LDMI 2023

Web Environment Integrity

What is it, where is it coming from, and where is it going?

POLITECNICO OPEN
unix LABS

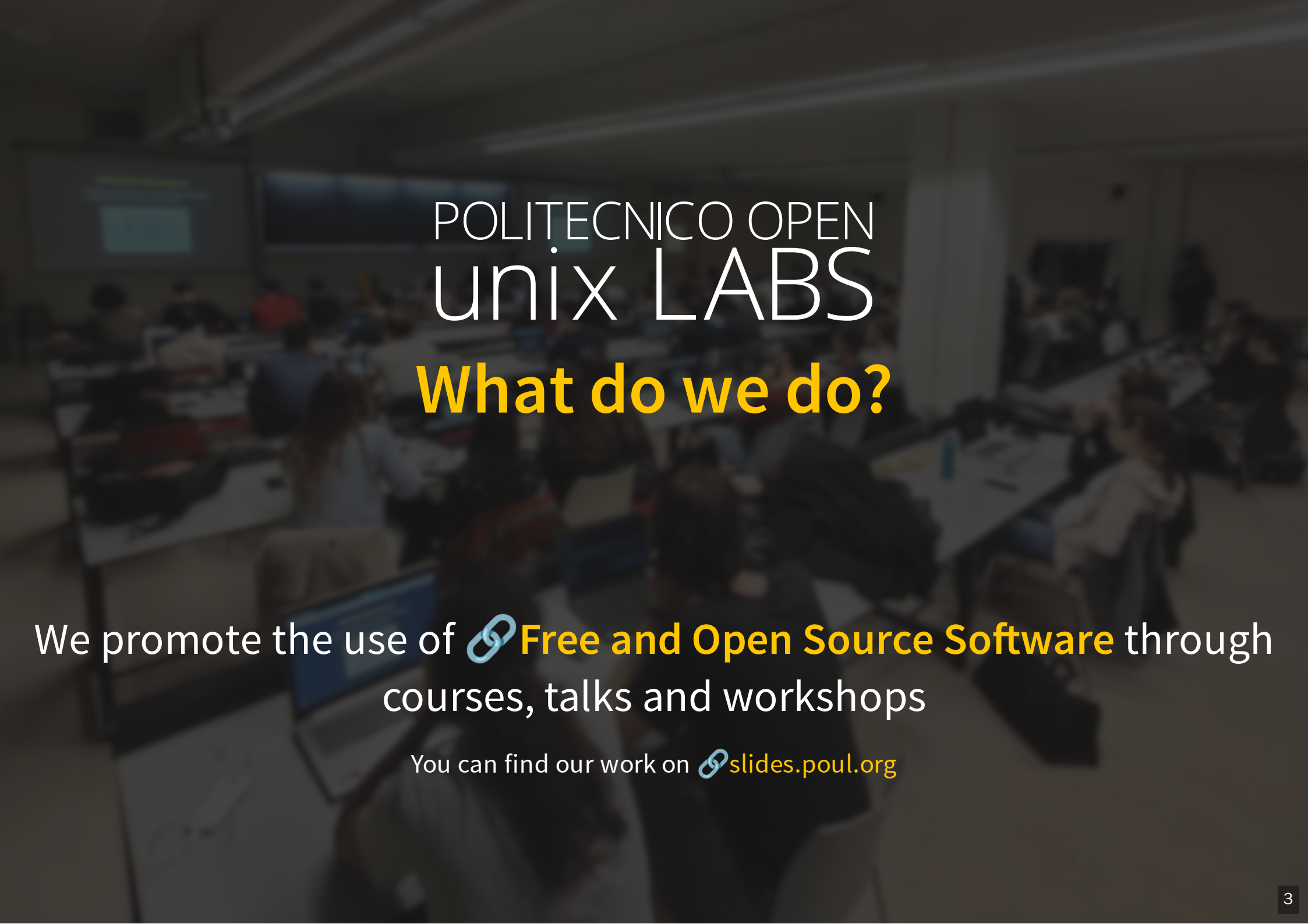
Valentina Sona
versus@poul.org

POLITECNICO OPEN

unix LABS

Who are we?

We are a non-profit *association* and *hacking community* formed by students from 🔗Politecnico di Milano, the largest technical university in Italy.



POLITECNICO OPEN

unix LABS

What do we do?

We promote the use of 🔗**Free and Open Source Software** through courses, talks and workshops

You can find our work on 🔗slides.poul.org

What is Web Environment Integrity (WEI)?

