MS4: Final Presentation

Quantum Key Reconciliation Application

Team:

Diogo Marto	108298
David Cobileac	102409
Tiago Pereira	108546
Vítor Santos	107186

Orientadores:

Armando Pinto, IT

Diogo Matos, IT

Index

Context & Vision

Reconciliation

- Motive
- Requirements
- Process
- Results & Outcomes

QeeP

- Motive
- Goals
- Architecture
- Results

Conclusions

Context

> ***At the end of the day, the goals are simple:***
> ***Safety & Security***
> ***- Jodi Rell***

Context

Quantum computers represent a possible future threat for current asymmetric crypto schemes with disastrous consequences.

Quantum Key Distribution aims to solve this by using eavesdropper-proof quantum channels to exchange symmetric keys.

Reconciliation is the phase of this process that outputs useful encryption keys.

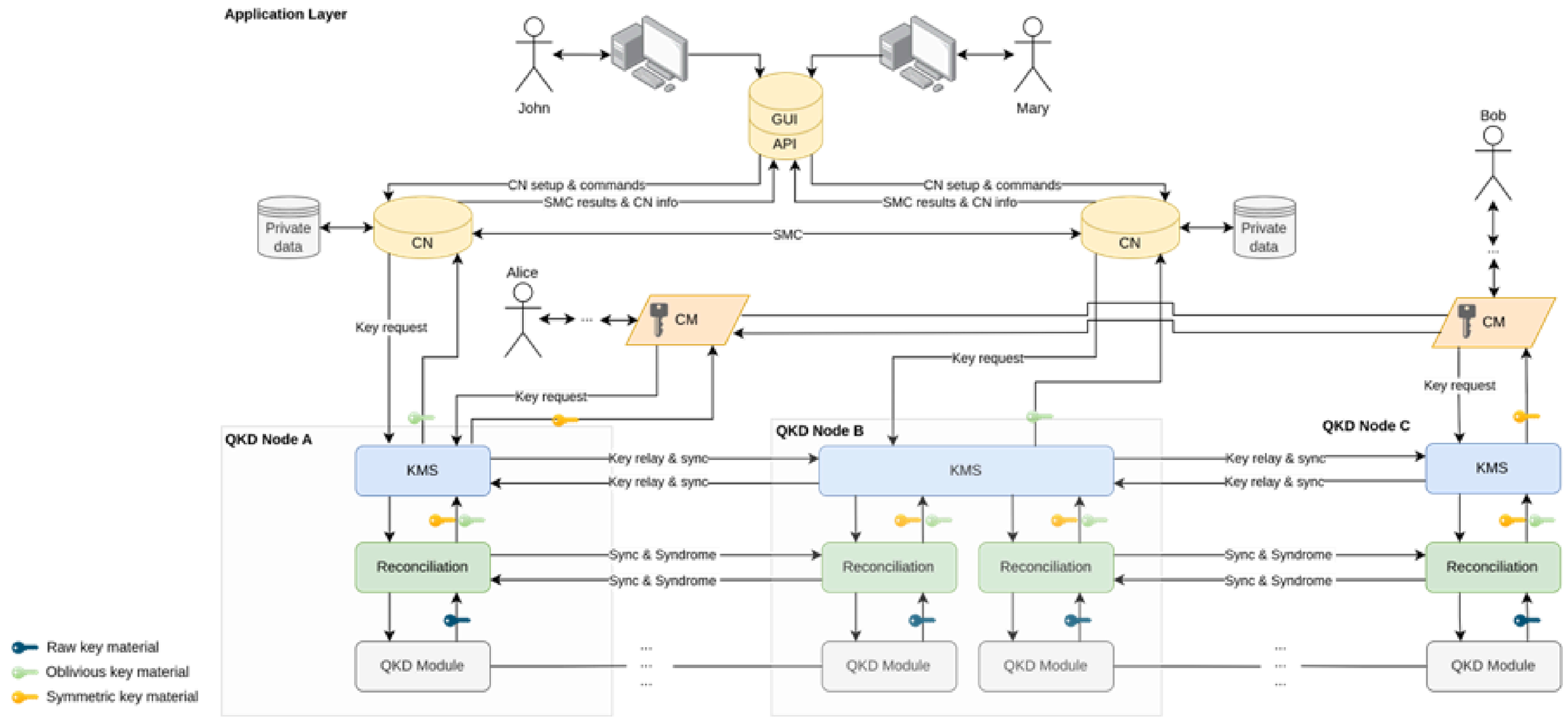
PART 1

Reconciliation

- Motive
- Requirements
- Process
- Results

Motive

SYSTEM ARCHITECTURE

