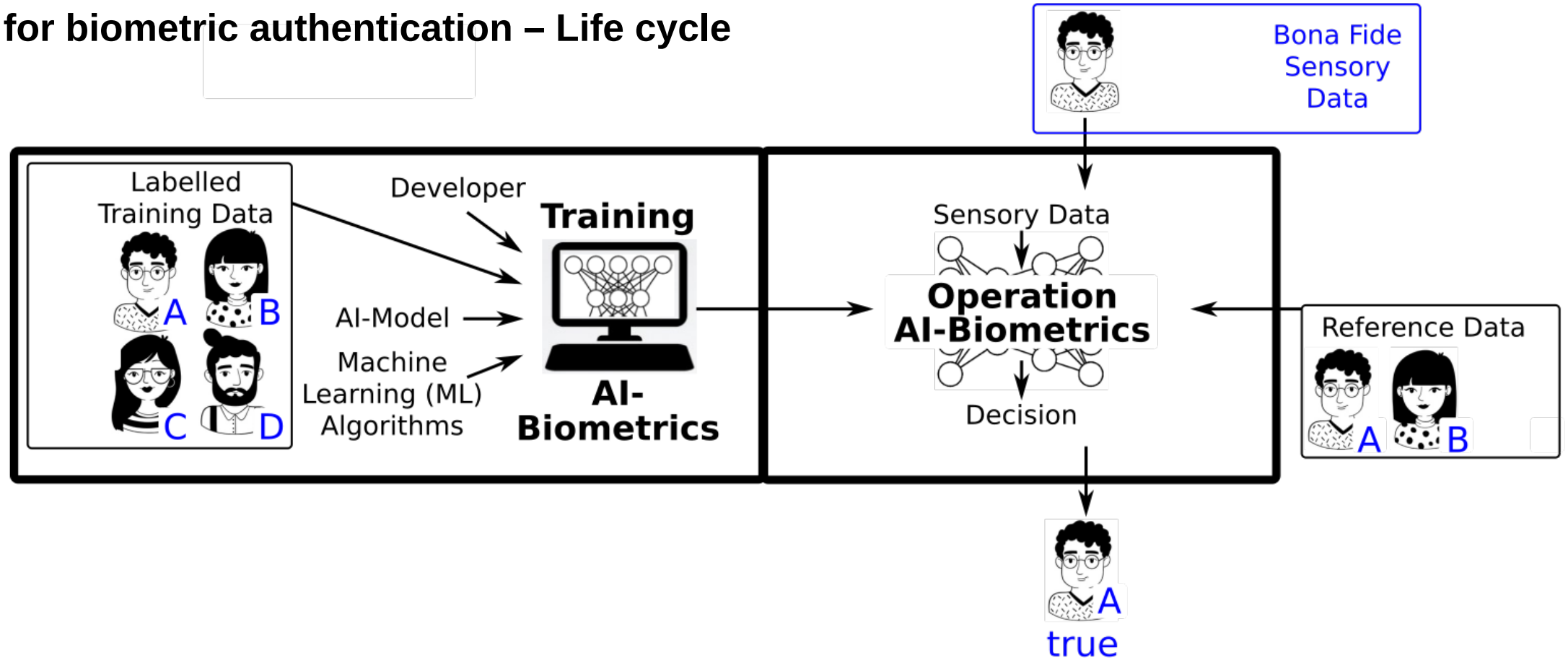
Bundesamt
für Sicherheit in der
Informationstechnik

