



**RÉPUBLIQUE  
FRANÇAISE**

*Liberté  
Égalité  
Fraternité*



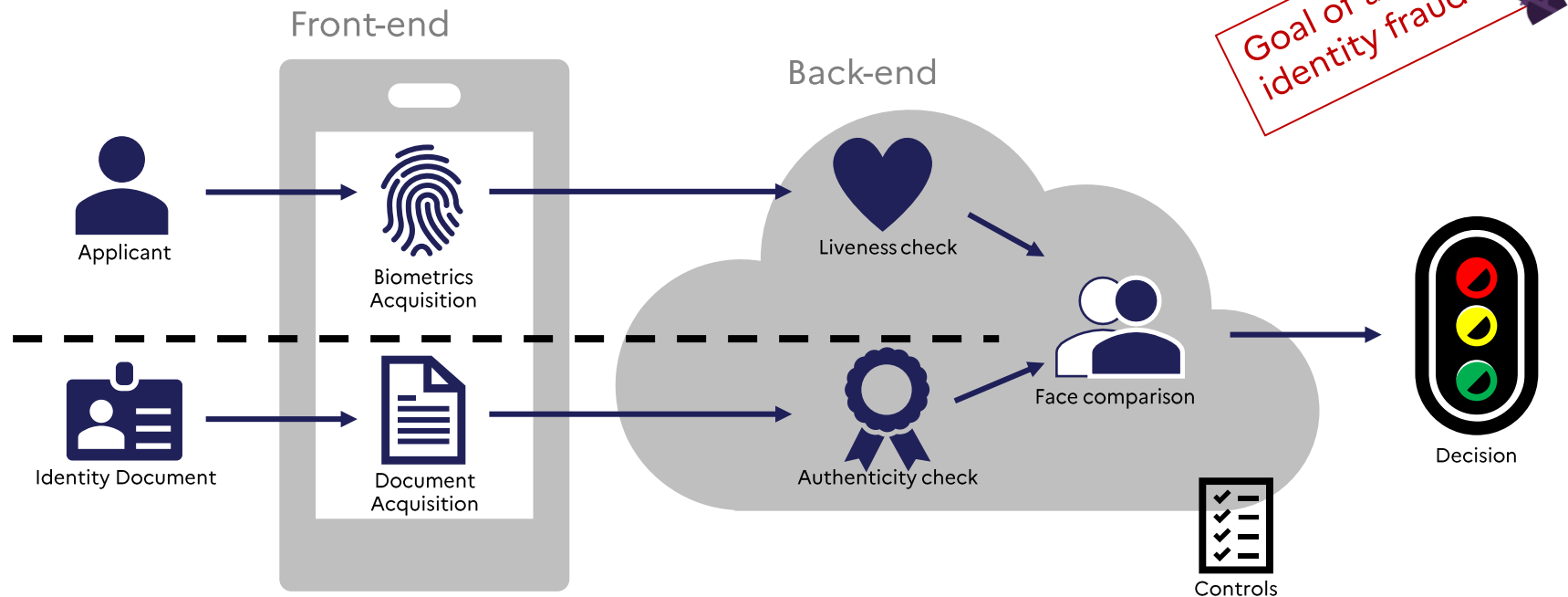
***ENISA WORKSHOP – MAY 10<sup>TH</sup>, 2023***

***REMOTE VIDEO IDENTIFICATION: ATTACKS AND FORESIGHT***

# **NATIONAL IMPLEMENTATIONS – FRANCE**

***SPEAKER: MICKAEL LAM / CERTIFICATION EXPERT - DIGITAL IDENTITY & TRUST, ANSSI***

# Remote identity verification concepts



*Source: Remote Identity Proofing: Attacks & Countermeasures, ENISA, January 2022*

# Agenda

**1. Conformity & IT Security**

**2. Biometrics & Document  
Authenticity**

**3. Foresights**



# 1. CONFORMITY & IT SECURITY



# Highlights of ANSSI risk analysis (1/2)



## Dynamic Acquisition

Risk: Use of physically or digitally manipulated biometrics / identity document media source

Counter measure: Require a video acquisition and random challenges instead of a picture, to complexify attack preparation.



