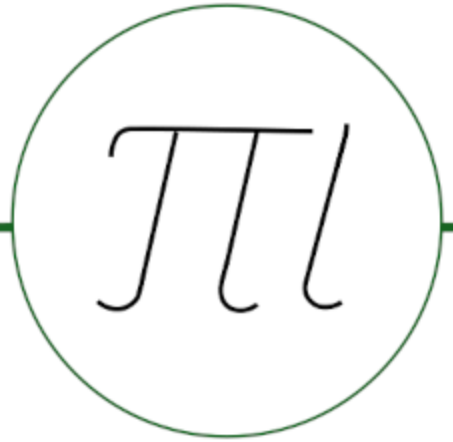


Federated Identities anyone ?

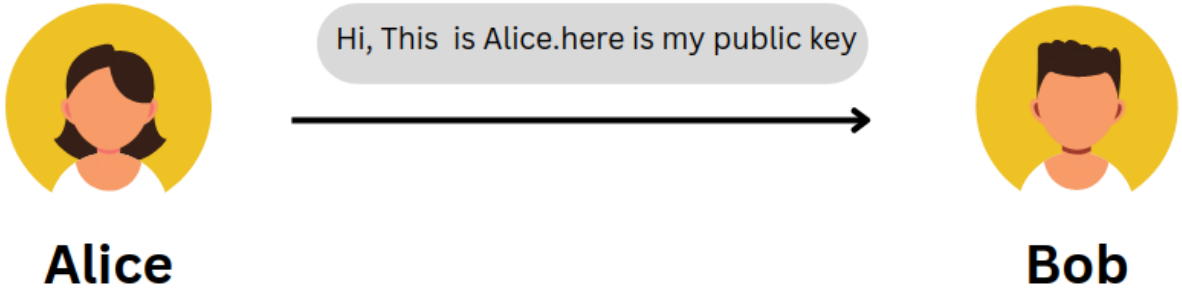
we've got lots of them ...

presented by
Stephan Schwichtenberg
pi-lar GmbH

Initial Scenario

To establish a secure communication between Alice and Bob, she is sending a request with her public key in plain text

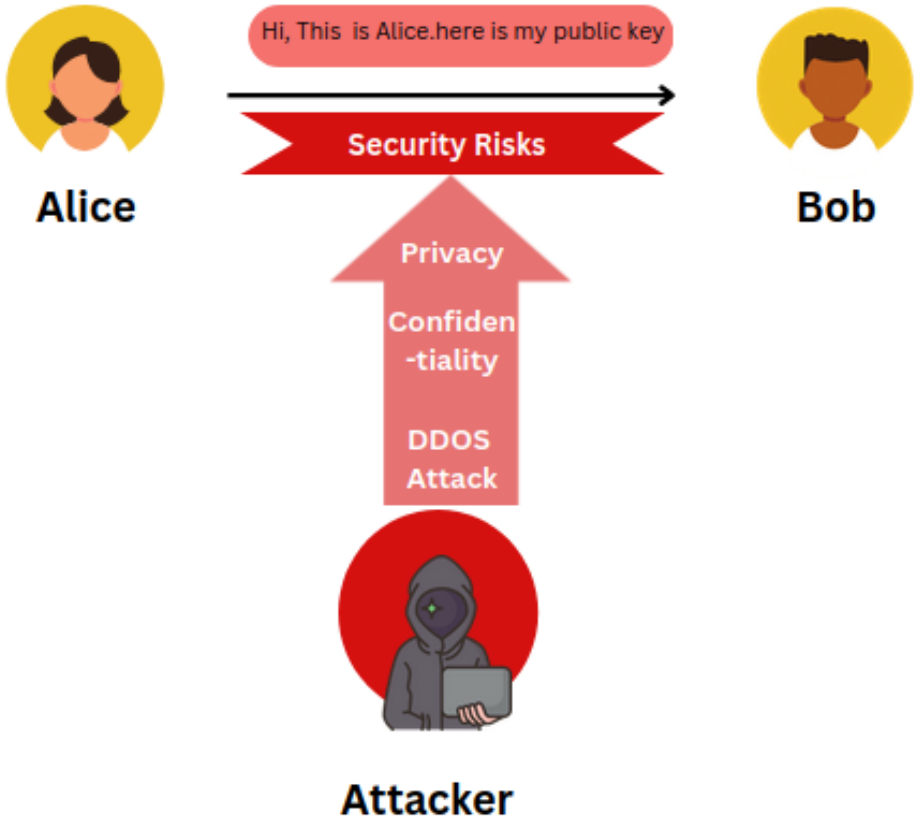
What could go wrong ?



Initial Scenario

To establish a secure communication between Alice and Bob, she is sending a request with her public key in plain text

