TÜV TRUST IT
TÜV AUSTRIA Group

ENISA & ETSI WORKSHOP
REMOTE IDENTITY PROOFING

THE CHALLENGE OF AUDITING DEEP LEARNING BASED IDENTITY PROOFING PROCESSES

MAY 3RD, 2022

Clemens Wanko - TÜV TRUST IT / TÜV AUSTRIA CERT

The challenge of auditing deep learning based identity proofing processes

I. What's audited?

II. What's the challenge?

III. What's lacking!

Illustration: Pixabay

O. Notes and definitions

1. The term „audit“ in the sense of these slides is **not** meant to follow a certain normative definition. Its rather meant to describe in general the process of checking whether specific relevant security-, quality-, assurance- or other goals are fulfilled and for this purpose making use of appropriate tools and techniques in order to gain corresponding evidence.
2. „Audits“ always are tailored to support a **specific use case** or implementation (e.g. EU Regulation 910/2014 for Trust Services under eIDAS) with regard to the question whether specific relevant security-, quality-, assurance- or other goals are fulfilled.

Illustration: Pixabay

I. What's audited?

Process flow of the overall identification process!

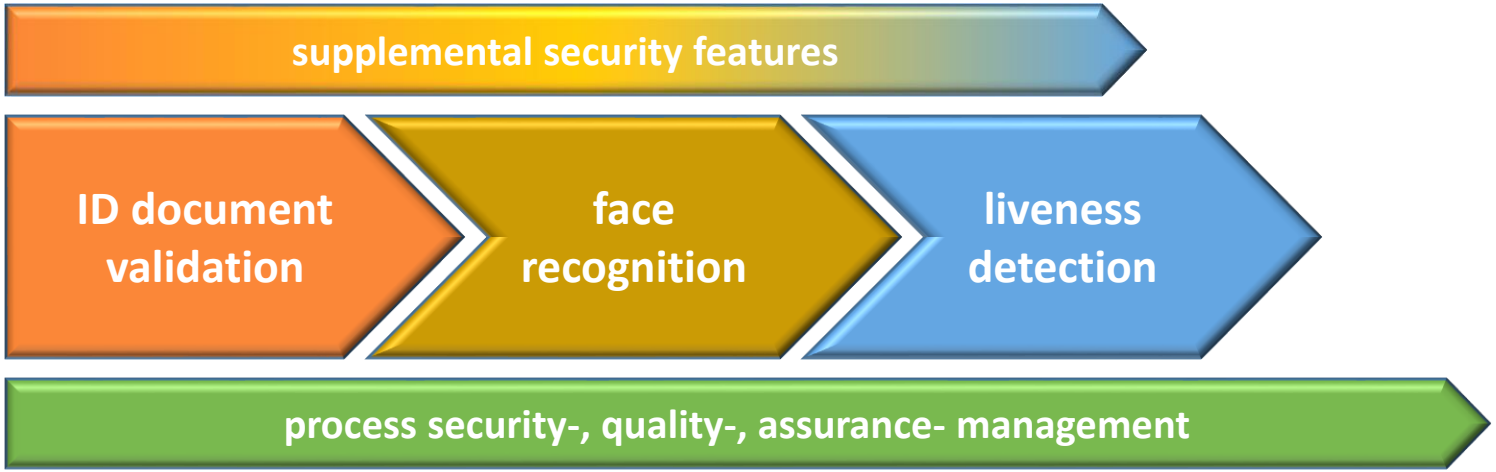

Illustration: Pixabay

II. What's the challenge?

- Per use case: identification of Key Security-, Assurance-, Quality- Identifier within the process
  We need reference values to target at!

- Deep learning based processes are "moving targets"!
  How do we audit these?

Illustration: Pixabay

I. What's audited?

Process flow of the overall identification process!

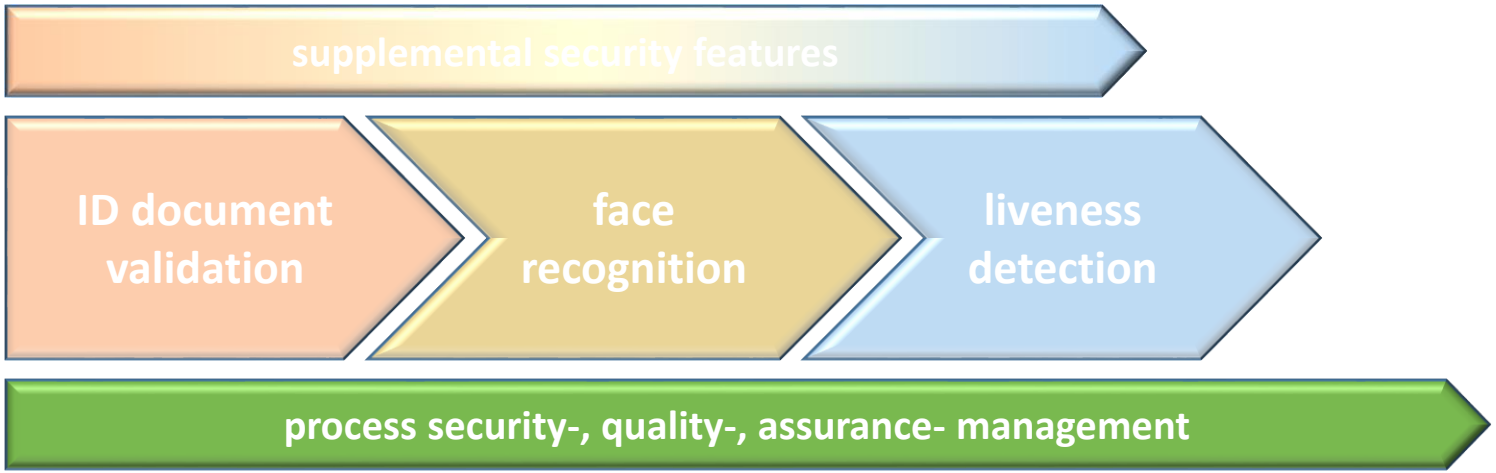

Illustration: Pixabay

III. What's lacking! (1)

- Key Security-, Assurance-, Quality- Identifier
  We need **CLEAR** reference values to target at!

Examples:

ETSI TS 119 461 as of July 2021, e.g.:

A.3 Application for issuance of QCP certificates as specified in ETSI EN 319 411-2:

Reference values missing, shall vs. should requirements, uses softeners in crucial areas (e.g. BIN-8.4.3-07, "FAR at the level of industry best practice") but without KAI depending on use case. And: it's a TS…

Illustration: Pixabay

III. What's lacking! (1)

- Key Security-, Assurance-, Quality- Identifier
  We need **CLEAR** reference values to target at!

Examples:

eIDAS 2 DRAFT as of March 2022

Art. 24 1(c) by using other identification methods which ensure the identification of the person **with a high level of confidence**, the conformity of which shall be confirmed by a conformity assessment body;

Illustration: Pixabay

III. What's lacking! (2)

- Process management **MUST** become audit focus point

Specific deep learning process related
- security,
- assurance and
- quality management

to be addressed by standards for ident-processes, like ETSI TS 119 461!

Illustration: Pixabay

Accredited Conformity Assessment Body

eIDAS eID schemes and Trust Services

TÜV TRUST IT
TÜV AUSTRIA Group

Clemens Wanko

TÜV TRUST IT
Waltherstr. 49-51
51069 Cologne
Germany

Phone +49 170 80 20 20 7
clemens.wanko@tuv-austria.com