## Hybrid Verification

Risk: Human and automated verification are subject to different risks.

Counter measure: Automated checks and human operators complement each other, but the final decision must be taken by a human operator.

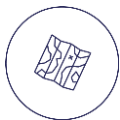


## Lost or Stolen Document Check

Risk: Use of a stolen or lost identity document.

Counter measure: Check validity of a identity document against a national registry (if registry is available).

# Highlights of ANSSI risk analysis (2/2)



## Territoriality

Risk: Difficulties to audit and guarantee GDPR compliance for providers outside of the EU.

Counter measure: The service provider must host, operate and administrate the service exclusively from a territory of a EU member state, including identity verification performed by human operators.



## Network Isolation

Risk: An attacker has successfully compromised corporate IT services and tries to gain access to remote identity verification service backend.

Counter measure: Logical isolation of remote identity verification service backend from other corporate IT services is mandatory. Physical isolation is recommended.



## Risk Analysis

Risk: Remote identity verification services are exposed to both IT security risks and risks specific to identity fraud.

Counter measure: Assess IT security risks and identity fraud risks in a documented risk analysis.

# Audits – Conformity & IT Security



**Conformity assessment**

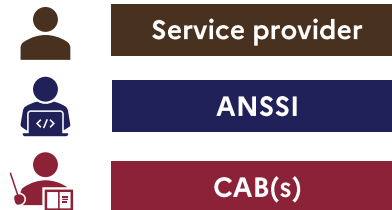


**IT security audits**  
(architecture, configuration,  
penetration tests)

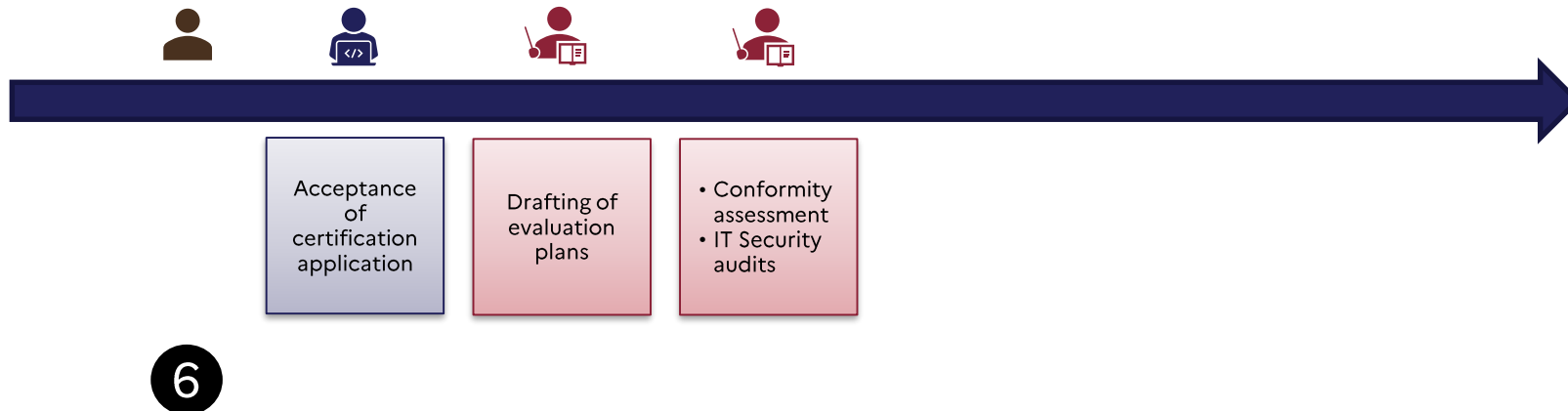
[1] List of assessment bodies candidates for PVID evaluation available here:  
<https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/centres-evaluation/>

[2] List of PASSI qualified assessment bodies available here:  
<https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf>