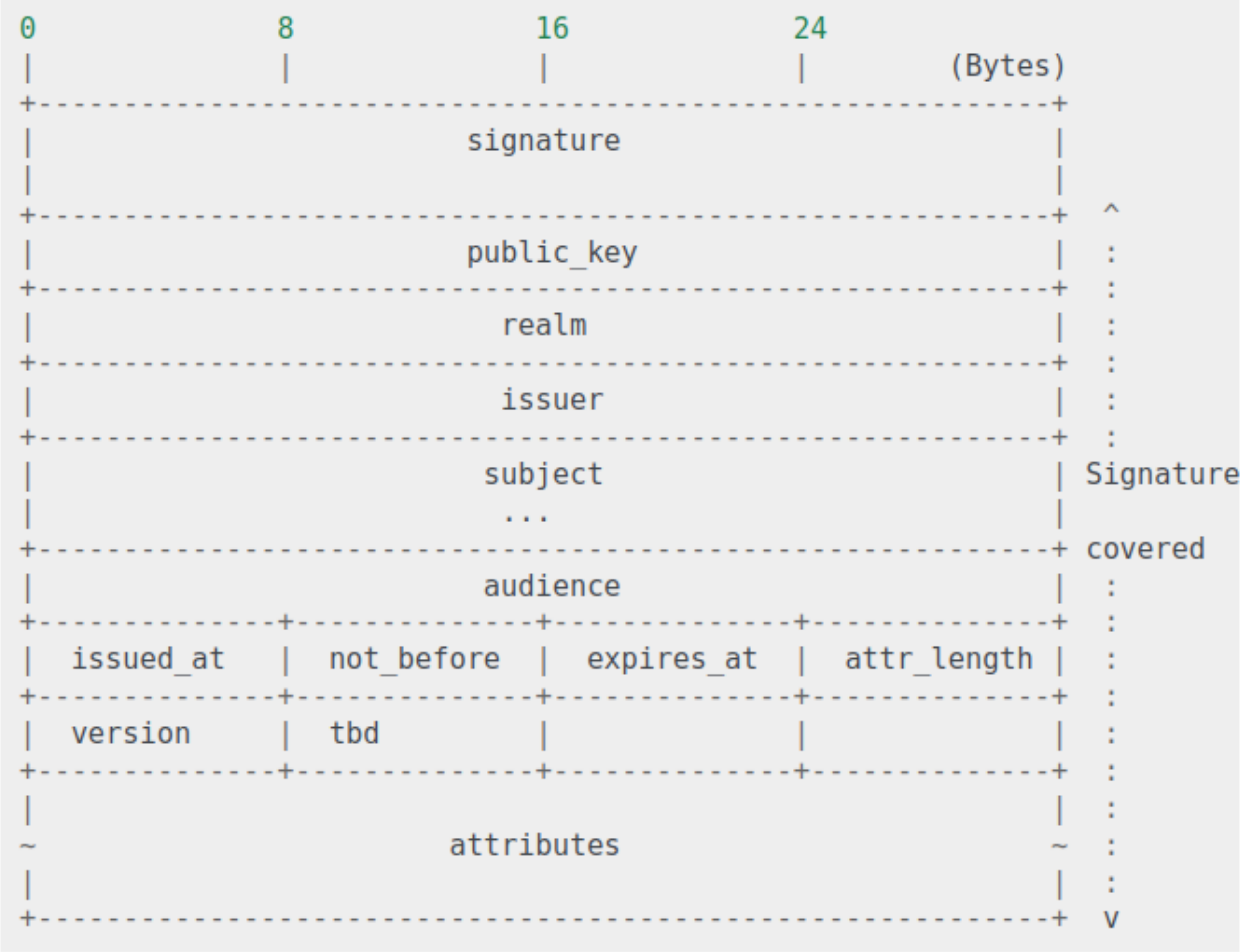
- Privacy Risks
- Group communication
- Malware Risks
- DOS Attack



Digital Identity

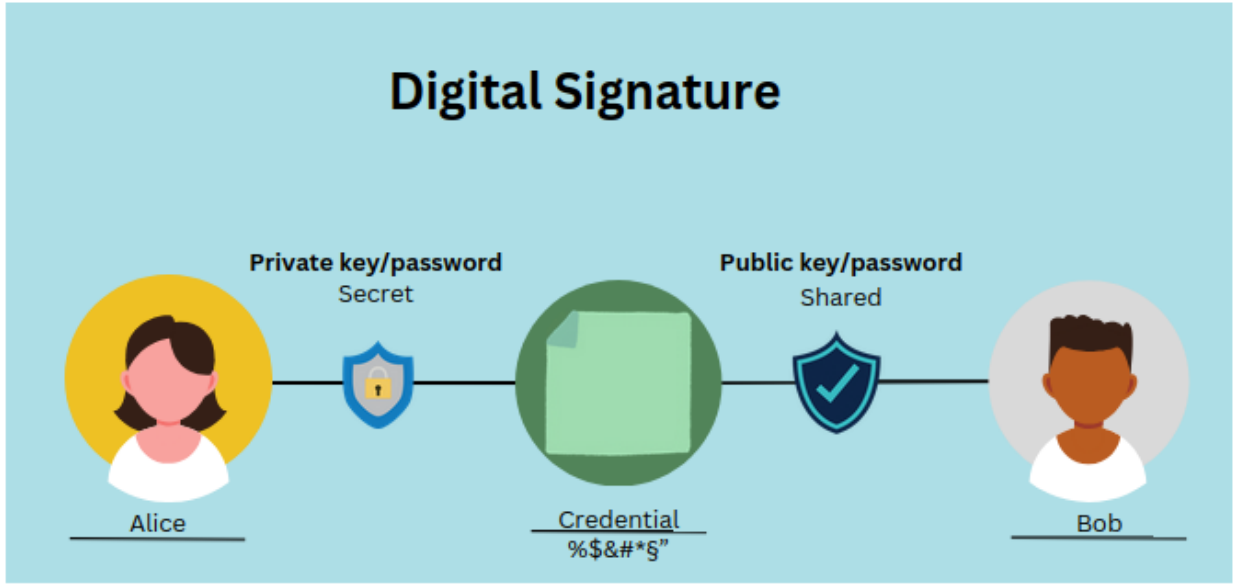
For authentication, Alice and bob exchange their digital Identity:

- similar to JWT
- issuer / audience are NPId
- include "realm" as additional attribute (NPId)
- binary serialization (CWT)
- includes a set of attributes that further serve authentication



