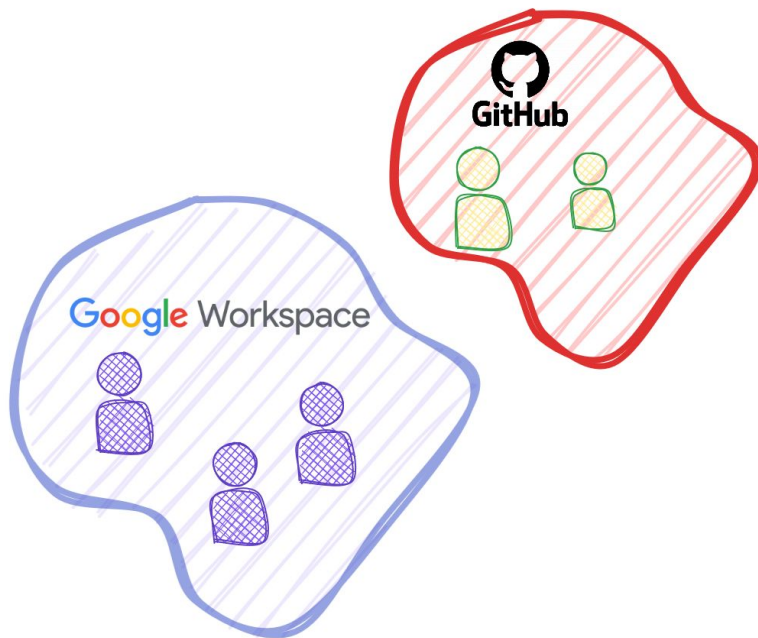# Message Layer Security (MLS) Web API proposal

Anna Weine
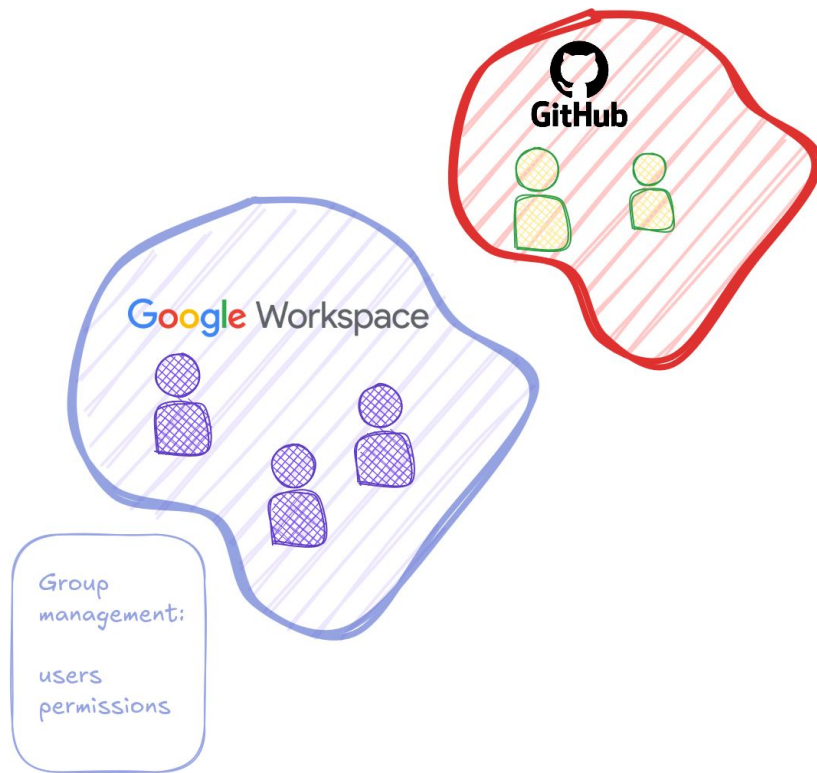
Web-Based Apps and Group Functionality