... and why are we *still* talking about it

Why WEI?

In april this year, a group of Google engineers came out with a proposal.

Speaker notes

Web Environment Integrity, at this time, is just a *proposal.* When it comes from google, it's not terribly strange to have *this* much outrage about a still to be developed proposal, if only because it's google, and we're *always* ready to be outraged by google.

Why WEI?

In april this year, a group of Google engineers came out with a proposal.

It got some pretty strong reactions:

🔗Mozilla: "[...] it contradicts our principles and vision for the Web."
🔗Vivaldi: "Simply dangerous."
🔗Free Software Foundation: "[...] an all-out attack on the free Internet"
🔗Brave Browser: "[...] the latest step in a terrible direction Google is pushing for the Web."
🔗Electronic Frontier Foundation: "WEI shouldn't be made. If it's made, it shouldn't be used. "

Why WEI?

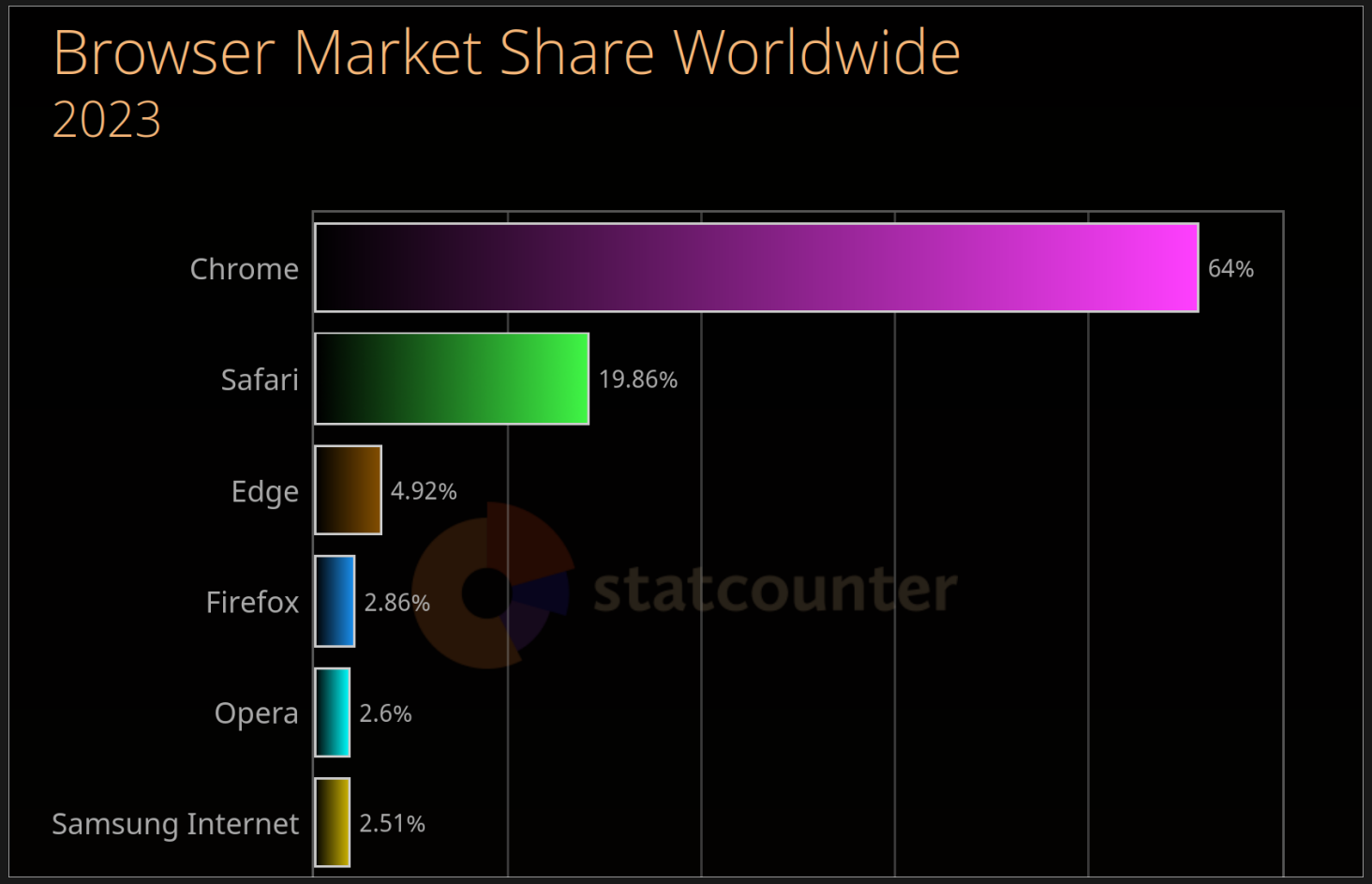
The cause of concern?

