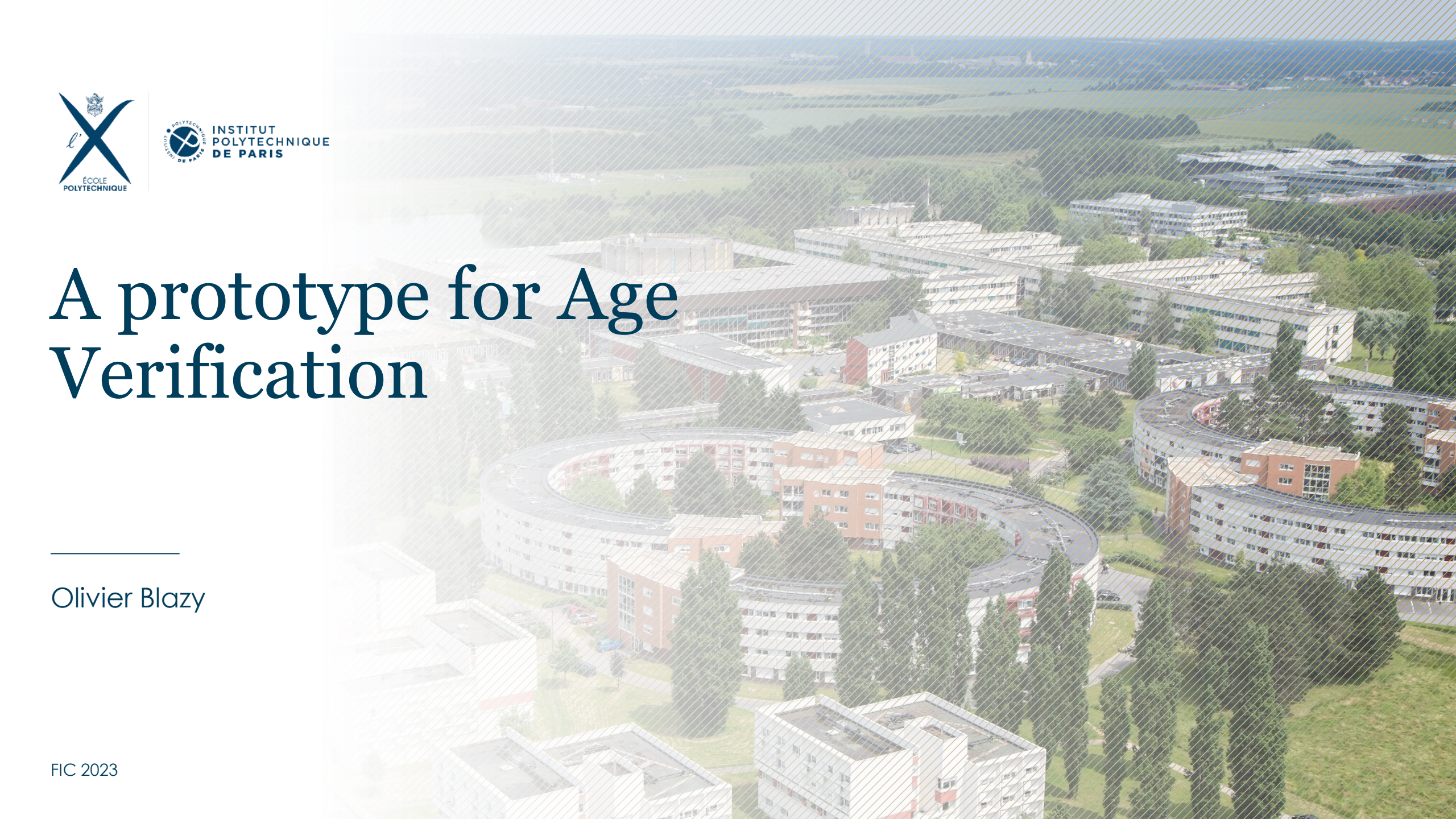


A prototype for Age Verification

Olivier Blazy

FIC 2023

A word of warning

This is my view as an academic of the project,

Nothing presented, written, said here should be seen as the official position of any French entities.

Brief Timeline

July 30th 2020

Law for mandatory Age Check

September 2021

Trial of "famous" plaforms in France

October 2021

Start of the collaboration with CNIL

December 2021

Arcom intimates platofrms to comply

January 2022

First fully packaged version

Spring 2022

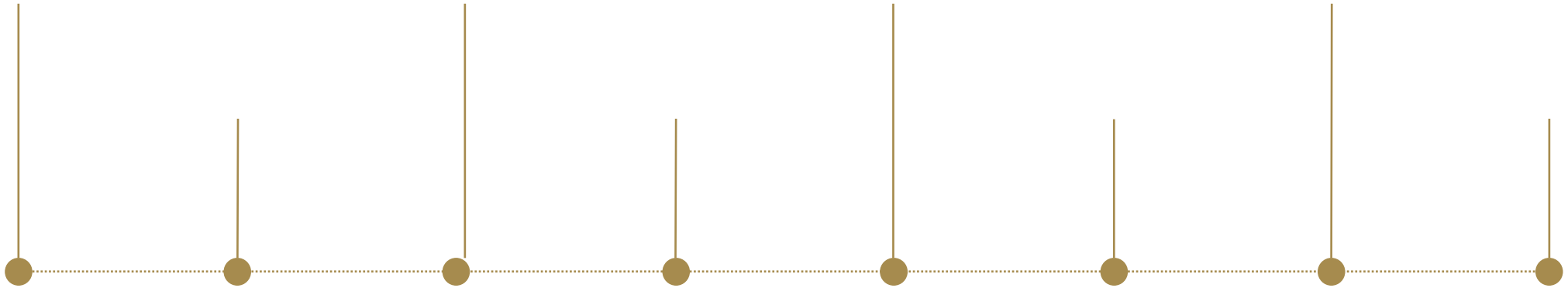
CADA on the PEReN forces public communication

