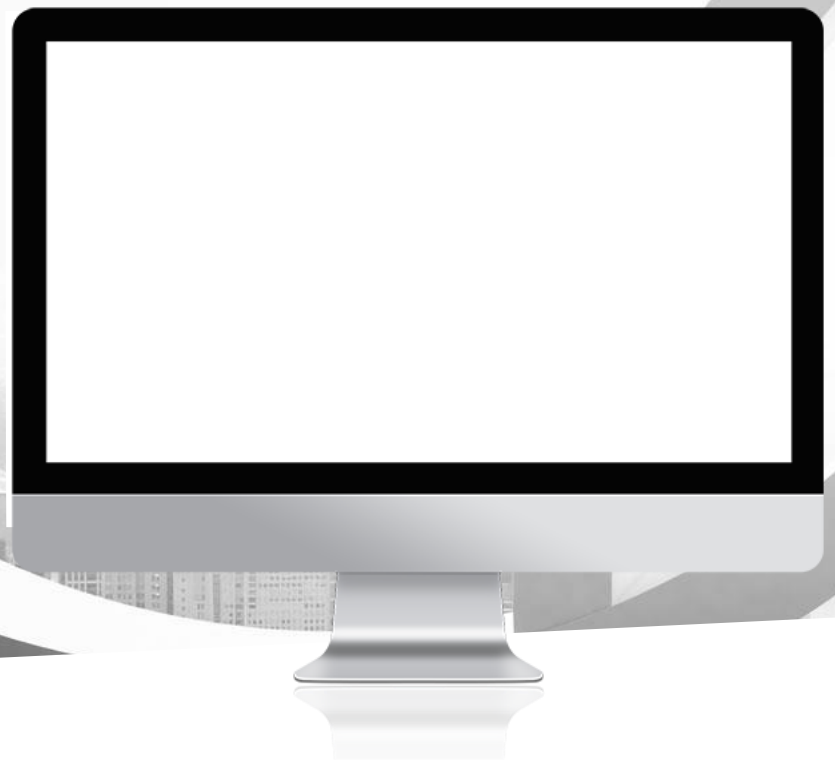
Share

Save

Sign



FIRST DAY AT OODRIVE

FRANCE - BELGIUM - GERMANY - HONG KONG - SPAIN - SWITZERLAND - BRAZIL

oodrive
LEADING BY TRUST

DAY'S PLAN

09:00	INTRODUCTION
10:00	WORKING
13:00	LUNCH BREAK
14:00	WORKING
15:30	PRESENTATIONS
16:00	FEEDBACKS

1

INTRODUCTION

oodrive
LEADING BY TRUST

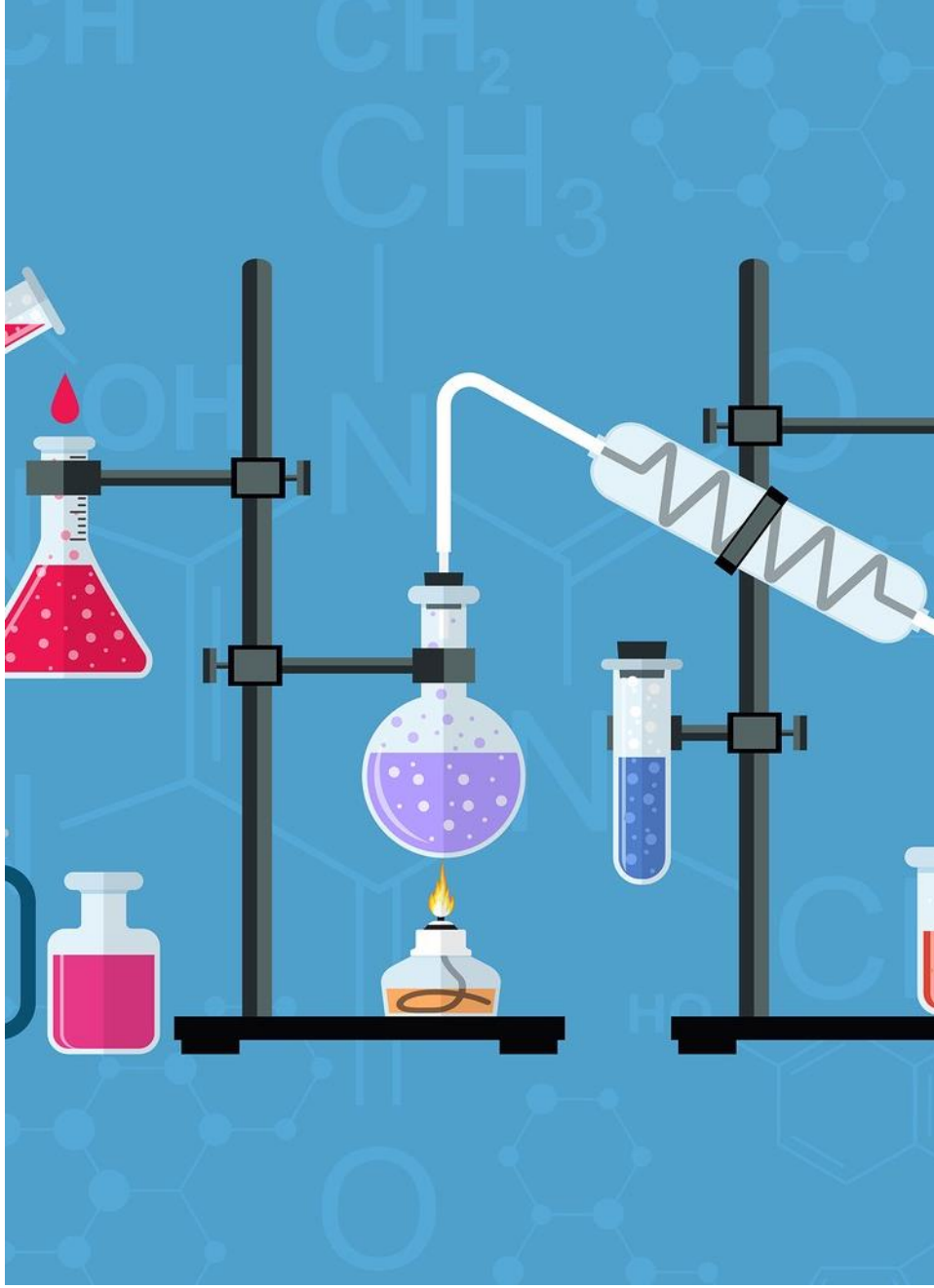
Arnaud Bellizzi
Shaman

Louis LIN
Lead dev

EXPERIMENT

First POEI with Oodrive

- Oodrive's involvement
  - Today !
  - Participation to your end project presentation
- Test Learn and Win



OBJECTIVES OF THE DAY

What are we expecting today?

Real-life situations

- Projects close to what we have at Oodrive
- Small teams working together for a common goal