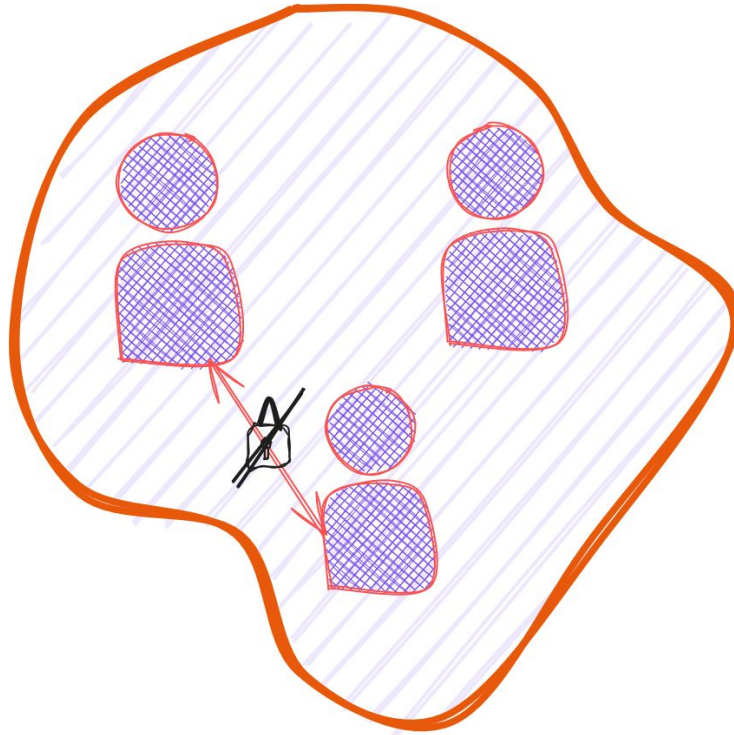# Web-Based Apps and Group Functionality

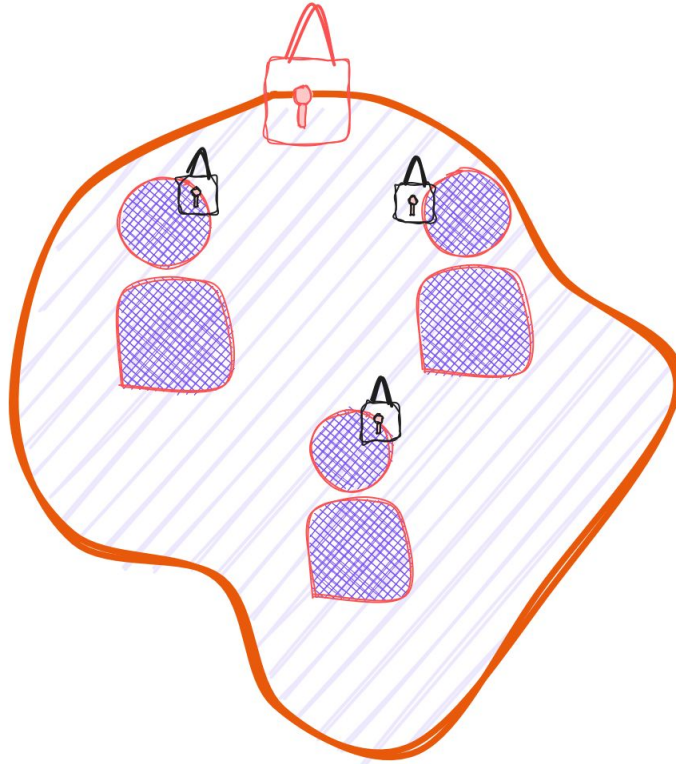# Web-Based Apps and Group Functionality

Web-Based Apps and Group Functionality
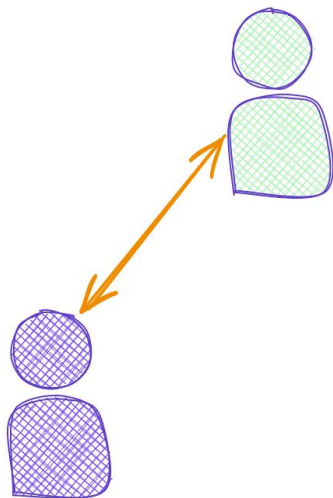
Web-Based Apps and Absence of E2E

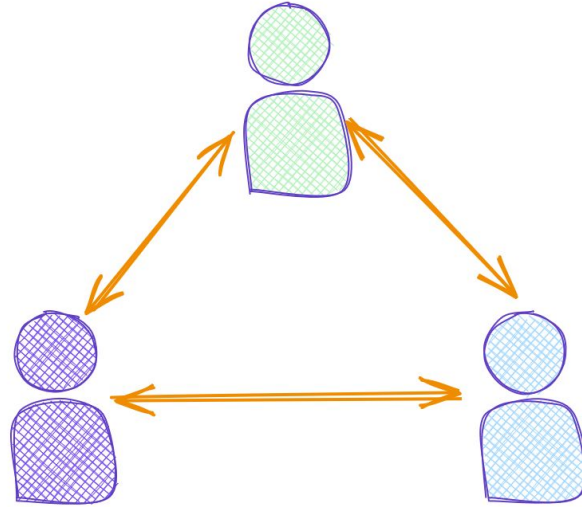# Web-Based Apps and Ideal Future
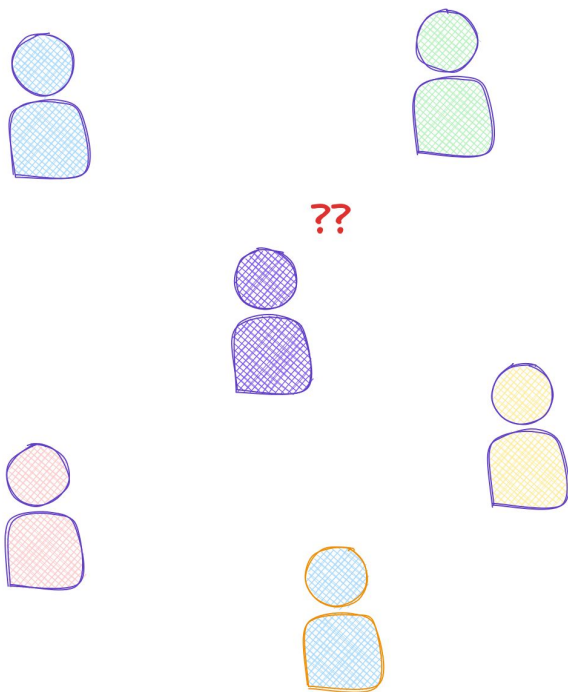
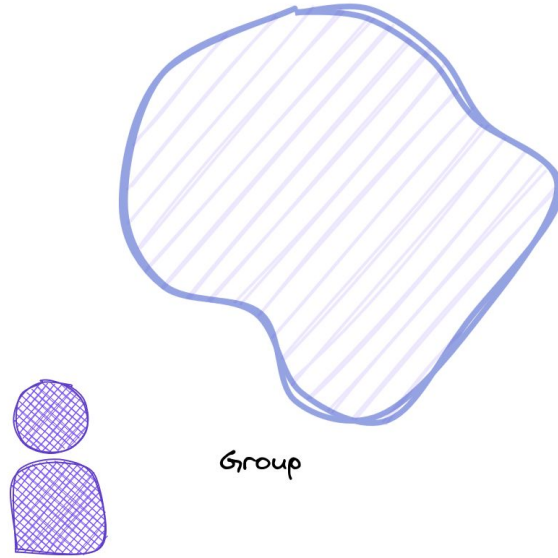# What's MLS and why do we care?