Digital Identity

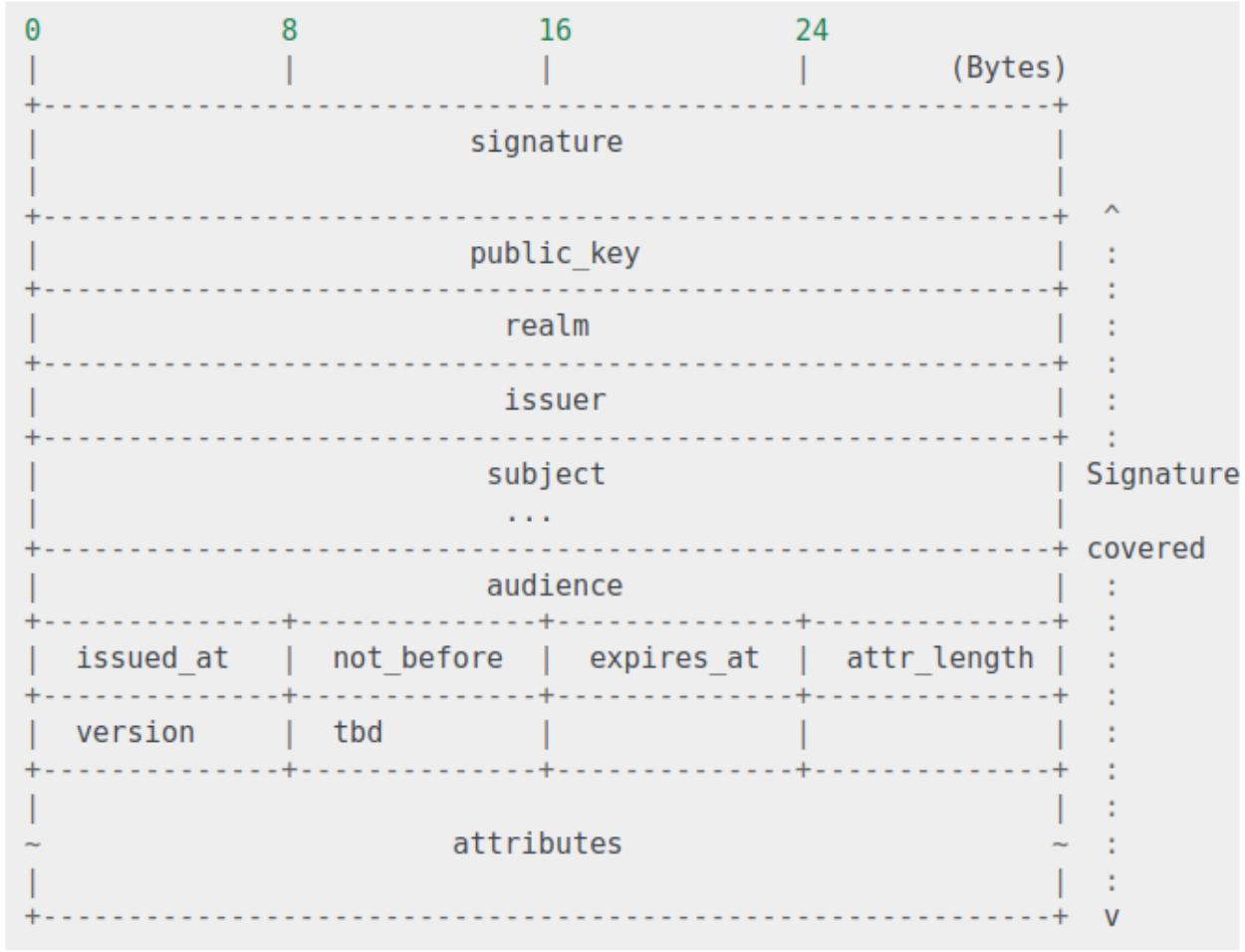
- Checking issuer field and verifying the digital signature of CA if it is maintained by a PKI
- Verify digital signature of Alice by her public key
- Each fingerprint is unique in the network



Digital Identity

For authentication, Alice and bob exchange their digital Identity:

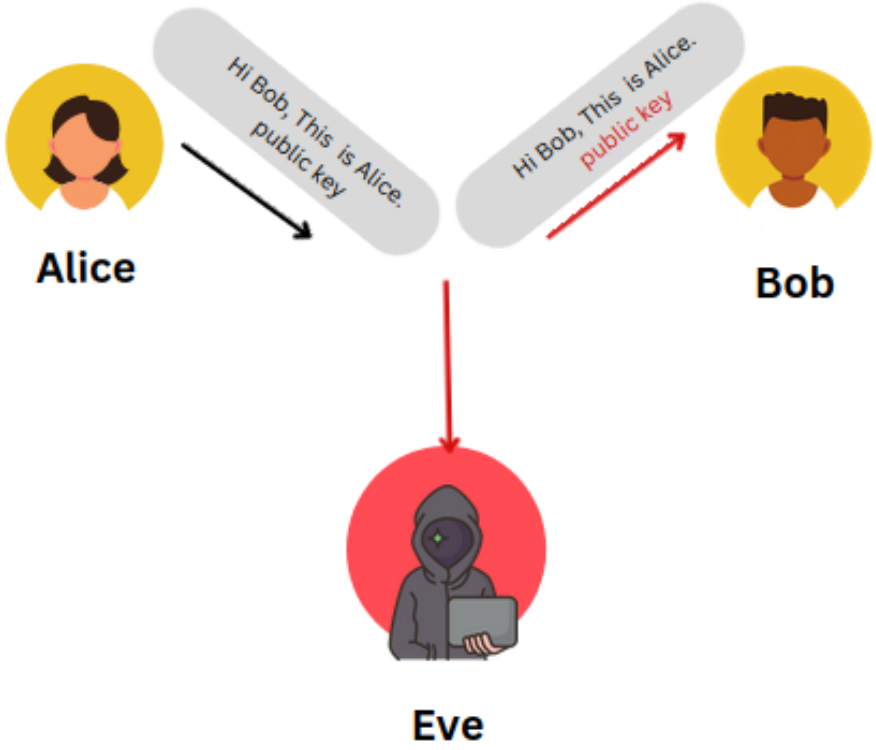
- NPId := 256-bit value, usually Blake2b Hash value
  - id1 = H("some.stupid.text")
  - id2 = H("this.is.alice")
- FP(Id) := H(signature(DI))
- NPSubject := NPId XOR NPId ...
  - id1 XOR id2
  - id1 XOR fp1



Dealing with Privacy

Lacking of Privacy several attack can be launched:

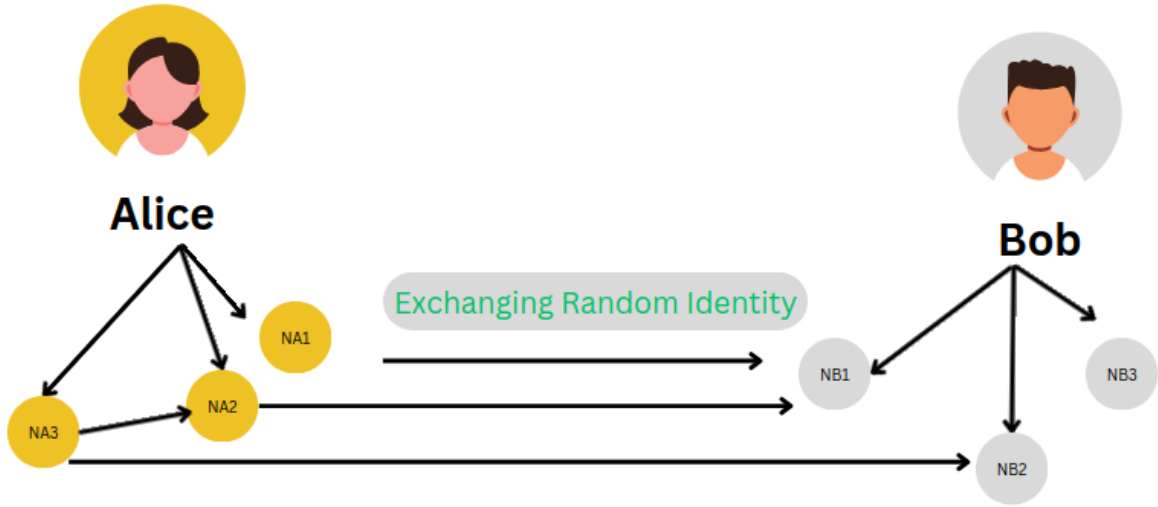
- Unauthentic Identity:
  The absence of proper authentication mechanisms can lead
  to identity spoofing, where Eve pretends to be Alice to gain access.
- Identity Theft:
  Eve can steal Alice's information, impersonate her, and communicate with Bob under false pretenses.