# Certification process



16 candidates since publication of PVID certification scheme





# Observed non-conformities

## Acceptance / Conformity assessment / IT security audits



**Hybrid Verification**



**Dynamic Acquisition**



**Territoriality**



**Risk Analysis**

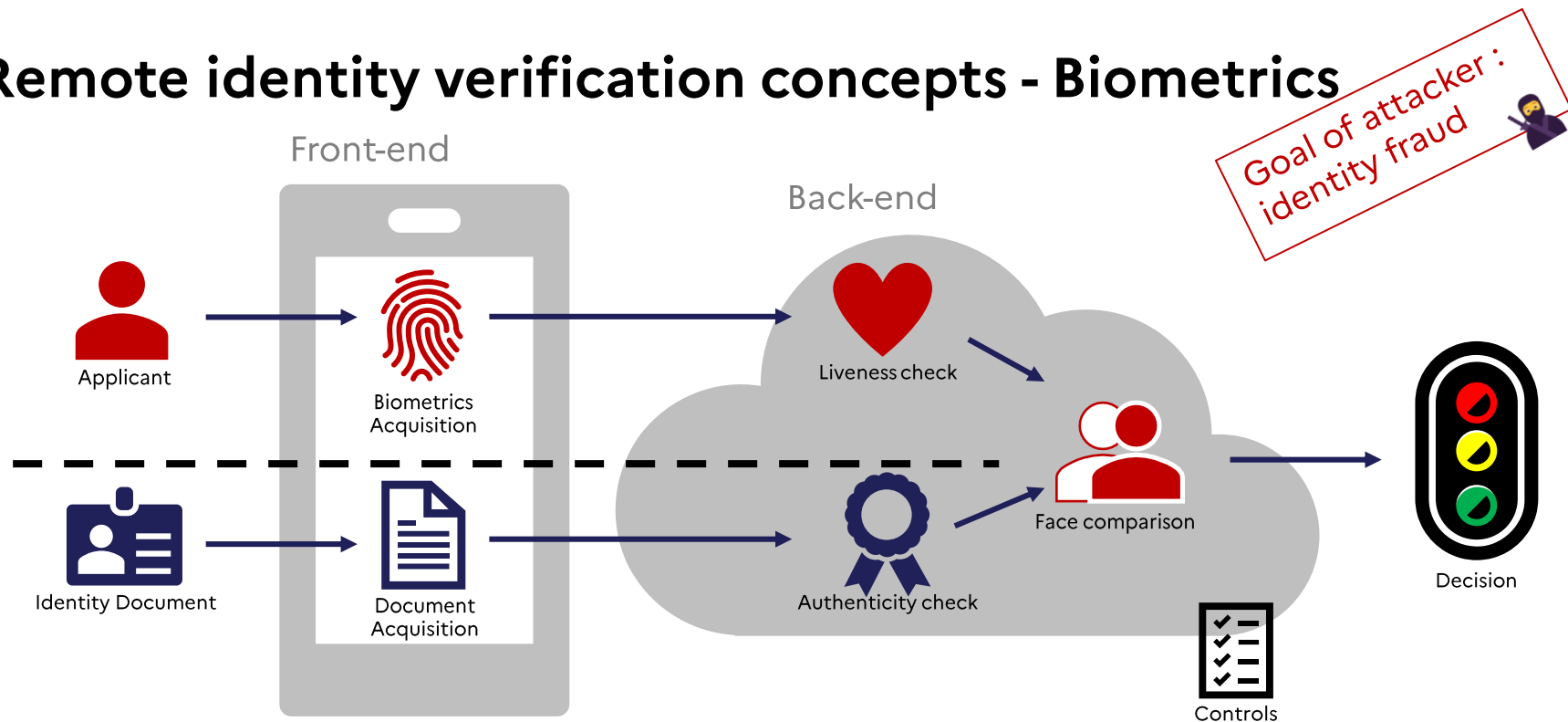


**Network Isolation**



## 2. BIOMETRICS & DOCUMENT AUTHENTICITY

# Remote identity verification concepts - Biometrics



Source: Remote Identity Proofing: Attacks & Countermeasures, ENISA, January 2022

# Audits - Biometrics tests



**Physical (*presentation*) tests  
of controls effectiveness  
on biometrics component**



**Digital (*injection*) tests  
of controls effectiveness  
on biometrics component**

**Attack potential measured with Common Criteria - Common Methodology for Information Technology Security Evaluation**



[1] List of assessment bodies candidates for PVID evaluation available here:

<https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/centres-evaluation/>

# Examples of attack levels in biometrics test plans

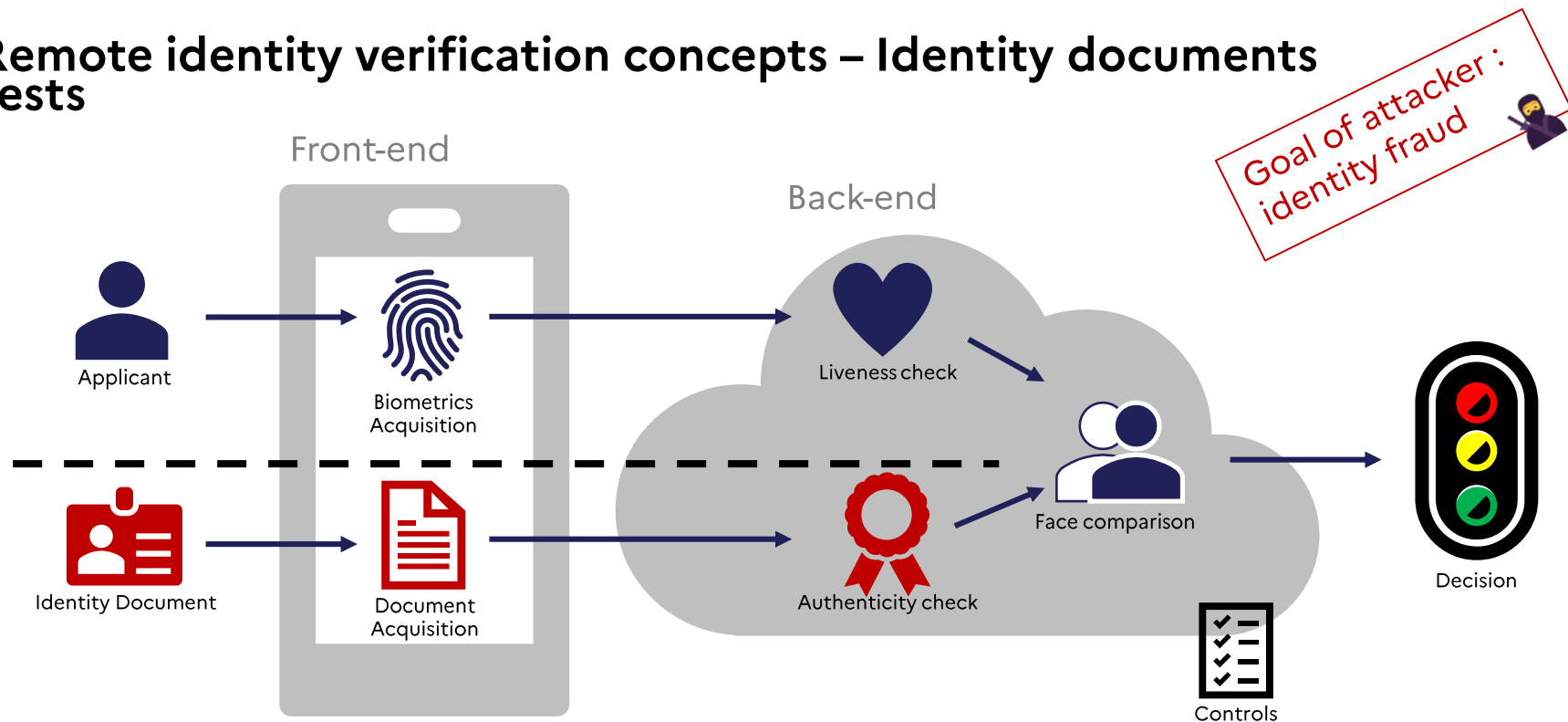
Silicone mask made from a public photo of the victim