June 2022

Official release on various repos

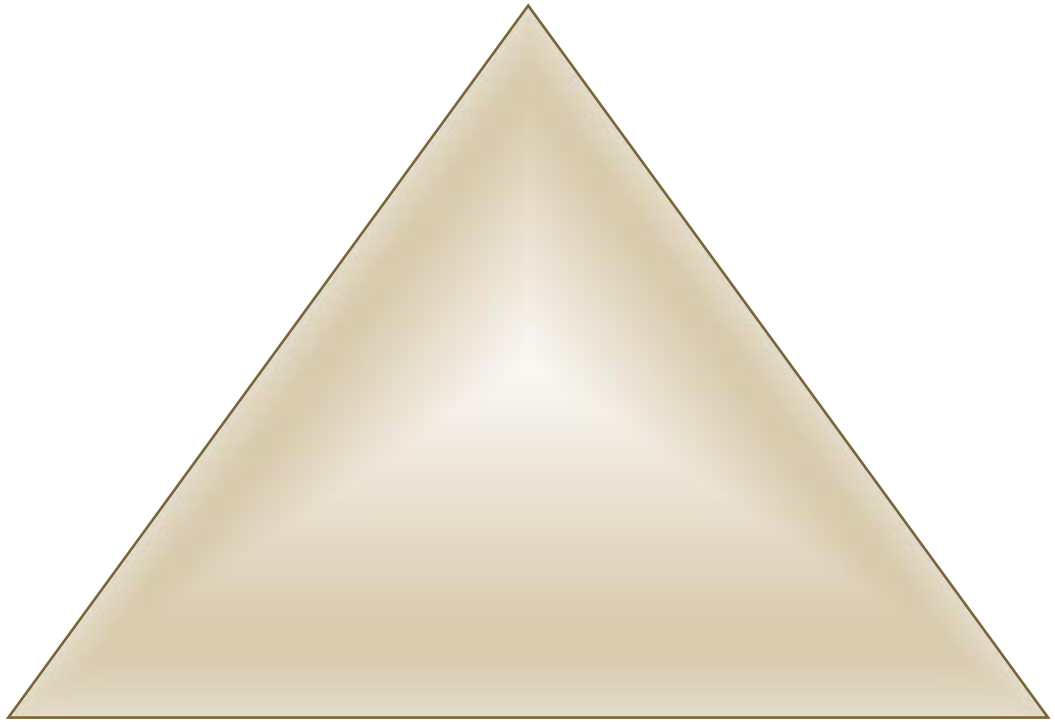
2023

An experiment?



A delicate Tripod

Unforgeability



Protection against the Verifier

Protection against websites

Unforgeability

It should not be possible to:

- produce a valid token, if we are underage
  - ➡ Use of a digital signature mechanism

- replay a token
  - ➡ Interaction is necessary

Protection against the website

The website should not learn:

- Our identity
- Our age (Knowing if someone is above 18, is not knowing he is 37)

  ➡ The answer should be a bit, and not contain the age. (GDPR: Minimisation)

- Learn which age check authority certified the age

  ➡ Signature should be anonymous (aka group signature)

Protection against the verifier

The verifier should not learn:

- Which age is expected (SN > 15 vs X-rated site > 18)
  - ➡ Three main thresholds exist, so answer to all 3
- Learn for which website the query is
  - ➡ The query should not contain information about the website
  - ➡ No direct communication between the website and the verifier

Very high overview of the prototype with CNIL and Peren

A meta-authority certifies the verifiers

→ Allow verifiers to prove they operate withing some legislative framework

When a user access a website, they receive a challenge

→ Separation + Unicity

The user forwards this challenge to a verifier of their choice

→ Separation + Choice

The verifier signs (for the meta-authority) the challenge

→ Anonymity of the verifier + Unforgeability

The user forwards the signature

→ Separation + Anonymity of the user

Upcoming evolutions?

The API is compatible with every age verification system

- No technical limitation, the legislator can pick those he finds suitable

The code is open, online for nearly a year

- Public audits are good, suggestions / evolutions are welcome
- Proposing a digital common is important in a digital context

A modular tool

- Possibility to integrate a mechanism to bill the verification to the platforms. (2 lines to tweak)
- Anonymity can be reinforced (blind signature, randomisation [already here])
- Can add an additional layer, so that User can check they are not targeted by their verifier
- Various trust level can exist for verifiers depending on the context

Pitfalls?

What about digital fracture?

- People accessing a website already have some tech available
- Might be an issue for tourists, so need for some age verifier not based on local IDs.

What about VPN?

- Independant from the solution… If the website don’t know they should do an age check
- Need for a global solution

Anonymity?

- In term of GDPR it’s pseudonymity. IP is not hidden.
- But the API does not weaken « more », the loss in privacy due to this
- Various trust level can exist for verifiers depending on the context

Merci

Olivier.blazy@polytechnique.edu

https://github.com/LINCnil/SigGroup

ÉCOLE POLYTECHNIQUE

INSTITUT POLYTECHNIQUE DE PARIS