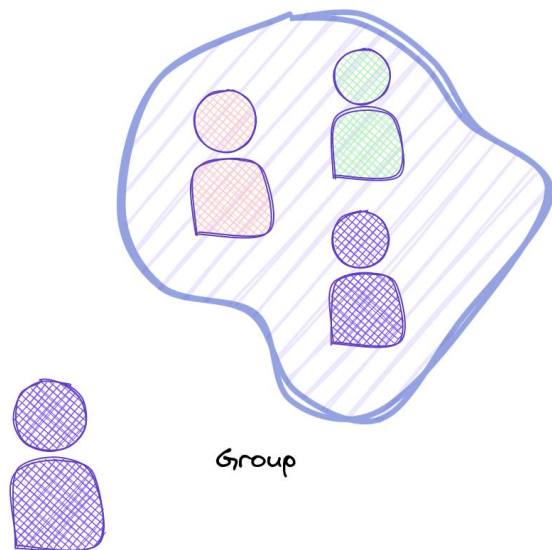# Traditional E2E communication

Traditional E2E communication

Traditional E2E communication

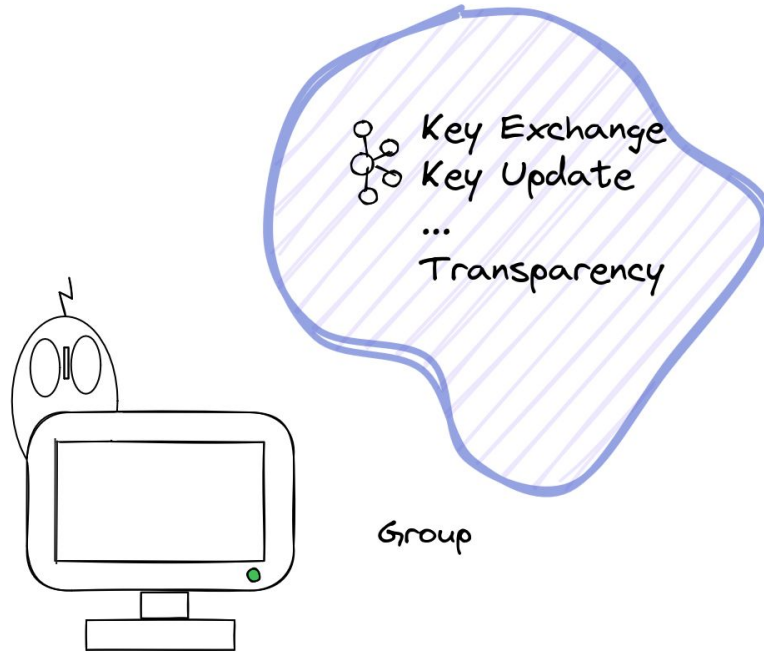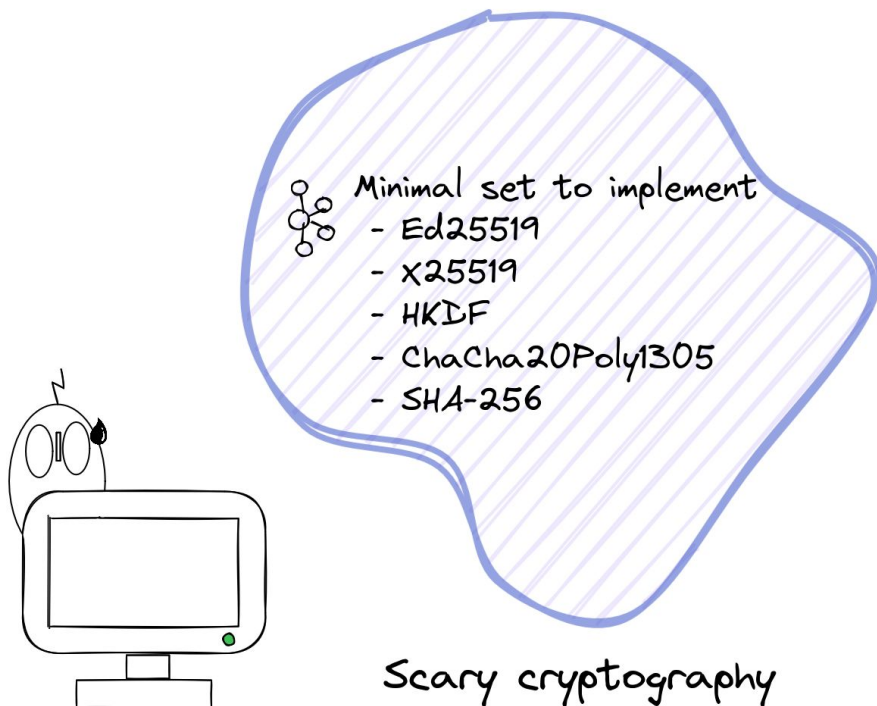# MLS solves this problem!

Group

MLS solves this problem!