Additional Random Identity

Let Alice and Bob interchange random identities first instead of their real identities

- unable to determine the true identity due to the presence of unique hash values
- Each may use more than on random identity
- multiple authentication path are available
- each actor is authenticated at least once



Additional Random Identity

Unpredictability :

- identity changing frequently with session making it difficult for attackers to predict the identity.

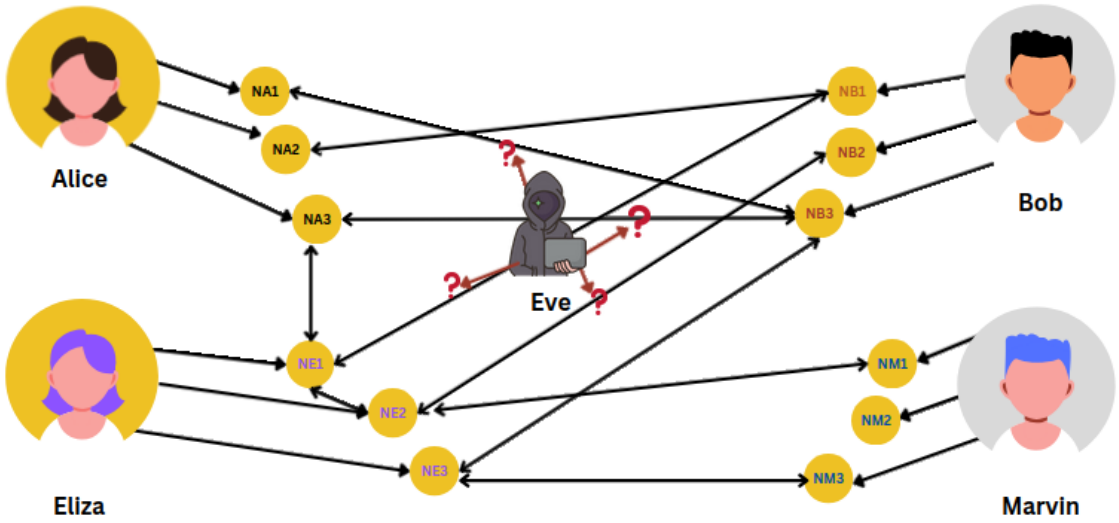
Impersonation Resistance:

- Even Attacker can steal, they can't reuse.

Obfuscation :

- Attacker can't acquire useful information from random identity.

But: Confidentiality ?

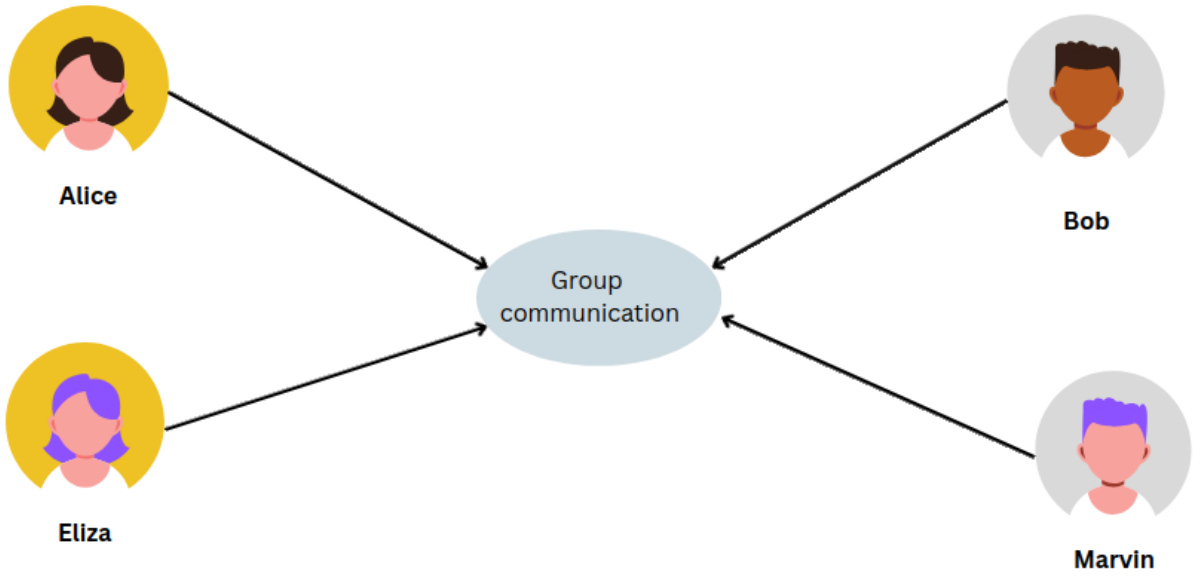


Group Communication

Up until this point, a network mesh has been displayed between two identities. Eliza and Marvin are introduced in order to provide group communication.

In general a Group Communication faces several challenges:

- Keys Distribution
- Privacy Concerns
- DDoS attack



Solution :

- use the fingerprints of the random identities for routing
- Let's add another Digital Identity: the intent token

What is an Intent Token?

Disposable Yet Official Identities

- a user has a mean to generate, control and use pseudonyms for different purposes

The purpose of intent token is:

- Generating a dedicated data channel for specific purposes
- Ensuring authentication of identities who are interested to communicate
- Ensuring time limited access with ephemeral key
- Ensuring scope limited access with additional attributes

```
realm         := <empty> | <fingerprint(realm)>
issuer        := <ifp>
subject       := 'urn:np:sub:'<hash(subject)>
audience      := <empty> | <fingerprint(realm)> | <fingerprint(issuer):
attributes    := { _np.partner_fp: nfp, <mx properties>, <?user suppli
public_key    := <pk(identity)>
signature     := <signature of above fields excluding attributes>
signature_ext := <signature of all above fields>
```

What is an Intent Token?