First look as a developer

- Meet the developer in you

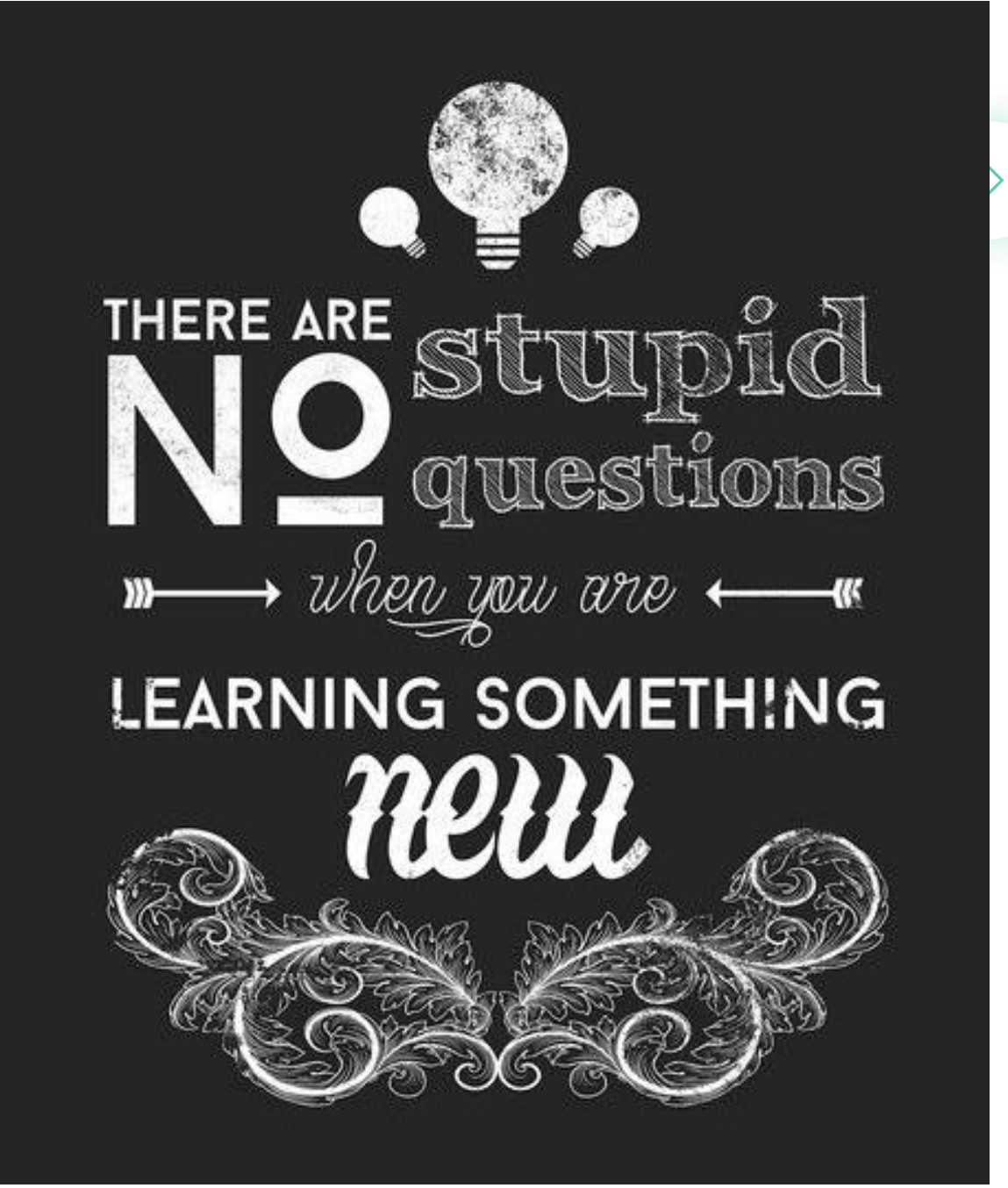
Share Oodrive's culture

- Knowledge sharing
- Helping people

FULL DISCLOSURE

Today's evaluation

- First look at your developer's side
  - How do you work as a team?
  - How do you tackle problems?
- Not final evaluation to join Oodrive



MINDSET

- Ask questions!

MINDSET

- Ask questions!
- Projects are HARD on purpose
  - They are not meant to be finished