Certification requirements for AI-based identification services

Dr. Christian Berghoff, Dr. Arndt von Twickel

ENISA/ETSI Workshop on Remote Identity Proofing
Munich/Internet, May 3rd, 2022

AI for biometric authentication – Life cycle

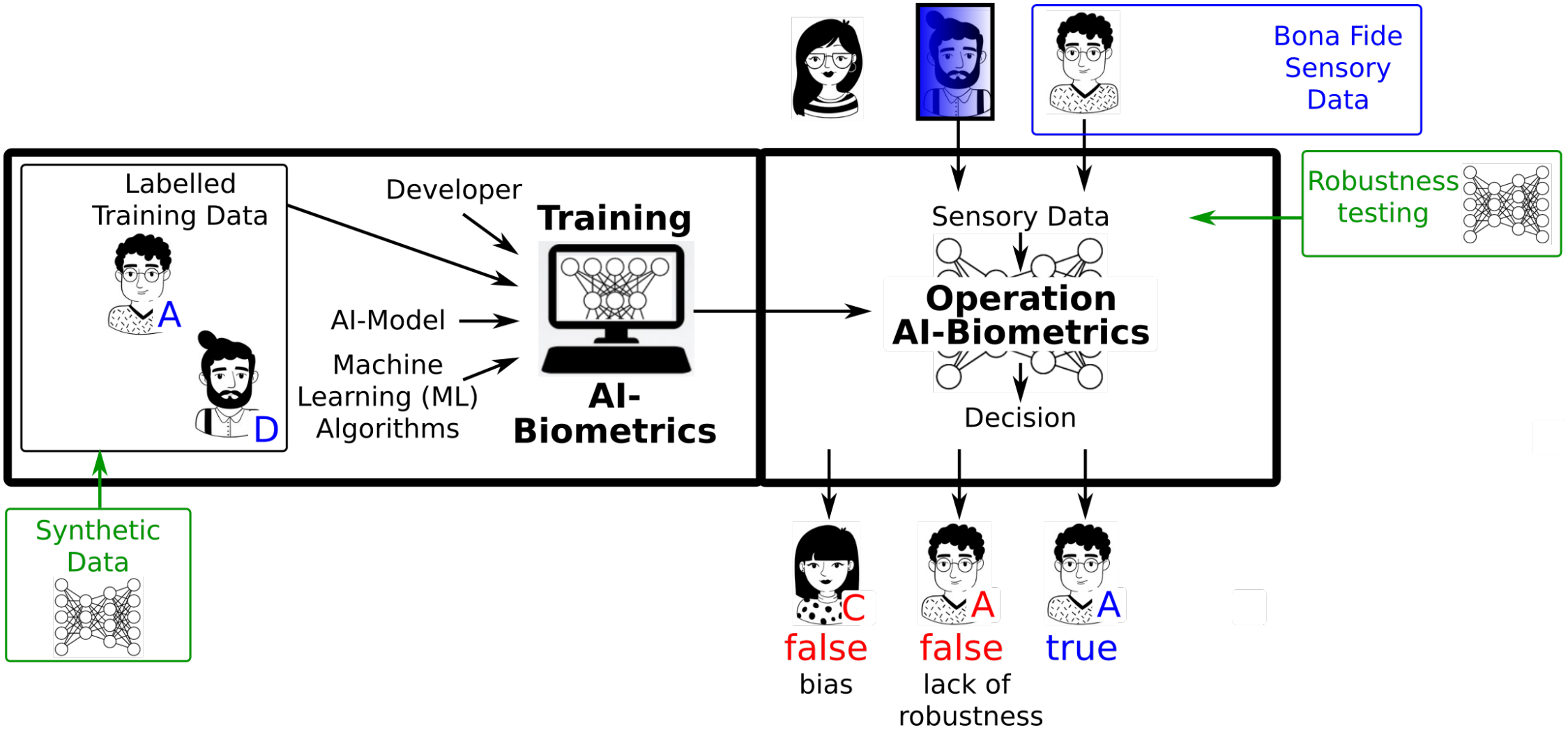


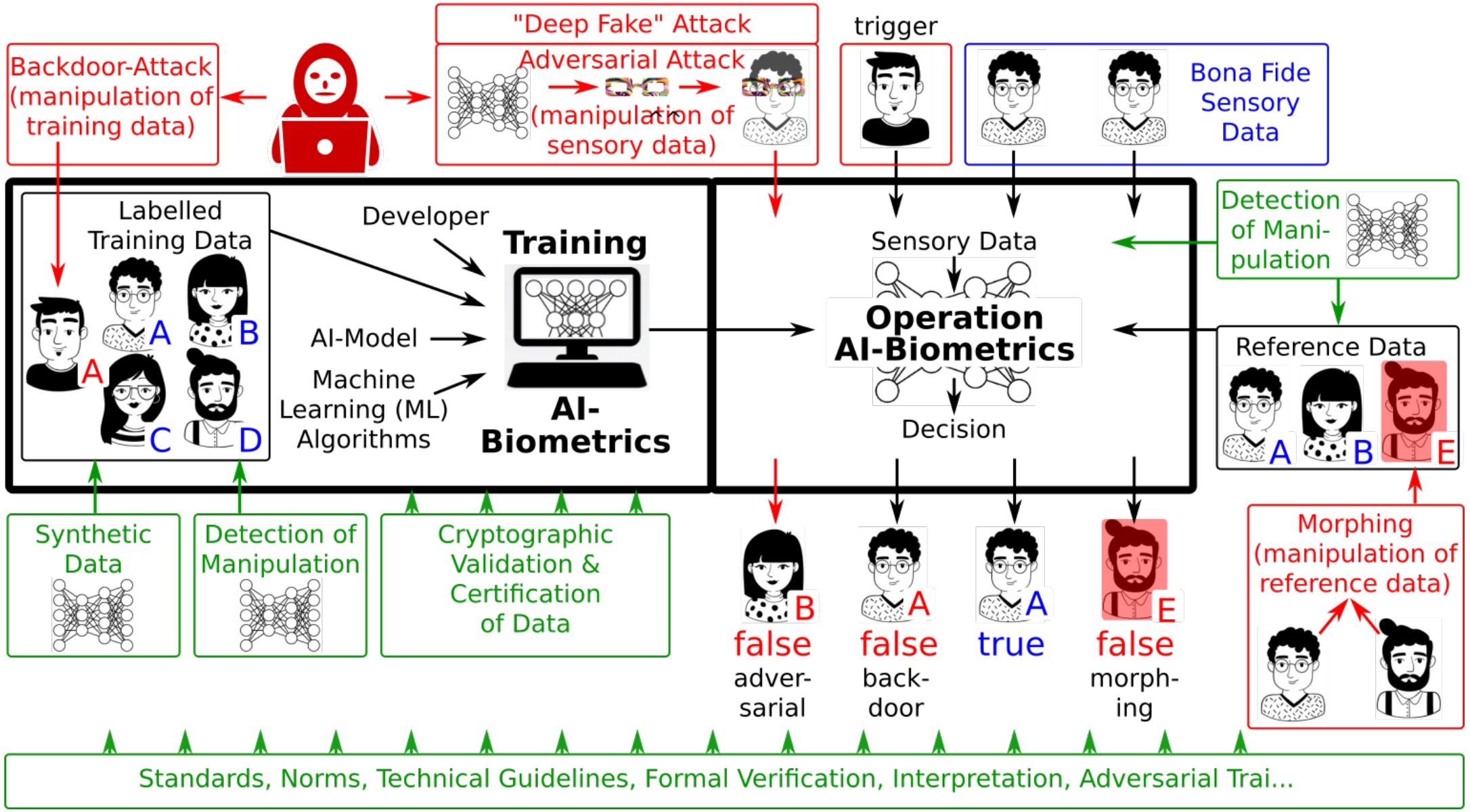
AI-based video identification – IT security challenges

- False Acceptance Rate (FAR) of system determines probability of success for trivial attacks; must be robust wrt.
  - Ambient conditions
  - Hardware
  - Feature values (e.g. sex, origin)
  - Natural changes (beard, glasses etc.)

- Further attacks are possible on different levels
  - Counterfeit documents
  - Presentation attacks
  - Video manipulation (media disruption)
  - AI-based attacks
  - Attacks targeting AI

Biased training data or a lack of robustness may facilitate impostor attacks




"Deep Fake" Attack
Adversarial Attack
(manipulation of sensory data)
Backdoor-Attack (manipulation of training data)
trigger
Bona Fide Sensory Data
Labelled Training Data
A
B
A
C
D
Developer
AI-Model
Machine Learning (ML) Algorithms
Training
AI-Biometrics
Sensory Data
Operation AI-Biometrics
Decision
Detection of Mani-pulation
Reference Data
A
B
E
Morphing (manipulation of reference data)
Synthetic Data
Detection of Manipulation
Cryptographic Validation & Certification of Data
B
false
adver-sarial
A
false
back-door
A
true
E
false
morph-ing
Standards, Norms, Technical Guidelines, Formal Verification, Interpretation, Adversarial Trai...

AI-based video identification – Problems and countermeasures

- Attacks (in particular digital ones) are reproducible due to determinism of AI system
- Availability of tools facilitates attacks significantly
  → Attacks scale better

- Countermeasures
  - Ensuring adequate performance (in particular FAR)
  - Penetration testing
  - Protect data integrity
  - Impede attack automation
  - Fraud detection
  - Manual inspection of samples

- BSI TR Bio-Ident defines requirements for biometric authentication (available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03166/BSI-TR-03166.pdf)

List of criteria for AI-based video identification

- Created by BSI in conjunction with BNetzA (Federal Network Agency, supervisory body for trust service providers)
- Criteria address threats and contain countermeasures for achieving a base level of IT security
- To be used for conformity assessment of AI-based video identification systems for trust services in Germany
- Available to affected parties upon request from BNetzA
- BNetzA has created English translation, which was made available to equivalent agencies in other MS

Thank you for your attention!

Contact

Dr. Christian Berghoff
E-Mail: christian.berghoff@bsi.bund.de

Dr. Arndt von Twickel
arndt.twickel@bsi.bund.de

Referat DI 11 - Bewertungsverfahren für eID-Technologien in der Digitalisierung

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185 -189
53175 Bonn