Disposable Yet Official Identities

- a user has a mean to generate, control and use pseudonyms for different purposes

```
realm          := <empty> | <fingerprint(realm)>
issuer         := <ifp>
subject        := 'urn:np:sub:'<hash(subject)>
audience       := <empty> | <fingerprint(realm)> | <fingerprint(issuer):
attributes     := { _np.partner_fp: nfp, <mx properties>, <?user suppli
public_key     := <pk(identity)>
signature      := <signature of above fields excluding attributes>
signature_ext := <signature of all above fields>
```

Allows the classification of different transport layer types

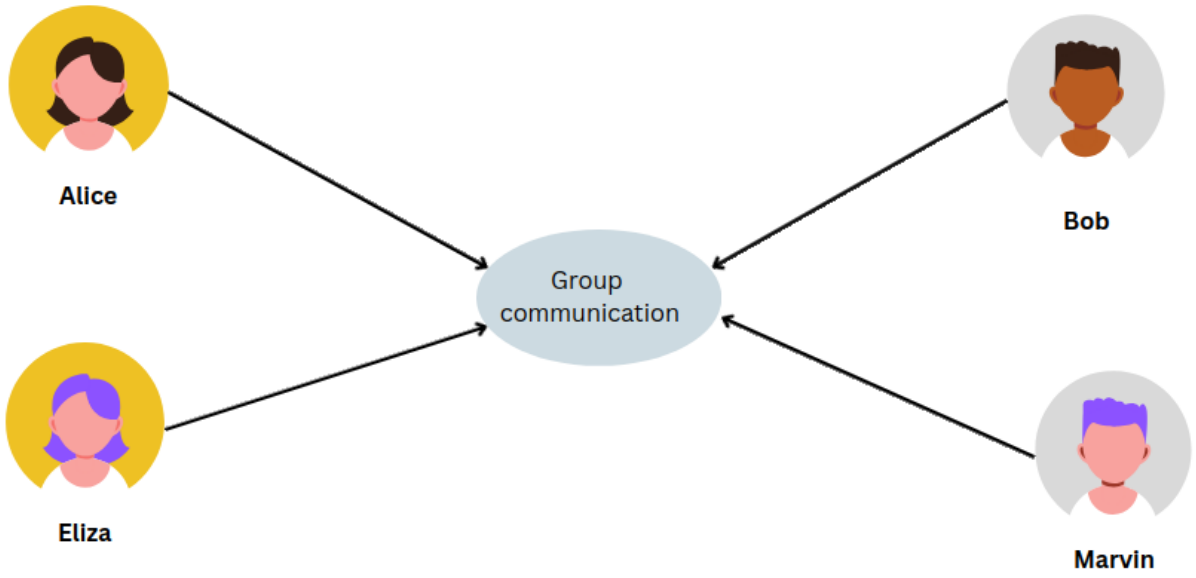
- Virtual: only token exchange happens
- Public: anybody may connect (API / interface)
- Protected: Limit access to AudienceId
- Private: Combined with FP(Alice) creates data channels for single systems

Group Communication

Through message intent token Alice, Bob, Eliza and Marvin are connected in group communication with dedicated data channel.

As a result:

- They establish a secured communication maintaining their privacy.
- During group communication, Alice and Bob can generate new E2E communication sessions since MIT represents a digital identity

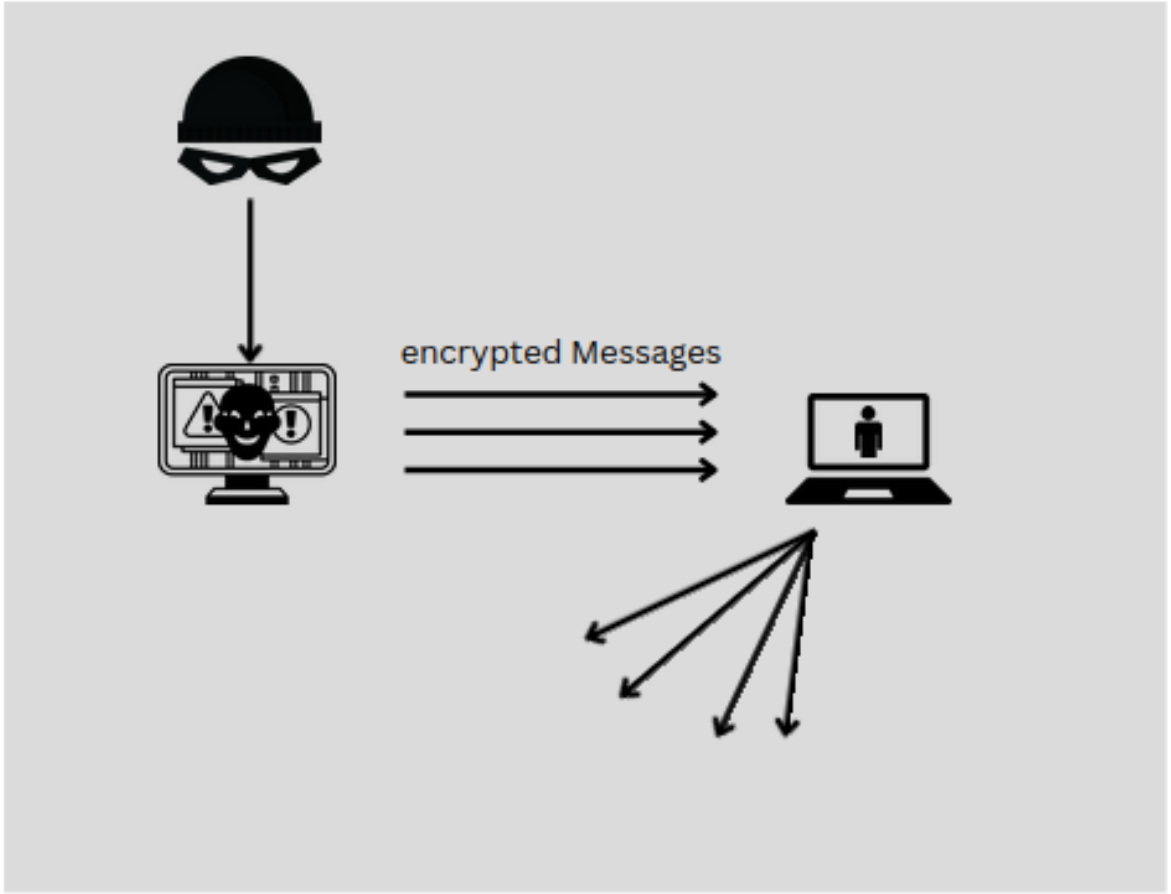


Confidentiality ? Solved ...