Group

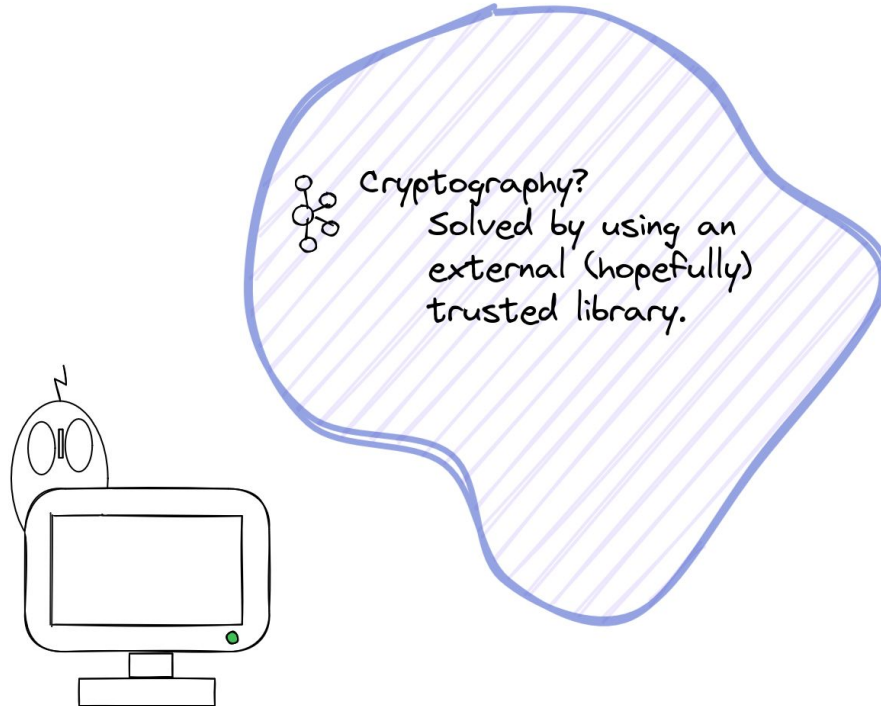# What's left is to implement

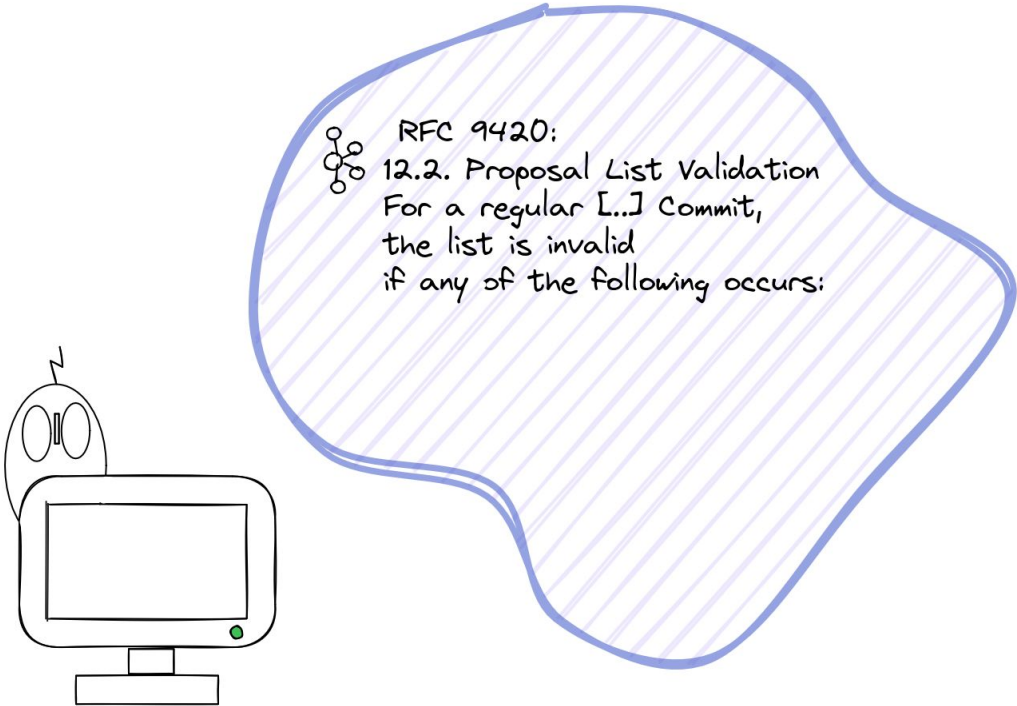# From the developer point of view - Challenge

From the developer point of view

Minimal set to implement
- Ed25519
- X25519
- HKDF
- ChaCha20Poly1305
- SHA-256

Scary cryptography

From the developer point of view

Cryptography?
Solved by using an
external (hopefully)
trusted library.

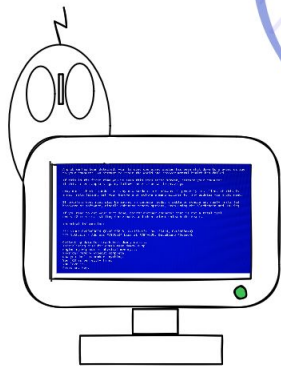# From the developer point of view

RFC 9420:
12.2. Proposal List Validation
For a regular [..] Commit,
the list is invalid
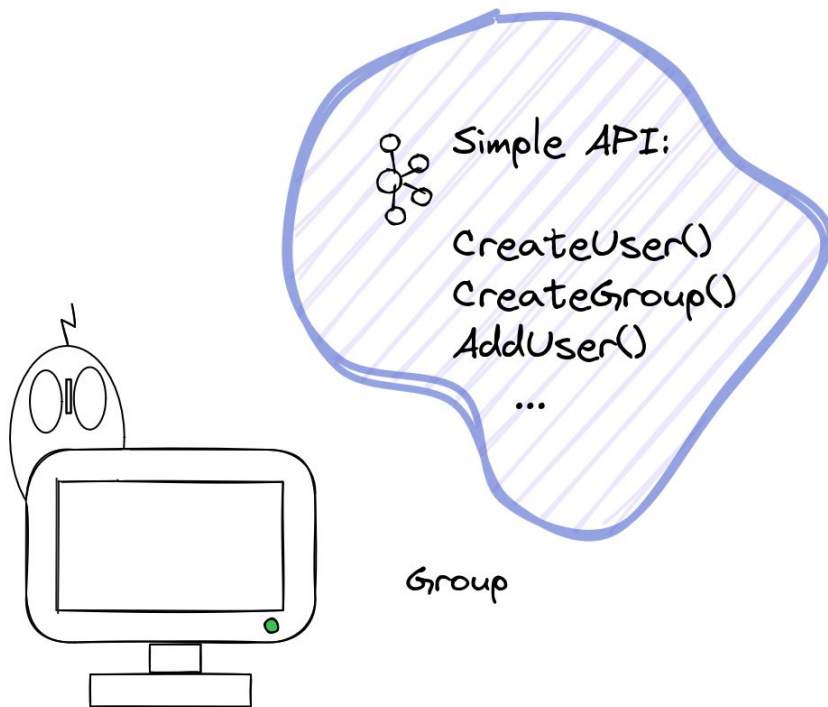if any of the following occurs:

From the developer point of view

RFC 9420:
12.2. Proposal List Validation
For a regular [..] Commit,
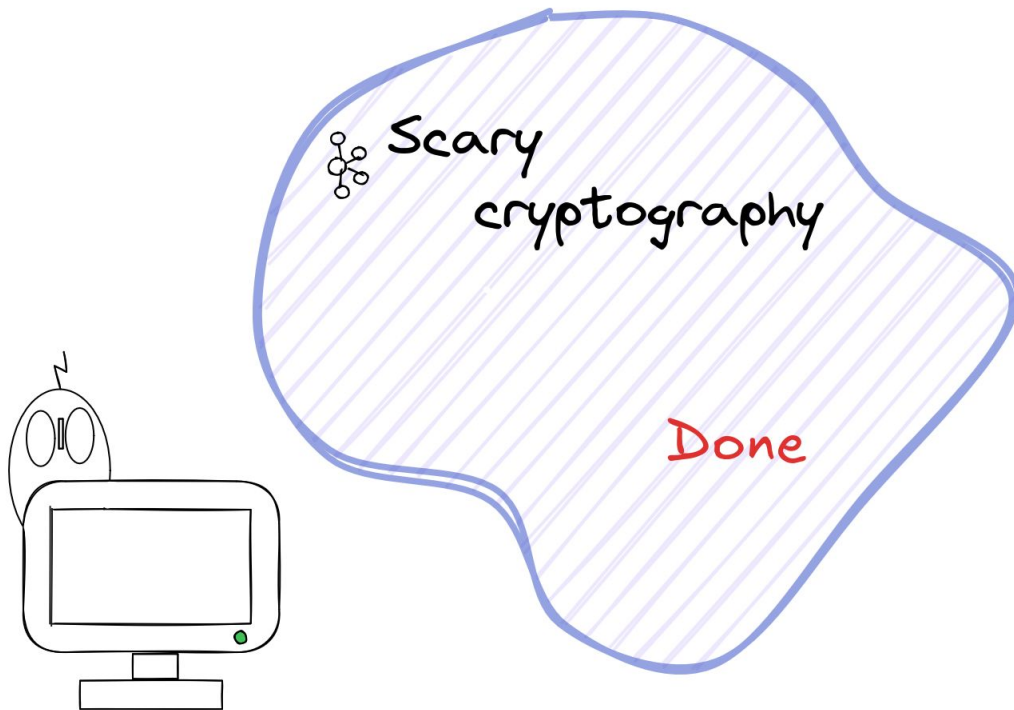the list is invalid
if any of the following occurs:
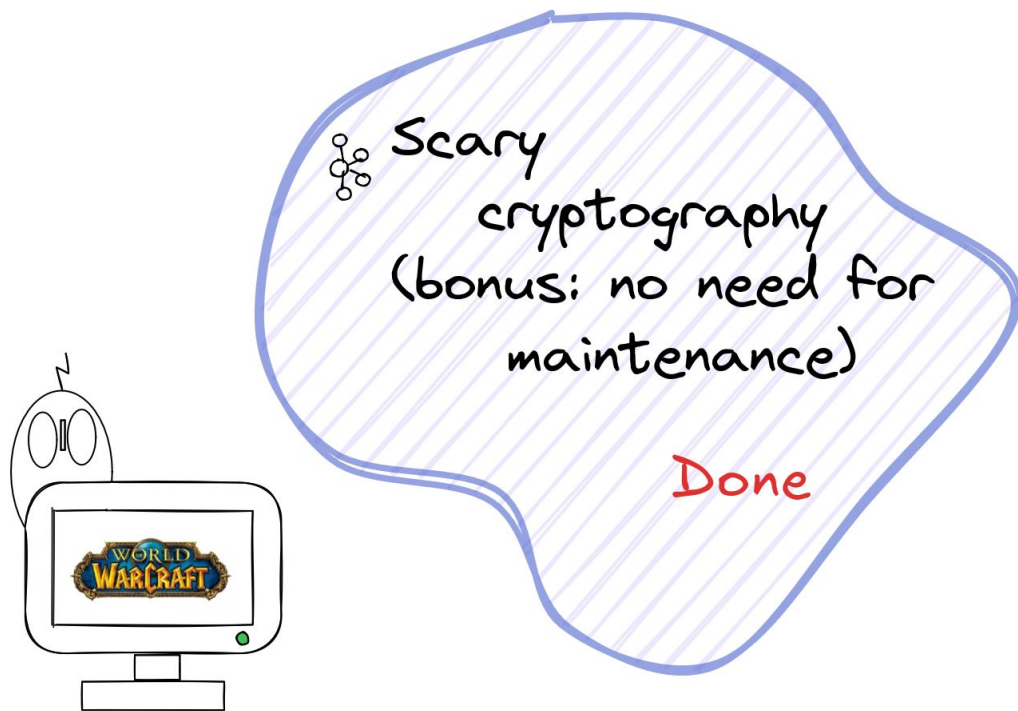
12 STEPS