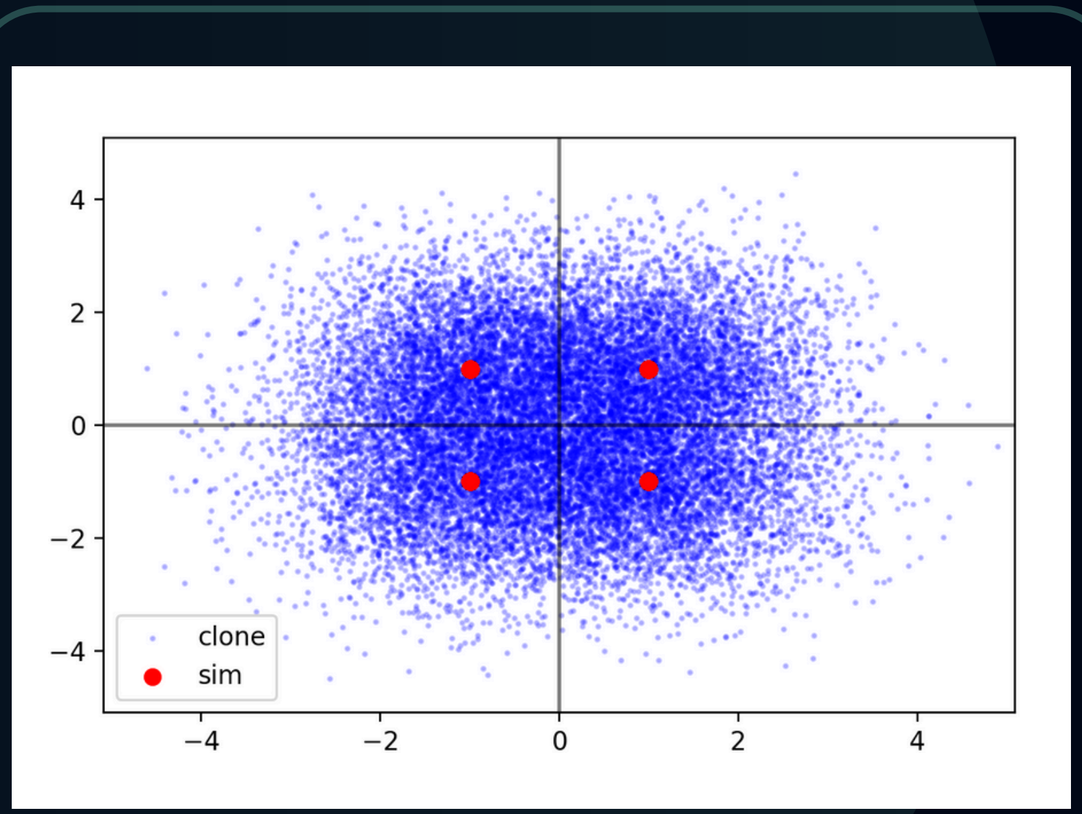


Motive

LAYER ARCHITECTURE

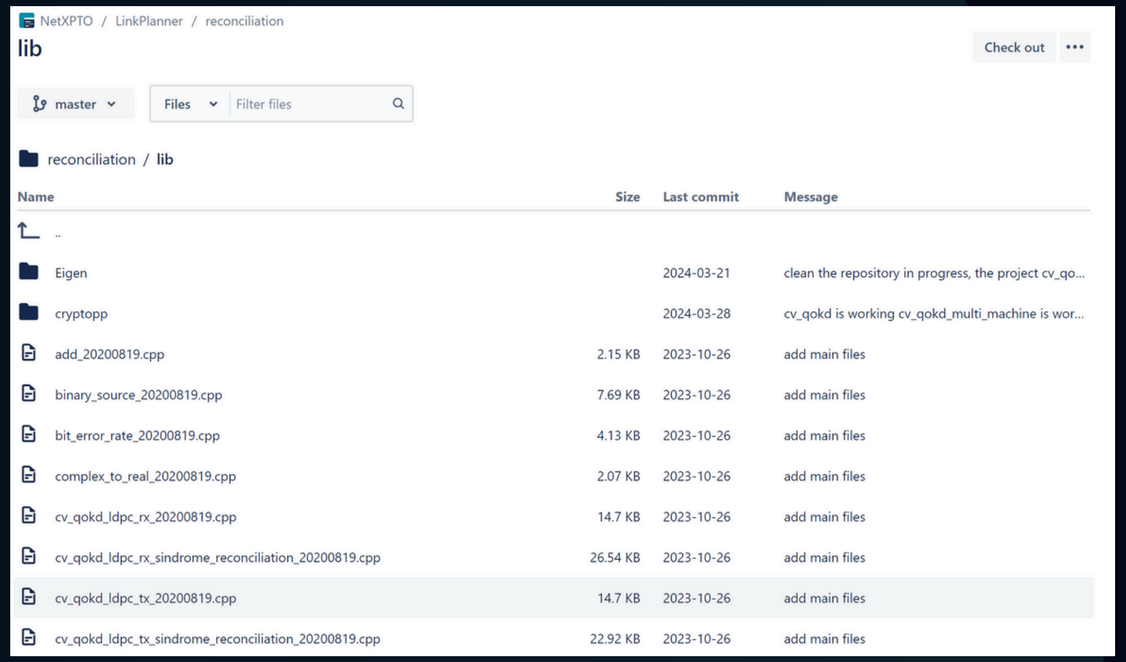
Objectives

- Develop/Fix Solutions
- QKD Layer Emulation
- Communication Protocols
- Local Key Storage
  & Management
- Comprehensible Docs



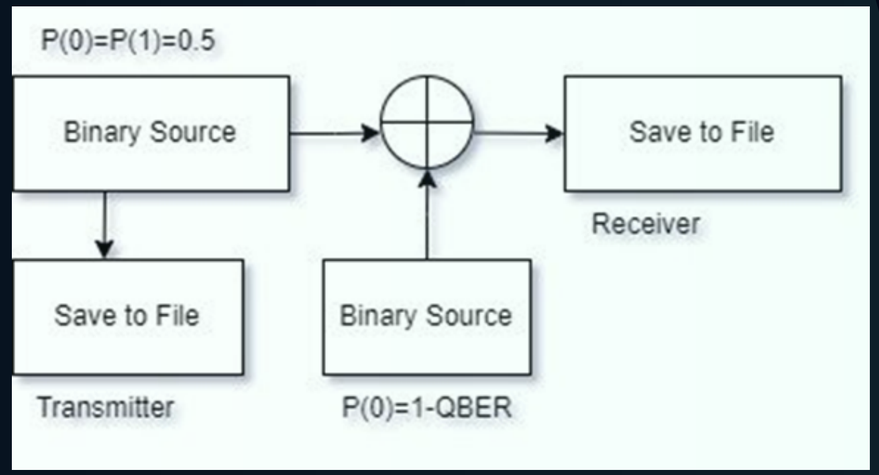
State of the art

- Implementations of reconciliation already existed with different features
- Uses a library called netxpto written in C++
- Some implementations worked between 2 computers