MINDSET

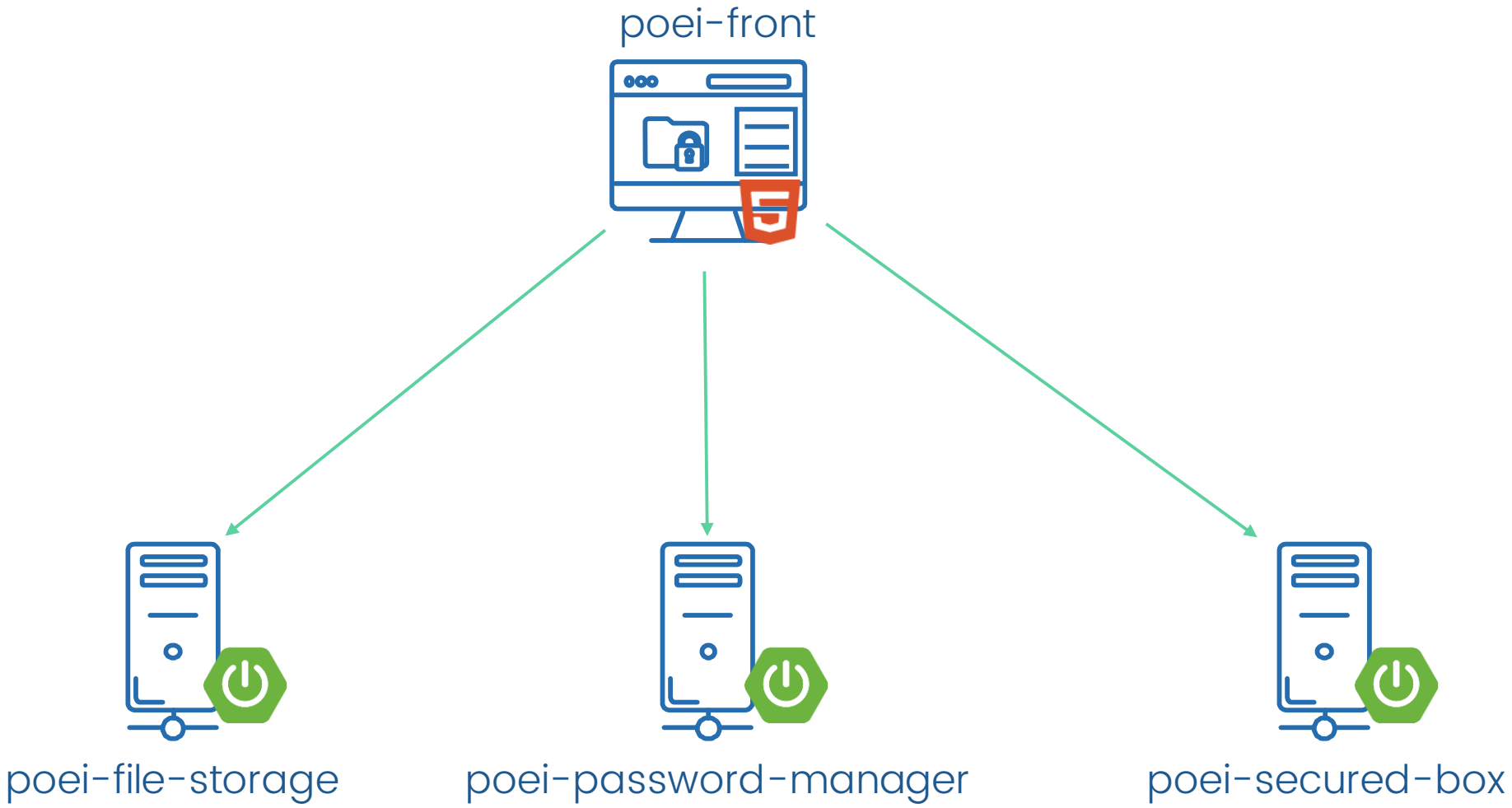
- Ask questions!
- Projects are HARD on purpose
  - They are not meant to be finished
- No competition!
  - Work as a team
  - Share your knowledge
  - Communicate your ideas
  - Different project for each team