Malware Risks

By allowing direct addressing and arbitrary content, attackers can send malware, trojans, etc.

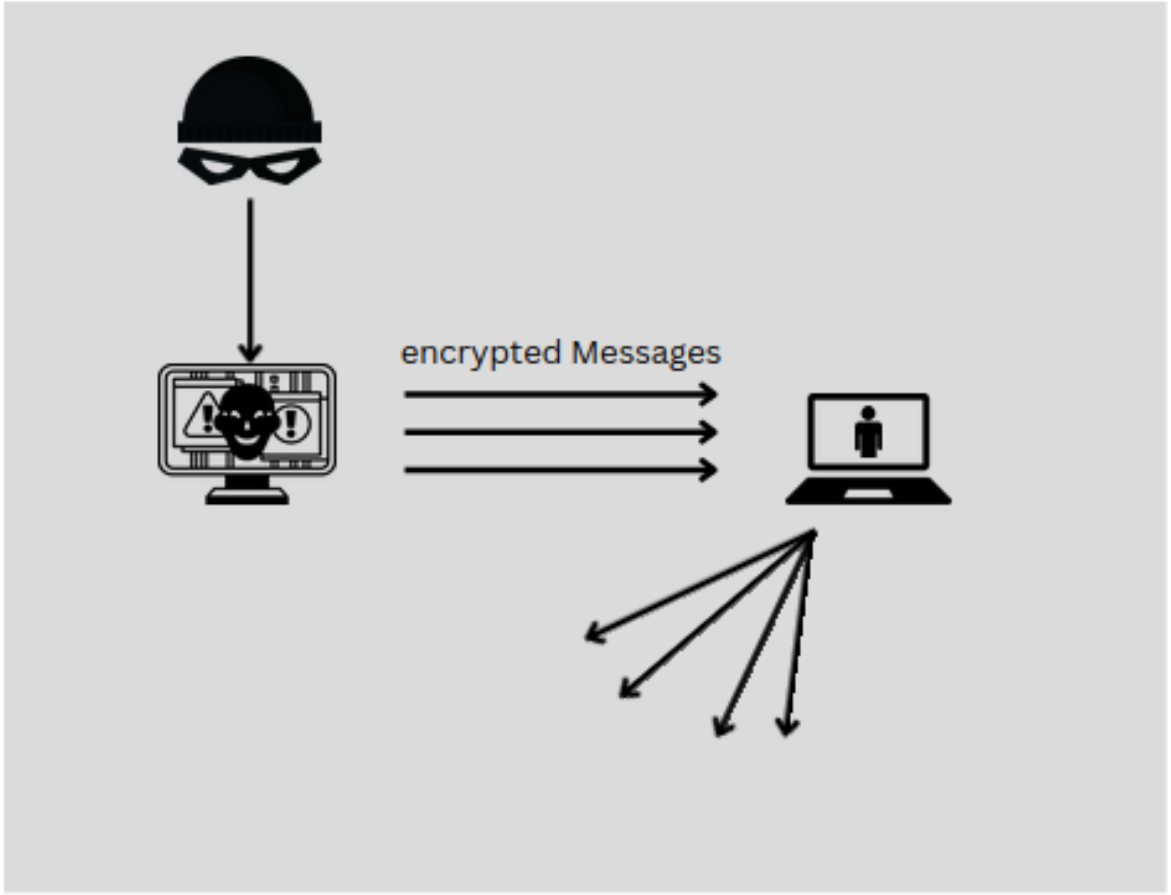
- Because of random identities simply sending is not possible, there is no direct addressing anymore
- Because of Intent Token: It is almost impossible cause attacker will visible
- Because of Intent Token: Each data channel can have strict validation and malware prevention



DoS attack

The goal of a denial-of-service (DoS) assault is to overload a targeted network with so many unauthorized requests that it is unable to function normally.

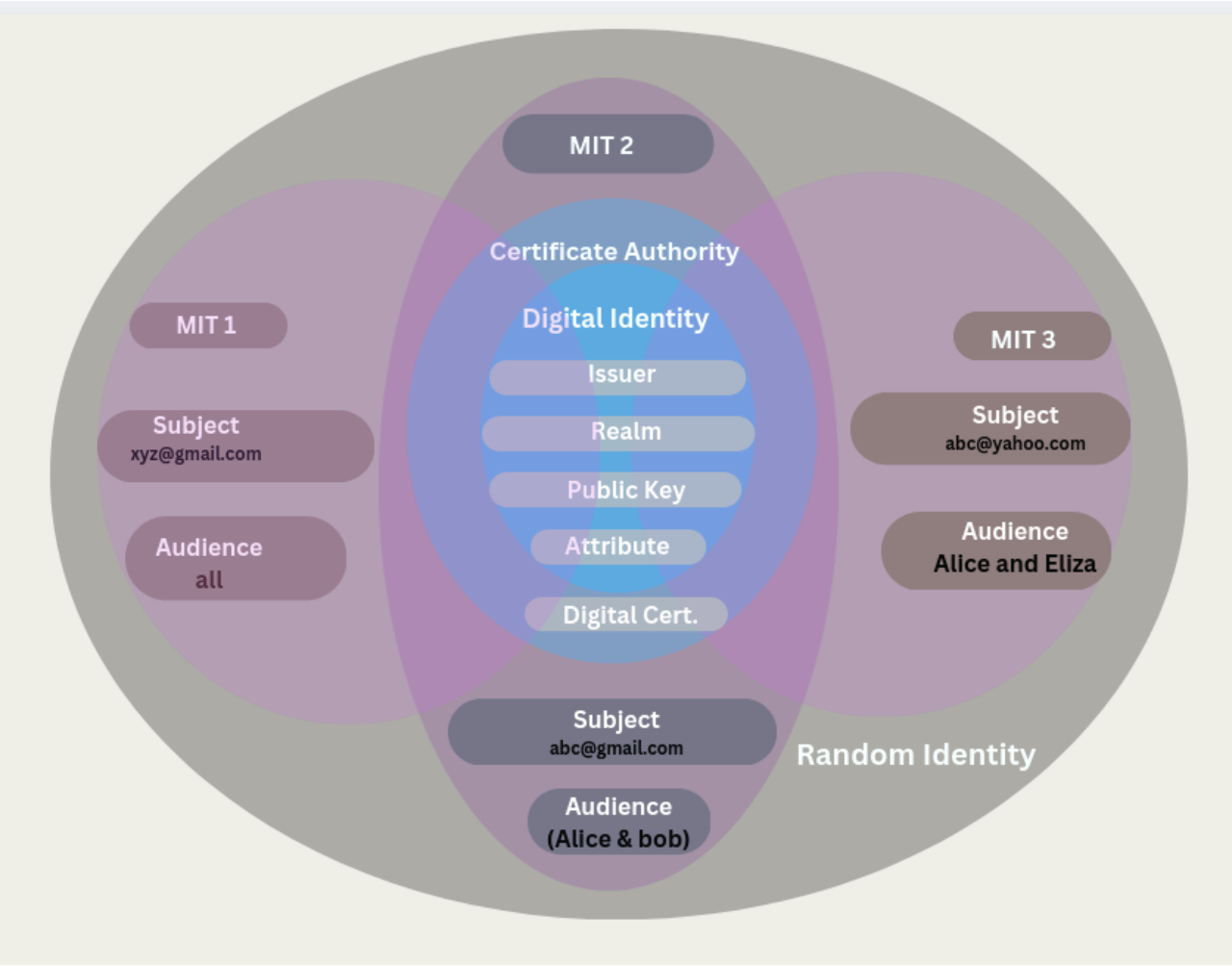
- Because of random identities simply attacking is not possible
- Because of Intent Token: almost impossible, attacker will be visible and unauthorized content will be discarded
- Because of Intent Token: almost impossible, unauthorized content will be discarded
- No Spam anymore :-)



