



ENISA WORKSHOP

REMOTE VIDEO IDENTIFICATION: ATTACKS AND FORESIGHT

Block 3:
Good practices for remote identity

*Cabinet of expertise
covering technologies, standards
and European policies within the
digital security and the Cyber
security*



CLR Labs

La Ciotat

*Technology Evaluation Laboratory
(Biometrics and Security)*

May 10th, 2023
Conference Centre De Bazel, Amsterdam, Netherlands

Some Remote Identity challenges

You need to use an uncontrolled device to perform the verification

- Smartphone
- PC
- Tablet

You are never sure about an identity:



- Claude Levi-Strauss 1949

You need to collect evidences to verify an identity:

- ID documents
- Biometrics traits
- Other sources

You need to be compliant with the EU GDPR

- Personal Identification Data
- Biometrics traits
- Picture

The 5 pillars of good practices for remote identity and associated challenges

***Have a
Clear
Business
model***

Login / Password
are free of charge

***Comply to:
Regulations
Standards
Certification
schemes
(PVID)***

National based: no
EU harmonized
approach

***Defend
against fake
ID
Documents
(physical and
digital)***

Not allowed to
produce fake
documents for
testing purposes

***Defend
against
Biometrics
attacks
(Biometrics
Presentation
Attacks and
Biometrics Data
Injection Attacks)***

GDPR Data Set and
combination of
cyber security &
biometrics expertise
are needed

***Implement
Cyber
Security
hygiene and
good
practices***

From risk management
,security by design, pen
testing, to security
audit (organizational,
physical, configuration
etc...)

Good practices for remote identity: focus on Biometrics

Biometrics data injection attacks are brand new topics compares to Presentation attacks !

3 vectors of attacks for Biometrics data injection attacks:

- ***Web browser on PC/Mac***
- ***Mobile Web browser on smartphone***
- ***Mobile Application on smartphone***

Still some state-of-the-art Presentation Attack Detection algorithms can be fooled by Presentation Attacks (High Quality Silicon Masks)

Full automatic systems are not enough for critical application such as identity verification – Hybrid systems : Automatic Detection systems and Human operators are a must (and training is key).

Alternative to Remote Identity ?

1. Address; -> **Meta data, geolocation?**
2. Age; -> **Human analysis or IA ?**
3. Gender; - > **Human analysis or IA ?**
4. Civil status; -> **Human analysis or IA ?**
5. Family composition; -> **Human analysis or IA ?**
6. Nationality; -> **Meta data, geolocation or IA?**
7. Educational qualifications, titles and licenses; **cross check with other pictures ?**
8. Professional qualifications, titles and licenses; **cross check with other pictures ?**
9. Public permits and licenses; -> **cross check with other pictures ?**
10. Financial and company data. -> **Data base crossing?**
11. Personal Identity Data : -> **Data base crossing, IA?**



Note this picture is free of rights

Thanks for your attention!
stefane.mouille@cabinet-louis-reynaud.fr