Criterion	Value	
Elapsed Time	< 48h	1
Expertise	Proficient	3
Knowledge of the TOE	Public	0
Access to TOE	Total access	1
Equipment / Cost	Specialized	4
<b>TOE resistant to attackers with attack potential of</b>	<b>Basic</b>	<b>9</b>

Deepfake with a model trained on a public video of the victim

Criterion	Value	
Elapsed Time	1 week	1
Expertise	Expert	6
Knowledge of the TOE	Public	0
Access to TOE	Total access	1
Equipment / Cost	Specialized	4
<b>TOE resistant to attackers with attack potential of</b>	<b>Enhanced basic</b>	<b>12</b>

# Remote identity verification concepts – Identity documents tests



Source: Remote Identity Proofing: Attacks & Countermeasures, ENISA, January 2022

# Audits - Identity documents tests



**Physical (*presentation*) tests  
of controls effectiveness  
on document component**

**Attacks with forged documents from  
police collection**



**Digital (*injection*) tests  
of controls effectiveness  
on document component**

***Work in progress...***



**Onsite audit**

# Observed non-conformities

## Biometrics tests / Identity Documents tests

### Biometrics tests



Solutions relying highly on automated biometrics fraud detection :

- Vulnerability to basic attacks
- Captured material unfit for human verification (short videos, no challenge)

### Caveats



- Operator bias
- Video quality (inconsistencies)
- Generally impossible to test all accepted documents
- Absence of a complete attack path

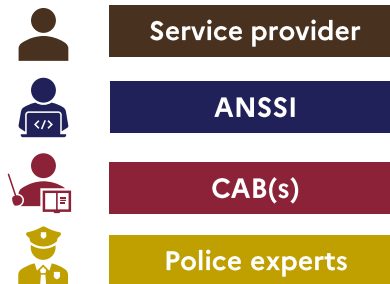
### Identity documents



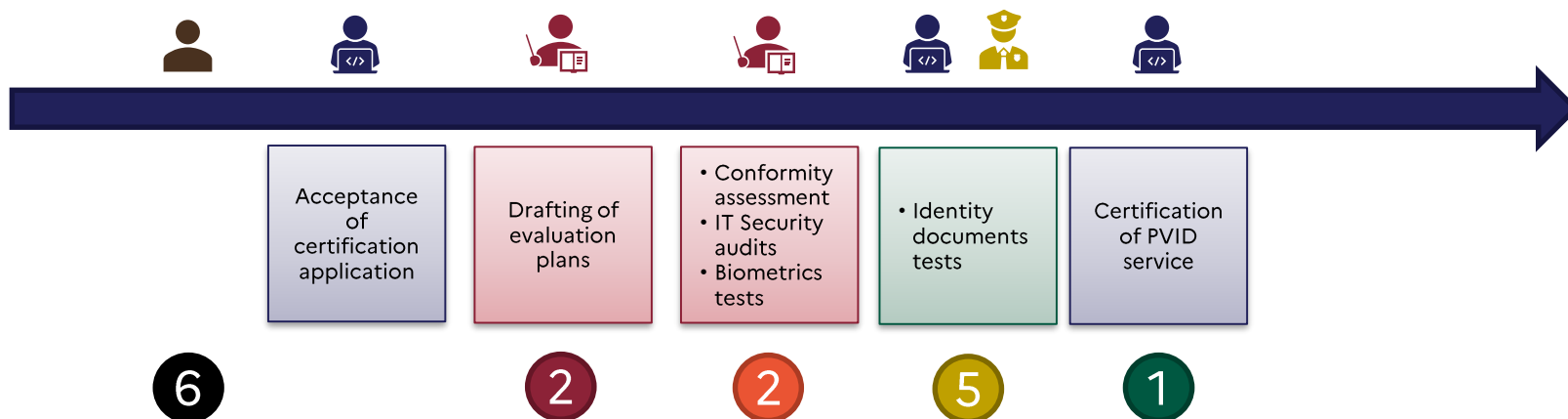
- One basic vulnerability common to all evaluated services
- Various levels of fraud knowledge and operator training, sometimes insufficient