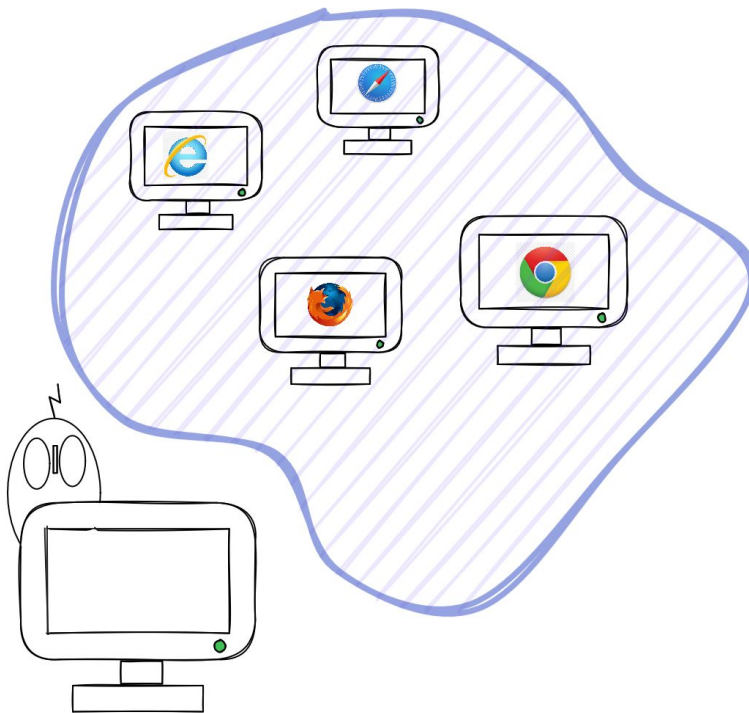# MLS WebAPI

MLS WebAPI from the PoV of a developer

No need to implement complicated cryptography

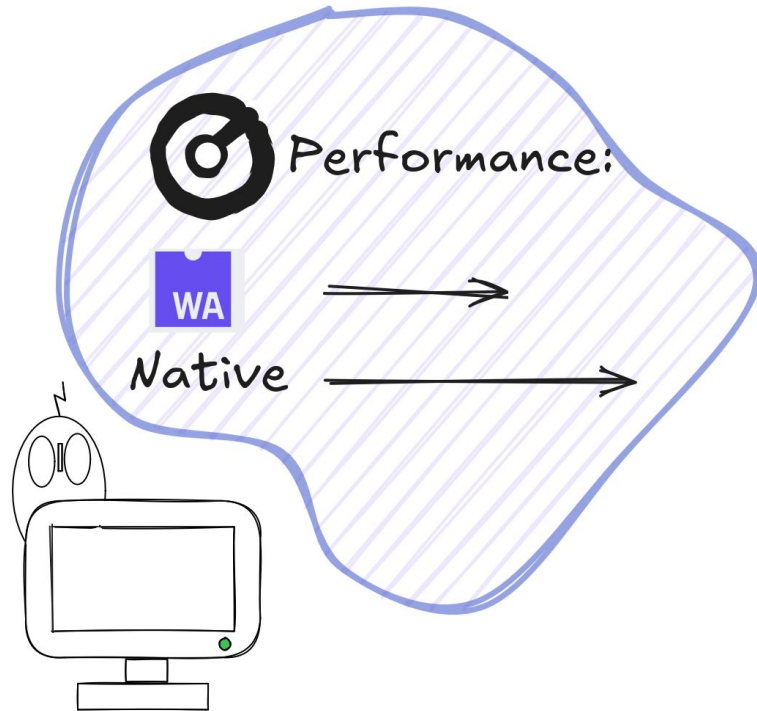# No external cryptography providers
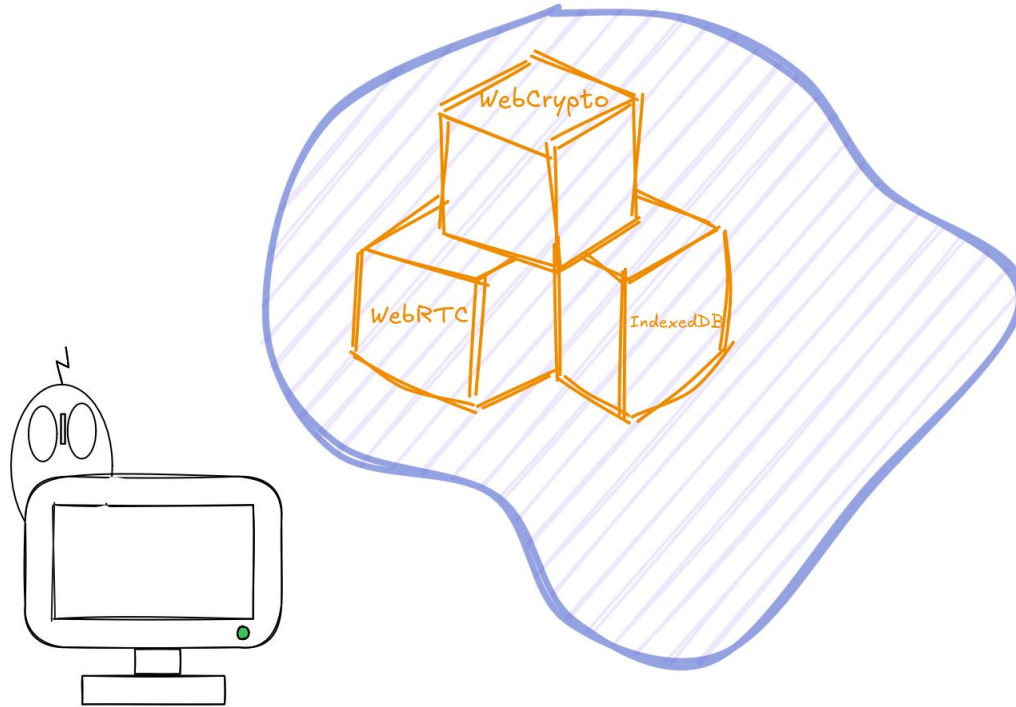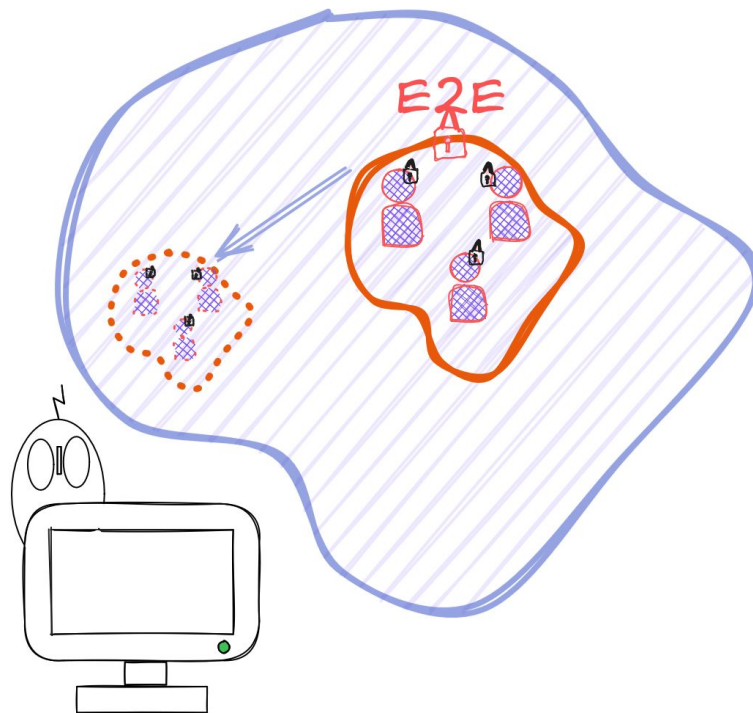
One API to rule them all