2

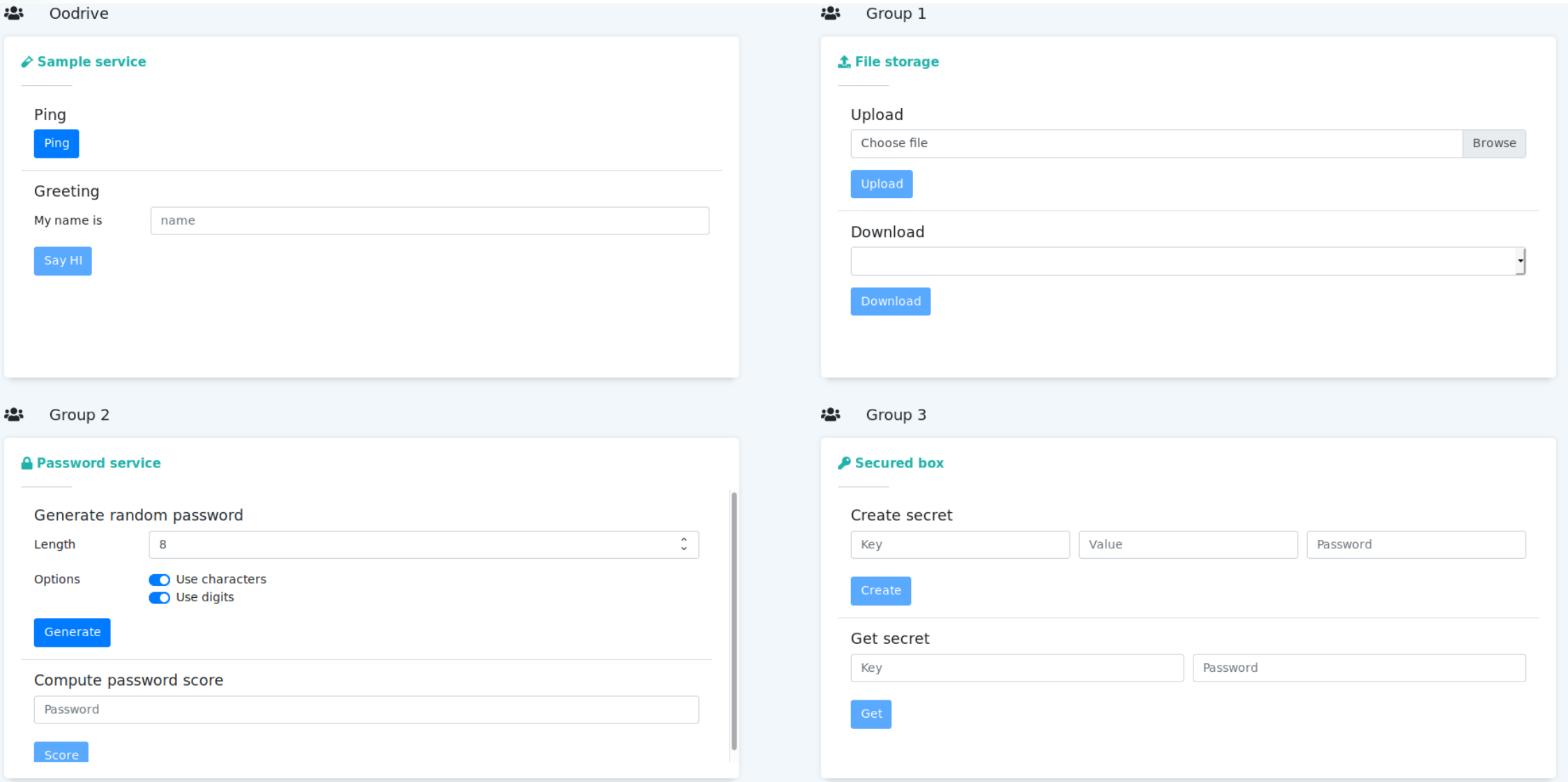
PROJECTS

oodrive
LEADING BY TRUST

POEI-DASHBOARD



POEI-DASHBOARD



POEI-FILE-STORAGE

Store files securely

Google drive

POEI-FILE-STORAGE

Store files securely

Upload

- Upload files to the server
- Save file contents to server file sytem
- Save file metadata in database

Download

- Fetch file metada
- Download file

Encrypt

- Encrypt all file contents on upload
- Decrypt file contents on download

POEI-PASSWORD-MANAGER

Generate random passwords & score passwords

';--have i been pwned?