User Identity

to use the cybersecurity mesh as a user:

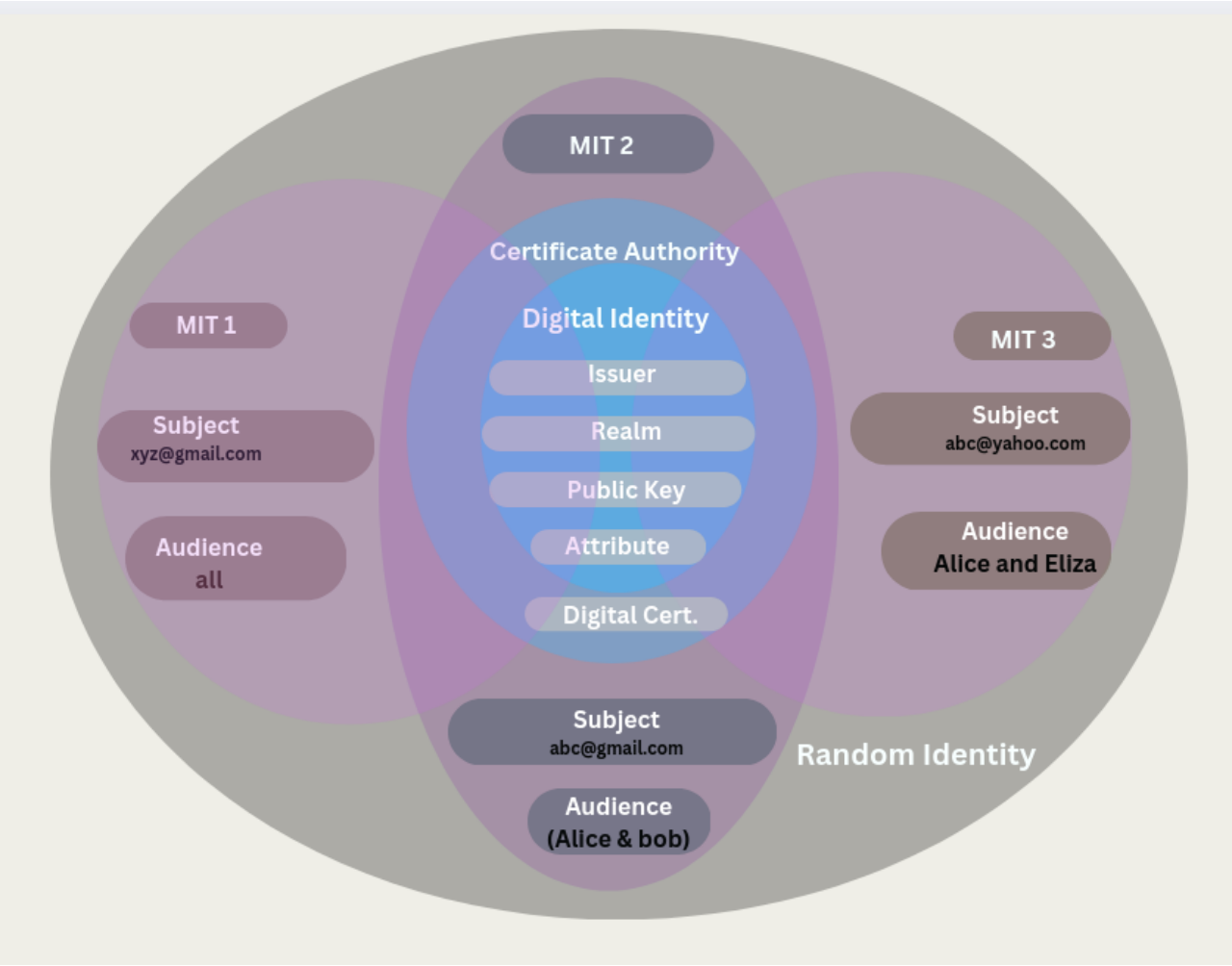
- for issuing digital certificate, create your personal CA
- derive additional digital identities
  - use your company fingerprint as realm
  - use your hobby group fingerprint as realm
  - use your family NPId as realm
- generating arbitrary number of dedicated channel based on intent tokens
- subscribe to other data channels with your specific intent token



Server Identity

to use the cybersecurity mesh for a server:

