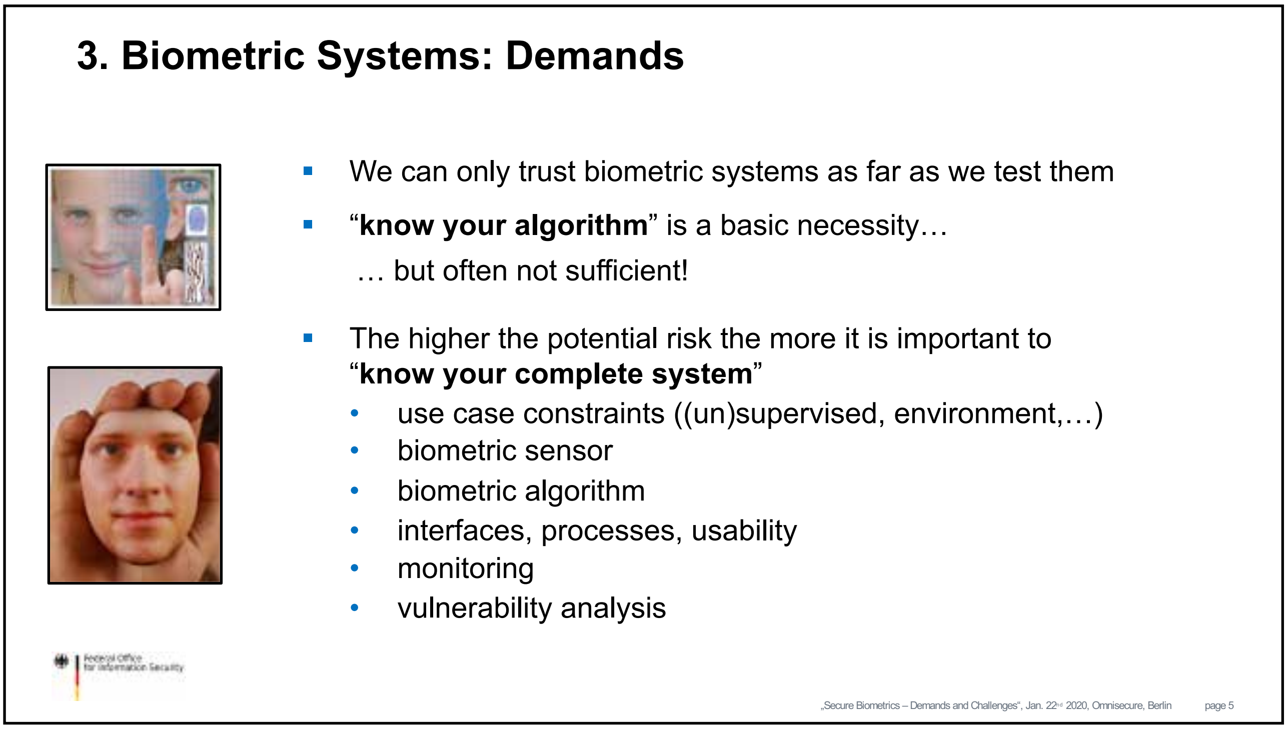
Deep Fakes

cotrolling / swapping faces in video feeds in realtime

This dude can make Donald Trump say anything.
WORLD TODAY
cgtn.com/america
Follow us @cgtnamerica