Keepass

E2EE

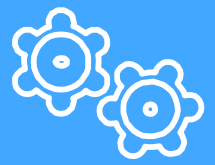
Heimdall

POEI-PASSWORD-MANAGER

Generate random passwords & score passwords

Generate

- Generate random password
- Customized password generation



Score

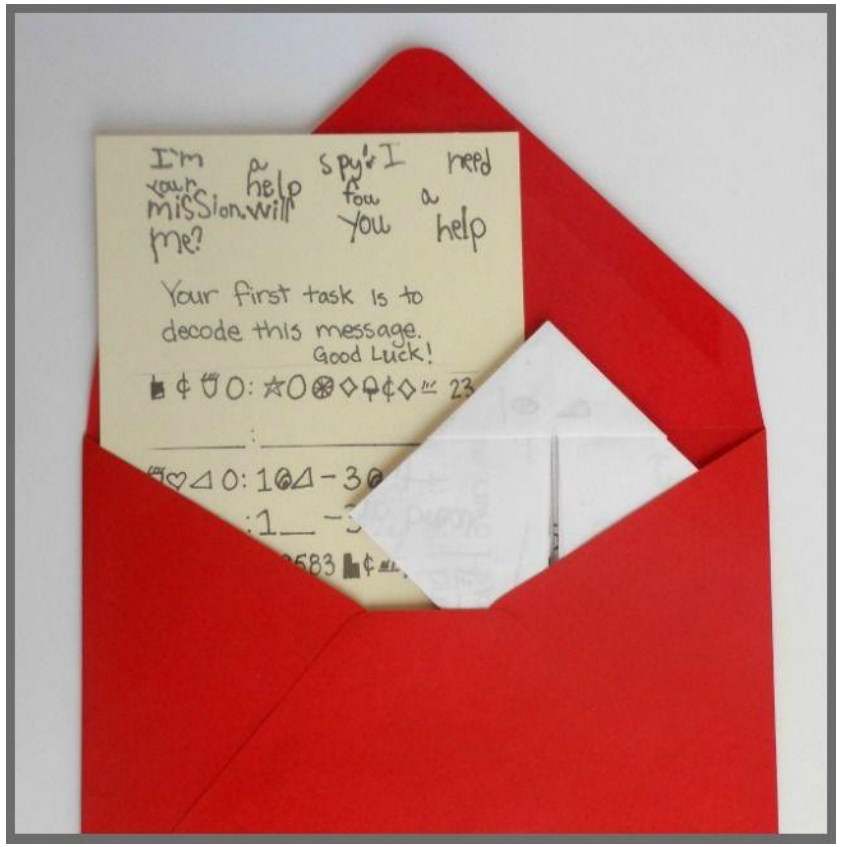
- Compute password score
- Save passwords in database