Native code and its benefits
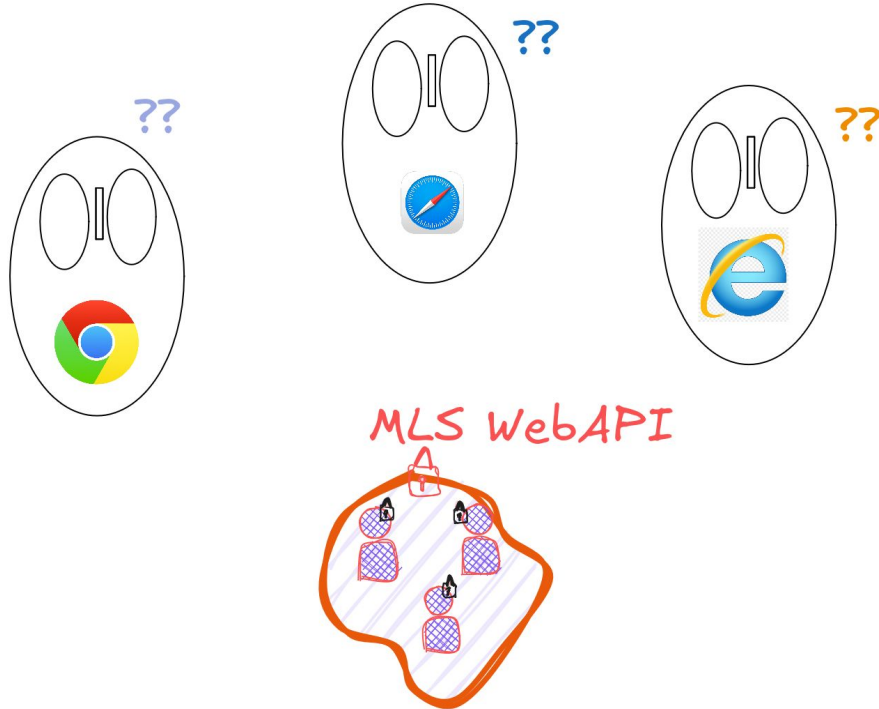
Native code and its benefits
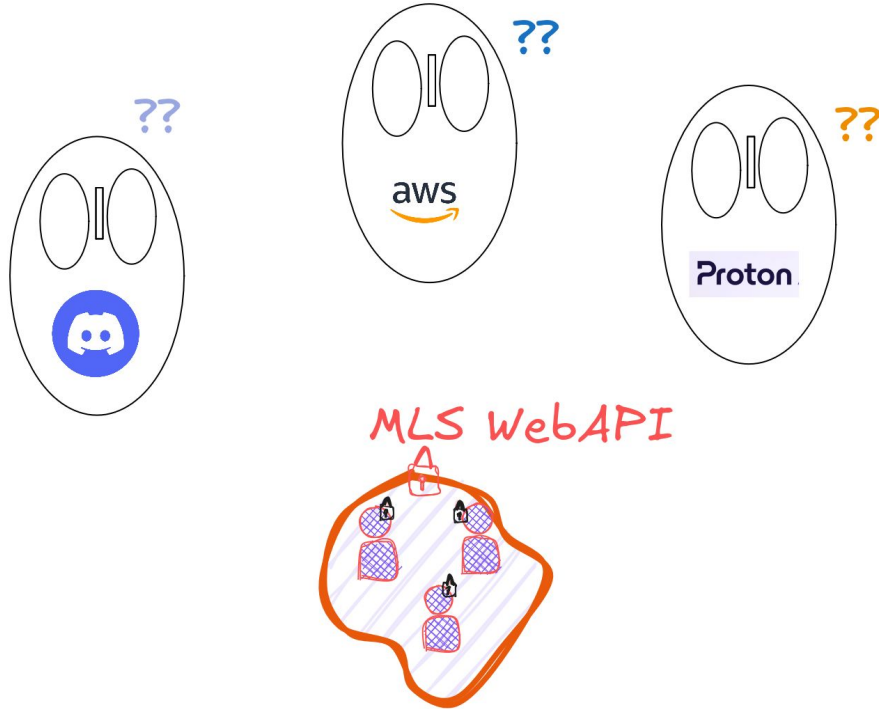
Browser-enabled transparency