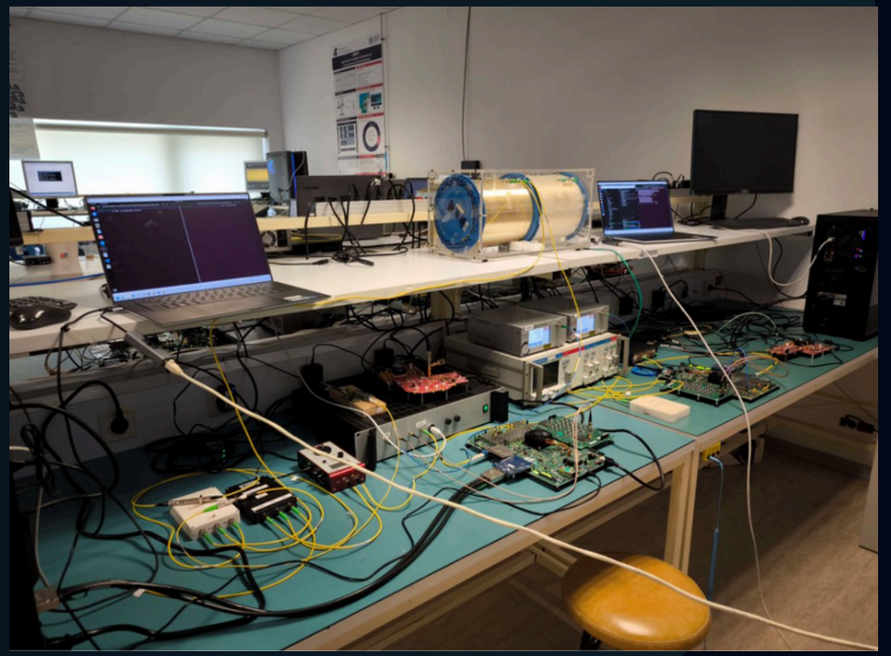
Goals

- Create emulators capable of simulating QKD Devices
- Integrate emulators with reconciliation
- Integrate reconciliation with KMS