# Certification process



16 candidates since publication of PVID certification scheme all at assurance level Substantial

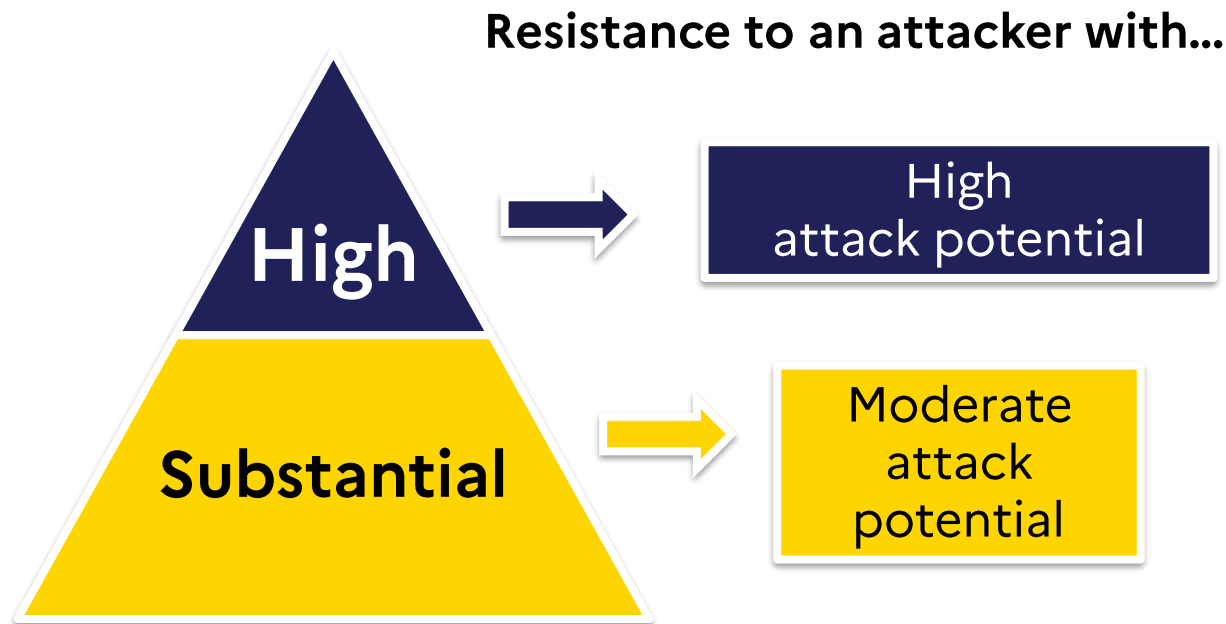


[3] List of certified services or ongoing certification is available here :  
<https://www.ssi.gouv.fr/entreprise/produits-certifies/prestataires-de-verification-didentite-a-distance-pvid/>



# 3. FORESIGHTS

# Assurance levels in PVID certification



## Why two assurance levels?

- 1/ Not all use cases require the highest level of security
- 2/ Consistency with eIDAS regulation

# Assurance level « High »



## Assurance level « Substantial » requirements



**Mobile  
application  
certification**



**Reinforced IT  
security  
measures**



**Resistance to  
biometric attacks  
of level high**



**Document  
authenticity check  
based on NFC chip**



**Mandatory lost  
and stolen  
document check**



# Regulatory limitations

## Chip reading

Identity document chip reading is limited for private service providers by regulation (EU) 2019/1157 (or some national regulations)

## Validity check

Access to lost and stolen registries for service providers is not available for all identity documents

## Tests with forged documents

Creation, storage and use of forged identity documents for tests is forbidden in most (all?) EU member states



**Need for a  
harmonized  
regulatory  
framework**



# Rapid evolution of attacks

Member states  
& providers



Attackers



Digital identity technologies



# THANK YOU FOR YOUR ATTENTION