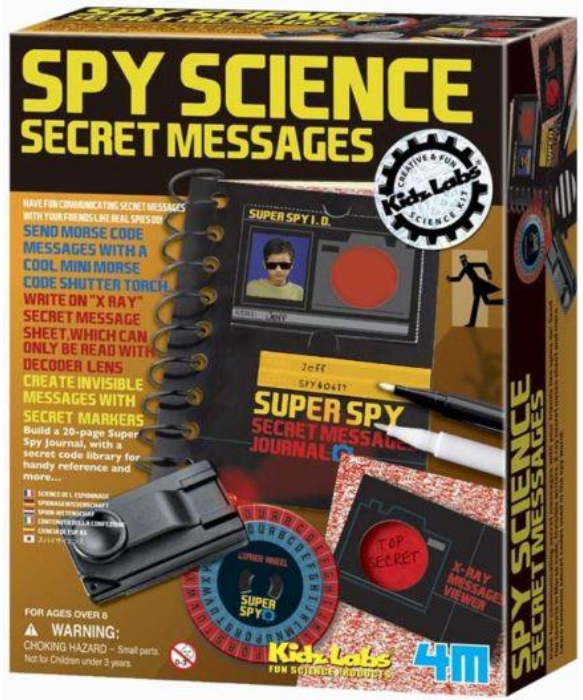
Hash

- Use password's hashes instead

POEI-SECURED-BOX

Store messages securely





POEI-SECURED-BOX

Store messages securely

Store

- Store messages mapped to a key with a password
- Save messages in the database

Fetch

- Fetch message from a given key

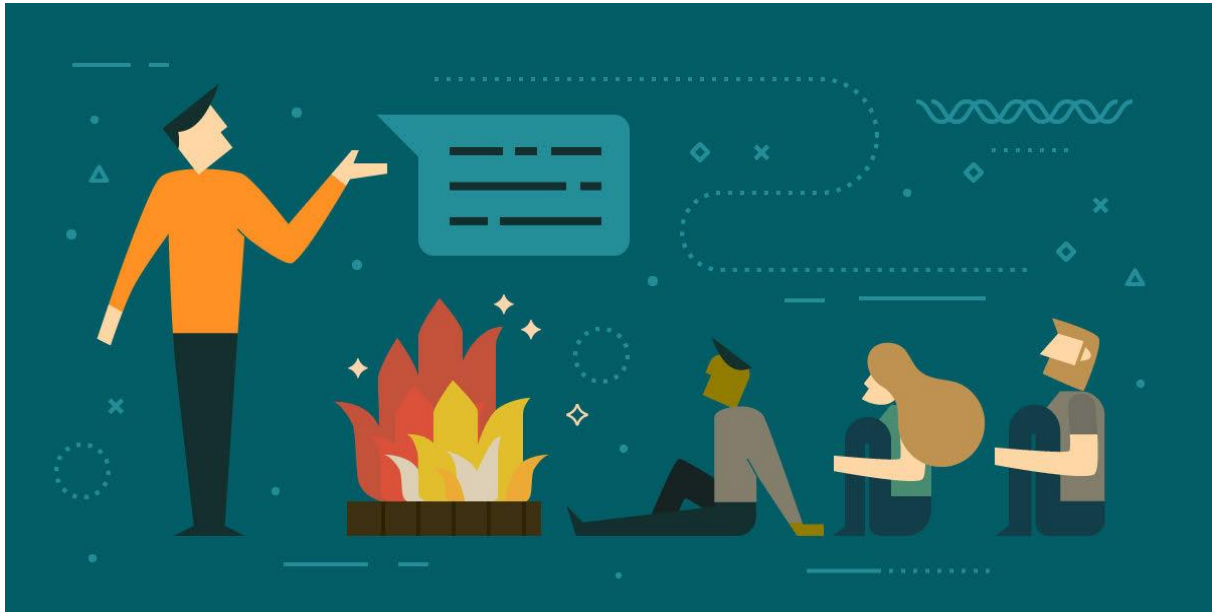
Encrypt

- Encrypt all messages using the given password
- Decrypt messages when fetching from a key