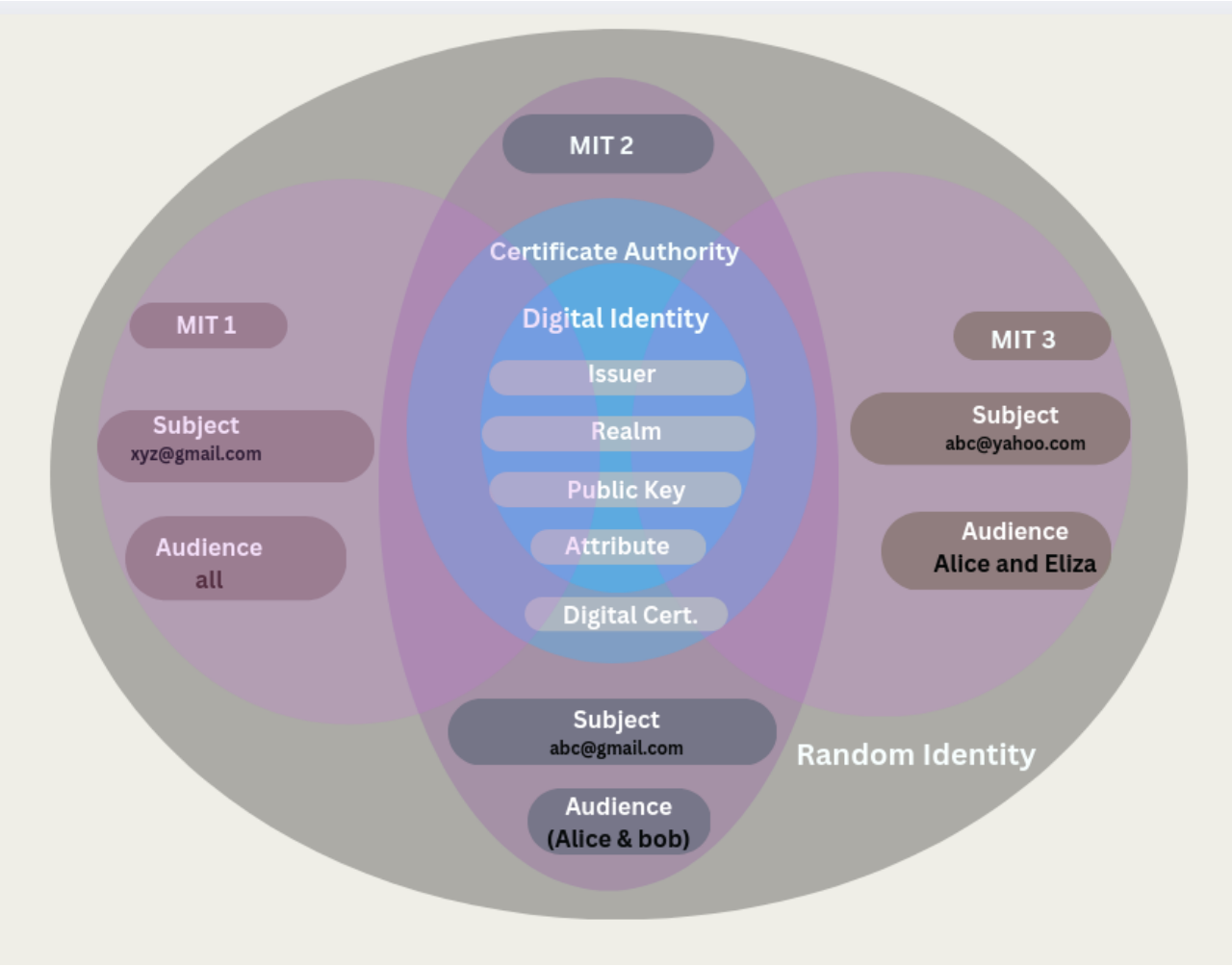
- for issuing local digital certificate, create your local CA
- derive additional digital identities
  - using own application fingerprint as realm
- create temporary SSH access with message intent token
- protect your different API with dedicated channel and message intent tokens
- no basic auth anymore :-)



Identity Provider

to use the cybersecurity mesh for an identity provider:

- for issuing digital certificate, IdP CA is created
- derive additional digital identities
  - use NPId's for different realms
- allow clients to register with a dedicated data channel and message intent token
- allow user to register with a dedicated data channel and message intent token
- The IdP doesn't need to store password anymore :-)

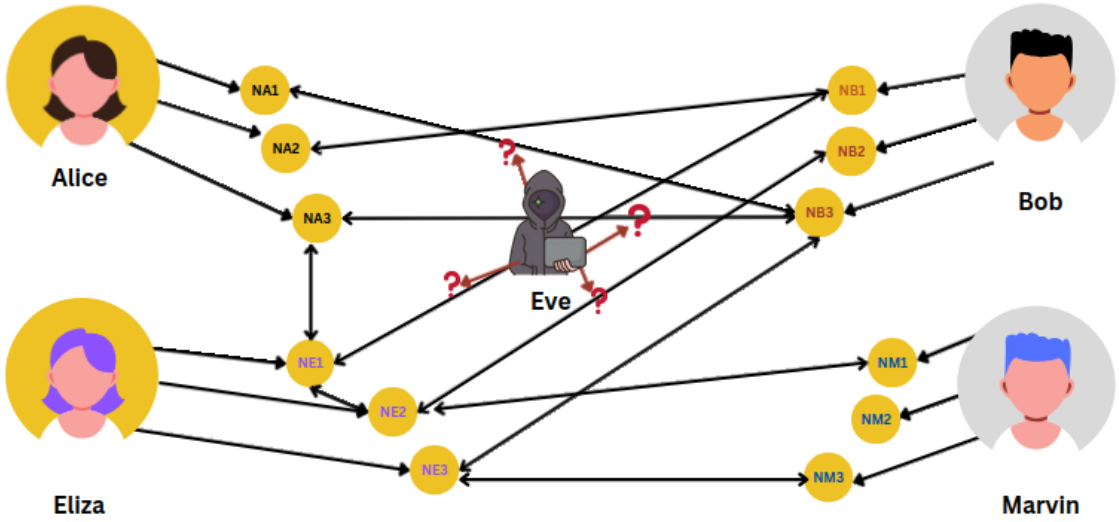


Conclusions

the neuopil cybersecurity mesh is a federated identity setup

each participant hosts its own micro PKI

federated identities is about group management



Funding


NGI
ASSURE


NGI
ZERO


open collective


FLUIDOS


pi-lar GmbH
Shaping
Digital
Environments

Thank you

Questions ?

https://www.neuropil.org

https://www.neuropil.io

https://gitlab.com/pi-lar/neuropil

https://gitlab.com/pi-lar/neuropil-k8s