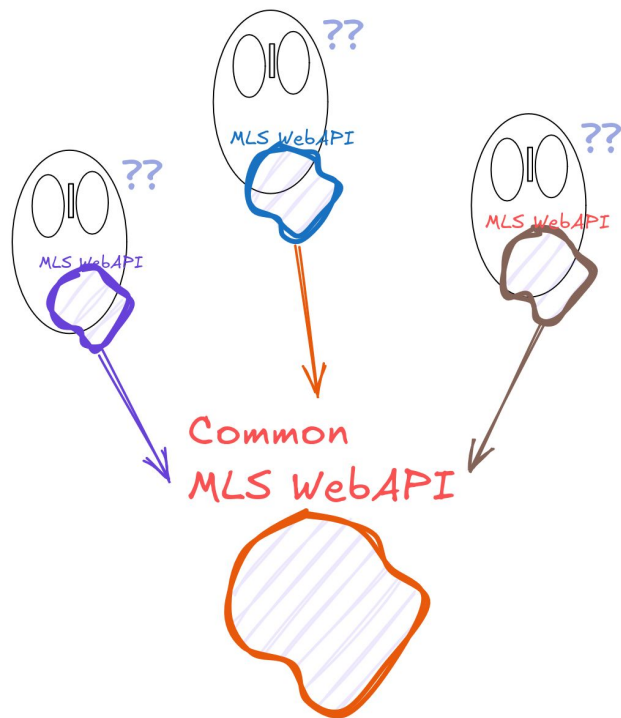We might have an idea, but there is still a lot of open questions…

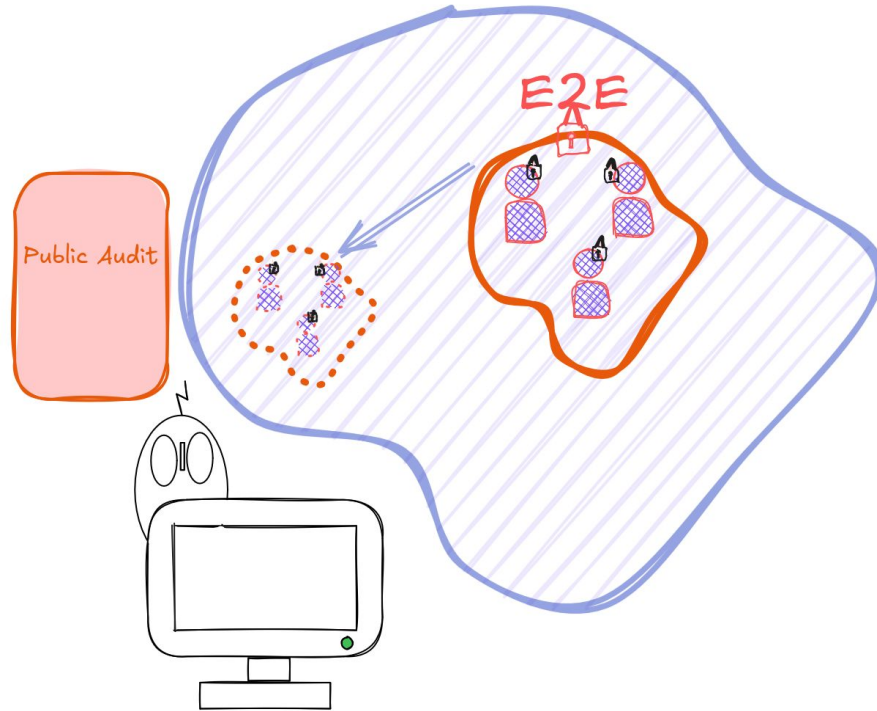# Interest from the browsers/developers?

Interest from the browsers/developers?

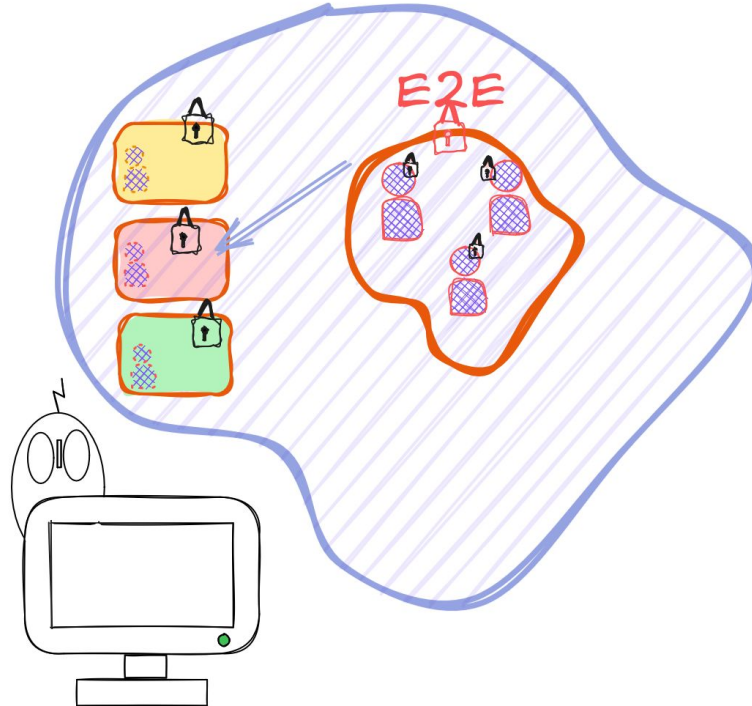# The Core MLS WebAPI, who wants what?

Browser role in group transparency

Partitioning and storage in the browser

MLS Web API proposal

Questions/Suggestions are welcome!