Speaker notes

It's an example of the kind of dangerous, unilateral decision a monopoly can push for. If you want other examples, my colleagues have a talk about that. It's a proposal that could do significant damage to the web even if only google implemented it.

Why WEI?

The cause of concern? Google could still unilaterally enforce this proposal despite the opposition.



Why WEI?

Current status

At this time, there is a protype, unreleased implementation inside Chromium for Android. All has been quiet on further development for a while.

Why WEI?

So why this talk?

So why this talk?

- It's a good case study on the influence of monopolies on web standard and policies.

So why this talk?

- It's a good case study on the influence of monopolies on web standard and policies.
- It's a new thing only in *scope:* all phones already have some form of this.

So why this talk?

- It's a good case study on the influence of monopolies on web standard and policies.
- It's a new thing only in *scope:* all phones already have some form of this.
- ... and just because it looks dead doesn't mean it will stay dead.

So what is this WEI proposal?

What is WEI?

From the 🔗WEI explainer:

With the web environment integrity API, websites will be able to request a token that attests key facts about the environment their client code is running in. For example, this API will show that a user is operating a web client on a secure Android device. Tampering with the attestation will be prevented by signing the tokens cryptographically.

What is WEI?

From the 🔗WEI explainer:

*With the **web environment integrity API**, websites will be able to request a token that attests key facts about the environment their client code is running in. For example, this API will show that a user is operating a web client on a secure Android device. Tampering with the attestation will be prevented by signing the tokens cryptographically.*

Speaker notes

It's an API, which means, in this case, that it's a service that someone provides

What is WEI?

From the 🔗WEI explainer:

*With the web environment integrity API, **websites will be able to request** a token that attests key facts about the environment their client code is running in. For example, this API will show that a user is operating a web client on a secure Android device. Tampering with the attestation will be prevented by signing the tokens cryptographically.*

Speaker notes

This service is provided not to users, but to the websites

What is WEI?

From the 🔗WEI explainer:

*With the web environment integrity API, websites will be able to request **a token that attests key facts** about the environment their client code is running in. For example, this API will show that a user is operating a web client on a secure Android device. Tampering with the attestation will be prevented by signing the tokens cryptographically.*

Speaker notes

Sensitive information is sent to the service in a verifiable way (no lies) which returns a token that attests that the server has received these facts. This is called remote attestation.

What is WEI?

From the 🔗WEI explainer:

With the web environment integrity API, websites will be able to request a token that attests key facts ***about the environment their client code is running in****. For example, this API will show that a user is operating a web client on a secure Android device. Tampering with the attestation will be prevented by signing the tokens cryptographically.*

Speaker notes

The information concerns the client machine, regarding the "underlying hardware and software stack". It means you cannot lie about detailed information such

What is WEI?

From the 🔗WEI explainer:

With the web environment integrity API, websites will be able to request a token that attests key facts about the environment their client code is running in. For example, this API will show that a user is operating a web client on a ***secure*** *Android device. Tampering with the attestation will be prevented by signing the tokens cryptographically.*

Speaker notes

What is the definition of secure? On what basis is this judgement given?

What is WEI?

From the 🔗WEI explainer:

With the web environment integrity API, websites will be able to request a token that attests key facts about the environment their client code is running in. For example, this API will show that a user is operating a web client on a secure Android device. ***Tampering with the attestation will be prevented*** *by signing the tokens cryptographically.*

Speaker notes

You have only two options: submit yourself to this "attestation" or refuse to. Is this opt out a real

What is WEI?

This kind of mechanism is called **remote attestation**.

Speaker notes

You have only two options: submit yourself to this "attestation" or refuse to. Is this opt out a real

How does ~~WEI~~ remote attestation work?

How does WEI work?

There are three actors in the WEI proposal:

The client browser

Which calls the WEI API

The website server

Which requests the WEI token

The attester

Where the WEI API lives, and the token is produced

How does WEI work?

The client browser

Which calls the WEI API

The website server

Which requests the WEI token

The attester

Where the WEI API lives, and the token is produced

The client wants to visit a website

How does WEI work?

The client browser

Which calls the WEI API

The website server

Which requests the WEI token

The attester

Where the WEI API lives, and the token is produced

The website says: "Show me proof you're trustworthy!"