WHAT ARE WE EXPECTING FROM YOU

Projects development

5-10 minutes presentation



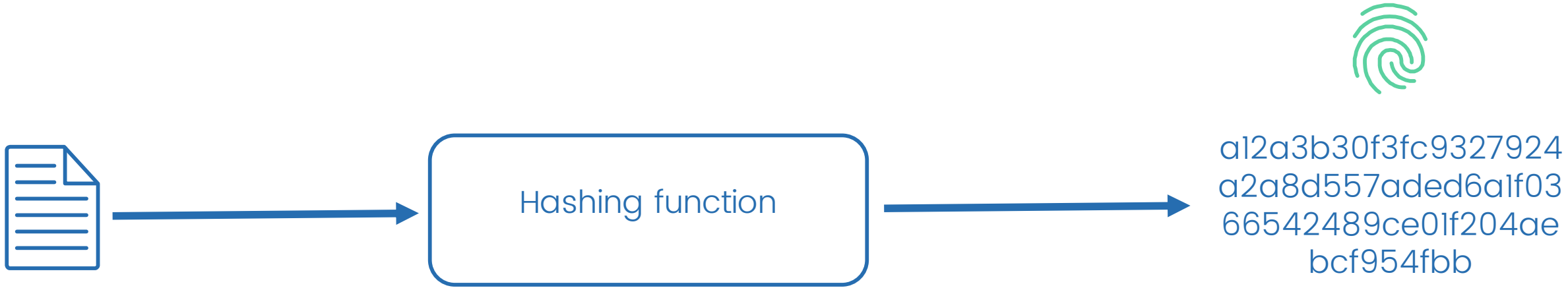
CRYPTOGRAPHY ESSENTIALS

Bring security based on cryptography to applications

Hashing

Symmetric encryption

HASHING

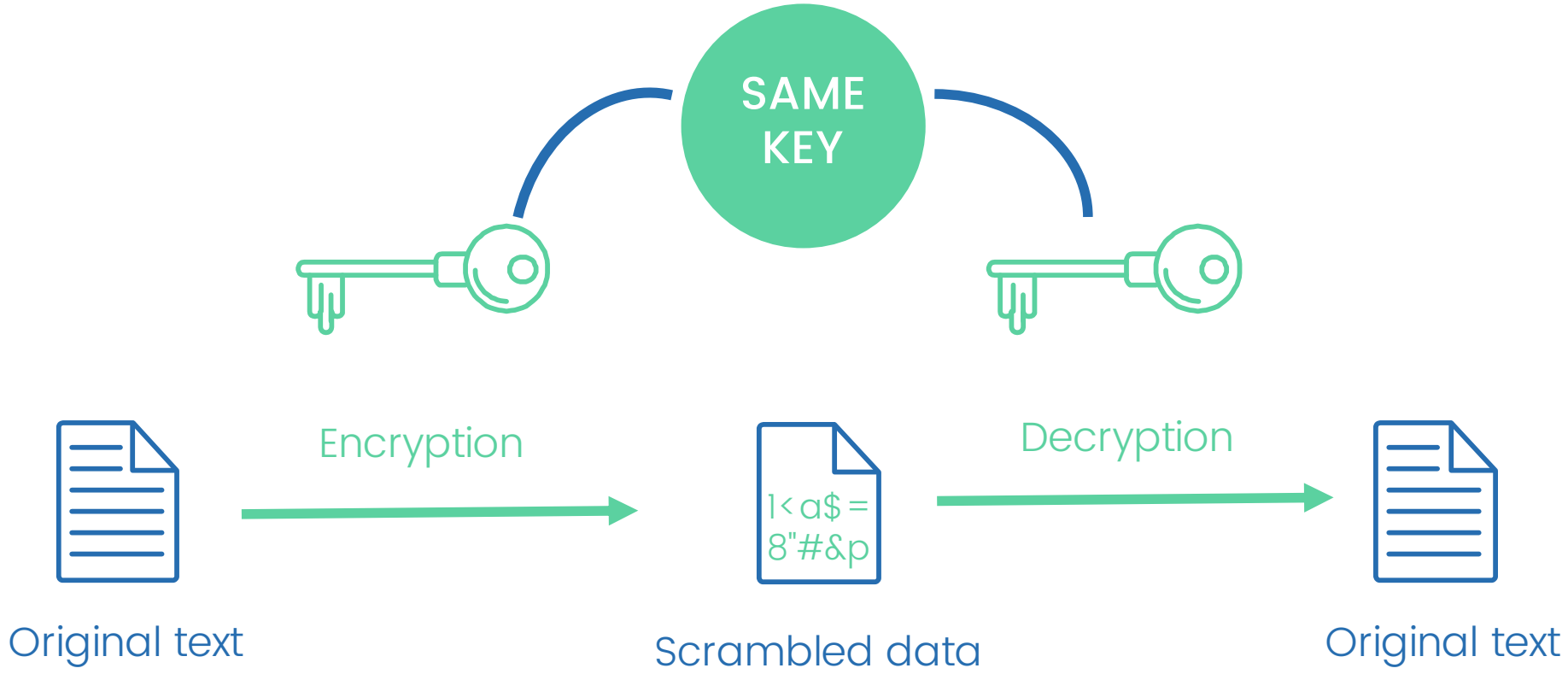


HASHING

Fingerprinting your data (password, file, …)

- Map data of arbitrary size onto data of fixed size
- Hashes are deterministic, i.e. for a given value, it must always generate the same hash
- Hashes are quick to compute for any given message
- Hashes are non-invertible, i.e. it is not realistic to reconstruct the input data from its hash alone without spending great amounts of computing time
- Well known cryptographic hash algorithms:
  - MD5: produces hash of 124 bits (16 bytes)
  - SHA-1: produces hash of 160 bits (20 bytes)
  - SHA-256: produces hash of 256 bits (32 bytes)
  - SHA-512: produces hash of 512 bits (64 bytes)

SYMMETRIC ENCRYPTION



SYMMETRIC ENCRYPTION

Encrypt data with a single shared secret

- Uses a single key for both encryption and decryption
- Industry Standard symmetric-key algorithm: AES (Advanced Encryption Standard)
  - Support encryption key in 256 bits (32 bytes)
  - Hint: Works well with SHA-256 hashes

PROJECT'S PICKS

LINK TO PROJECTS

https://github.com/oodrive/poei

YOUR TURN!