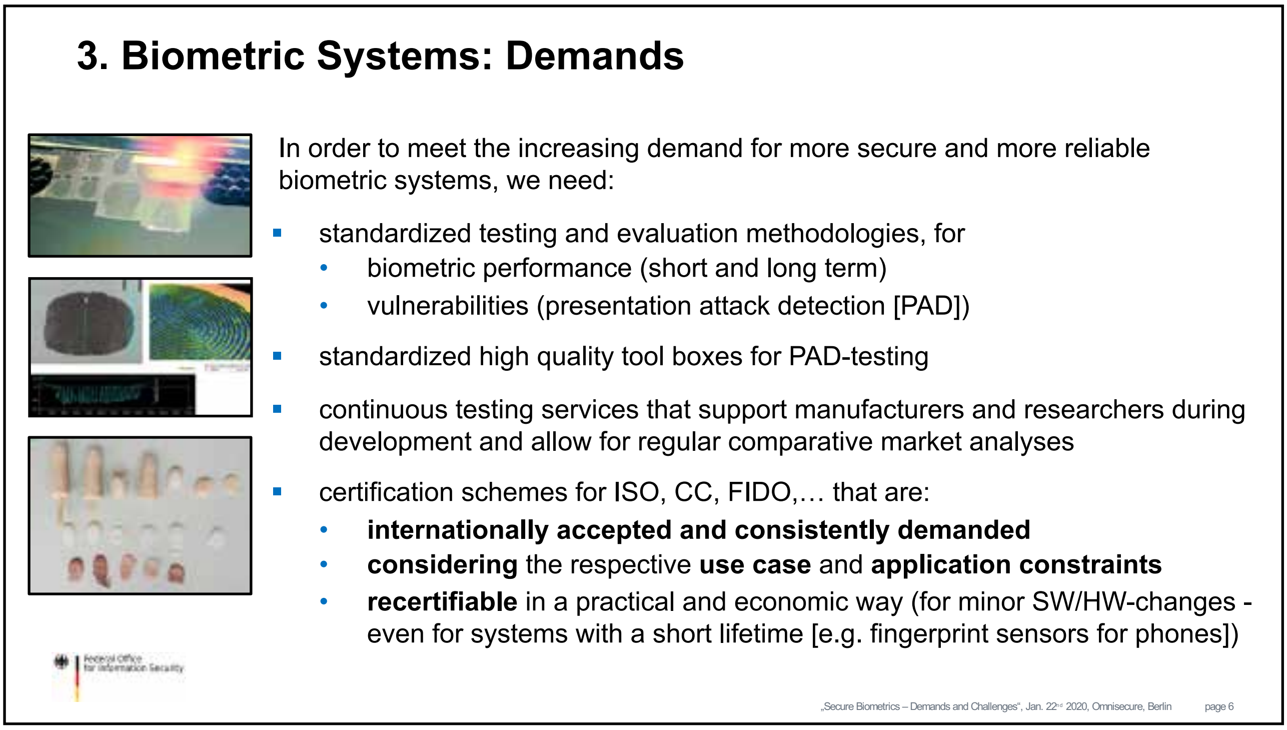
Research Deep Fake results
Source: https://www.youtube.com/watch?v=gLoI9hAX9dw

Chinese „fun" App: ZAO
Source: https://www.youtube.com/watch?v=LNVY51r63Ac



3. Biometric Systems: Demands

- We can only trust biometric systems as far as we test them
- “**know your algorithm**” is a basic necessity…
  … but often not sufficient!
- The higher the potential risk the more it is important to “**know your complete system**”
  - use case constraints ((un)supervised, environment,…)
  - biometric sensor
  - biometric algorithm
  - interfaces, processes, usability
  - monitoring
  - vulnerability analysis



3. Biometric Systems: Demands

In order to meet the increasing demand for more secure and more reliable biometric systems, we need:

- standardized testing and evaluation methodologies, for
  - biometric performance (short and long term)
  - vulnerabilities (presentation attack detection [PAD])
- standardized high quality tool boxes for PAD-testing
- continuous testing services that support manufacturers and researchers during development and allow for regular comparative market analyses
- certification schemes for ISO, CC, FIDO,… that are:
  - **internationally accepted and consistently demanded**
  - **considering** the respective **use case** and **application constraints**
  - **recertifiable** in a practical and economic way (for minor SW/HW-changes - even for systems with a short lifetime [e.g. fingerprint sensors for phones])

4. Biometric Systems: BSI activities

The BSI will do its part and enhance its activities in that field by:

- developing national technical guidelines
- developing Common Criteria evaluation methodologies and protection profiles
- supporting FIDO and ISO
- developing reproducible PAD-tool boxes
- testing of biometric systems
- developing PAD-technologies for various biometric modalities

Thank you for your attention!

Contact

Markus Ullmann, BSI DI11

Federal Office for Information Security
Godesberger Allee 185-189
53175 Bonn

E-Mail: markus.ullmann@bsi.bund.de