How does WEI work?

The client browser

Which calls the WEI API

The website server

Which requests the WEI token

The attester

Where the WEI API lives, and the token is produced

The client can't just say "I am!" so he has to go to the attester and show him some kind of *official ID*

How does WEI work?

The client browser

Which calls the WEI API

The website server

Which requests the WEI token

The attester

Where the WEI API lives, and the token is produced

The attester reads the information on the ID and judges wether the client is trustworthy and secure, and gives it to the client as a **token**

How does WEI work?

The client browser

Which calls the WEI API

The website server

Which requests the WEI token

The attester

Where the WEI API lives, and the token is produced

The client presents the token to the website, who then decides, based on the judgement inside it, what to do.

How does WEI work?

Key points:

- Someone has to be the attester.
  - The explainer suggests Google Play as an example
- The device must be able to provide some kind of unforgeable "ID" listing its specifications
- The attester has to emit a **judgement** based on the specifications

Where does WEI come from?

Where does WEI come from?

The 🔗repository containing the proposal was published on the 25th of April 2023.

The proposal comes from a group of Google engineers, and not from Google itself - that has so far made no statement about it.

Where does WEI come from?

It's actually born at least a year before that, when it's presented to the 🔗Anti-Fraud Community Group, a volunteer interest group under the W3C community.

The proposal is stated to come from the Google **Privacy Sandbox Anti-Fraud team**, and it's discussed in several meetings during the year.

After the explainer was published, discussion moved on to implementation details.

Where does WEI come from?

The discussion revolved around:

- The goal: they want to know whether we are running on **“actual devices.”**
- What behaviours/information can be collected to recognize humans without fingerprinting them?
- How to collect them in an unforgeable manner h.e. **exposing trusted computing hardware to the web.**

Where does WEI come from?

The original inspiration

WEI is not a new idea, but a "porting" to the world wide web of an already existing mechanism:

The Google SafetyNet (now Play Integrity) API

Obviously, Apple has a similar API for its apps too, the App Attestation Framework

Where does WEI come from?

From the 🔗SafetyNet documentation

*The SafetyNet Attestation API provides a **cryptographically-signed attestation**, assessing the **device's integrity**. In order to create the attestation, the API examines the device's **software and hardware environment**, looking for integrity issues, and comparing it with the reference data for **approved Android devices**.*

Where is WEI going?

... based on what we've seen before

Where is WEI going?

On the matter of policy: one company making the rules

Content of the proposal aside, we've seen this happen many times already (Manifest V3, JPEG-XL...)

Where is WEI going?

Approved hardware and software: obsolescence and requirements

Windows 11 requires a TPM to be installed, and WEI is sure to require some kind secure enclave as well, cutting off old or custom hardware.

Where is WEI going?

The customization struggle: tinkerers beware

On Android, custom ROMs users have to jump through many hoops to get around SafetyNet and be allowed to use banking or digital ID apps.

Where is WEI going?

A look at SafetyNet evaluation criteria

Table 1. Examples of how device status could affect the values of `basicIntegrity` and `ctsProfileMatch`

Device Status	Value of `ctsProfileMatch`	Value of `basicIntegrity`
Certified, genuine device that passes CTS	`true`	`true`
Certified device with unlocked bootloader	`false`	`true`
Genuine but uncertified device, such as when the manufacturer doesn't apply for certification	`false`	`true`
Device with custom ROM (not rooted)	`false`	`true`
Emulator	`false`	`false`
No device (such as a protocol emulating script)	`false`	`false`
Signs of system integrity compromise, one of which may be rooting	`false`	`false`
Signs of other active attacks, such as API hooking	`false`	`false`

And the migration guide to the revamped 🔗Play Integrity API

Where is WEI going?

Next steps

Developement is not looking alive, right now, but discussion still is and seems to be moving in the direction of interoperability with **PrivacyPass**: the topic has showed up at recent IETF meetings.

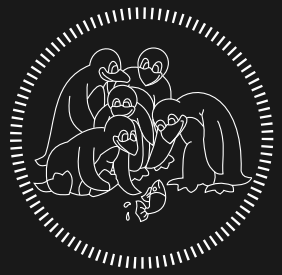
They're also discussing several implementation details, and development might just be paused while they discuss specifics.

Where is WEI going?

Conclusions

As often happens, most of these side-effects of the proposal will be mostly noticed by the open source community - so we're the ones that have to keep an eye on it.

Thank you for your attention!



POLITECNICO OPEN
unix LABS

Valentina Sona
versus@poul.org