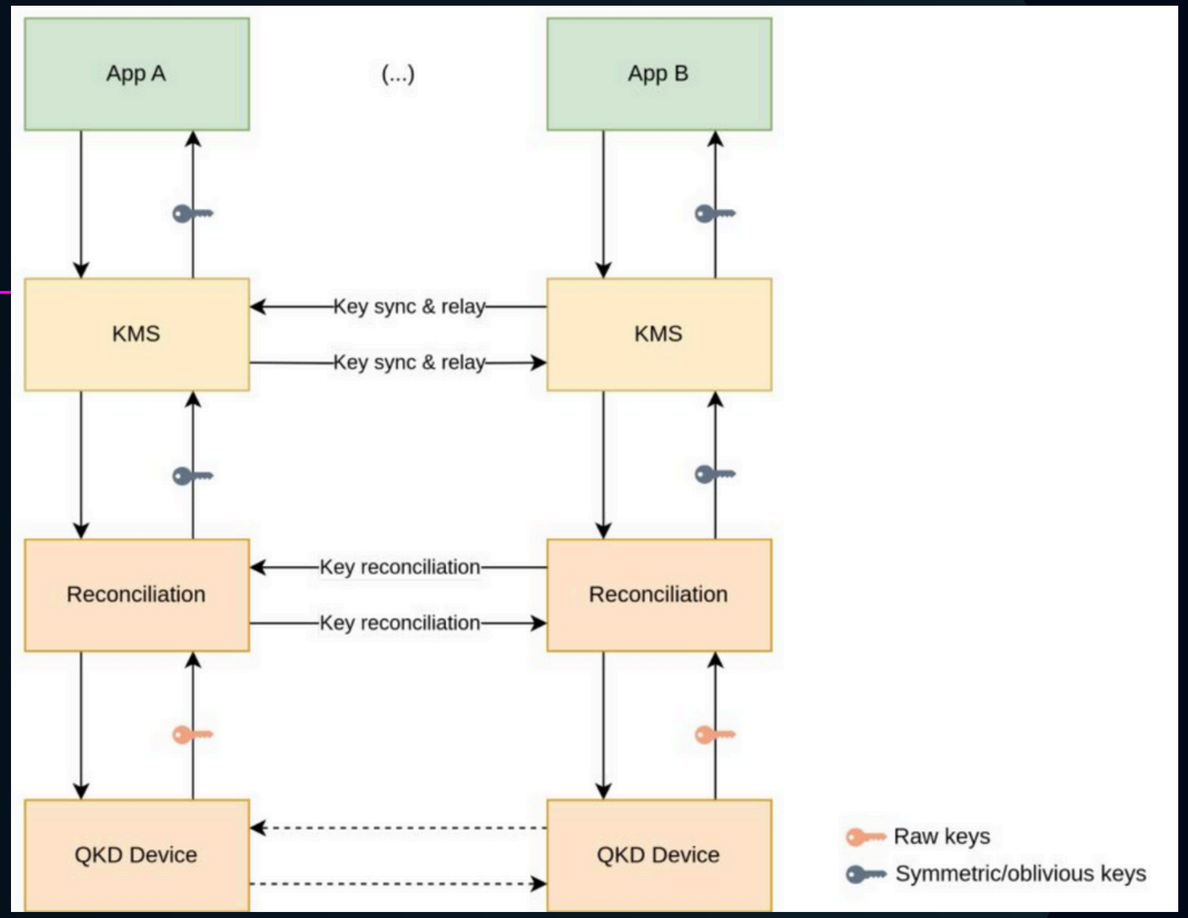
Outcomes

- The actual source code and application
- Documentation of our work
- Demonstration
- Presentation



Demonstration

- 4 computers in total, 2 on reconciliation and another 2 on KMS
- Was successful in processing raw keys into symmetric keys and storing them on KMS.



PART 2

qeep

- Motive
- Goals
- Architecture
- Results

Motive

- Secrets management apps are pretty safe in their classical sense.
- QKD physical networking products already exist, but are too low-level.

qeep

QeeP's Vision

- Why not both?
- Quantum-proof secrets management for both users and organizations
- Quantum-proof messaging platform

State-of-the-Art

Password/secrets management - Bitwarden

- E2EE for all data, both in transit and at rest.
- Relies on a master password known by the end-user to derive an encryption key.
- Reliance on asymmetric cryptography for authenticity

State-of-the-Art

Secure messaging - WhatsApp

- E2EE for all data, both in transit and at rest.
- Historical data backups using aforementioned master password mechanism.
- Modern Signal protocol for all messaging.

State-of-the-Art

Main takeaways

- SoA of secure storage and messaging platforms are NOT quantum-proof.
- Reference for E2EE data handling & new messaging protocol design.

Requirements

Analysis

Finding ways to achieve results

Methodology

Unified Process' Requirement Analysis:

- Domain & documentation research on QKD and secure protocols (Done)
- Interviewing target users and stakeholders (Done)
- Extensive research on critical system design and standards (Not done)

Actors

- **Individual user** - QeeP's most basic secret management and messaging features
- **Organizational user** - QeeP's more advanced features, tailored for organizations
- **Organizational admin** - Advanced organization vault management features
- **QeeP admin** - website management

Use cases

Secrets management package

- **Authentication** - logging in, signing up... - all actors
- **Secrets management** - storing, retrieving, deleting - all actors
- **Organization management** - vault ops, inviting users - organizational admin

Messaging package

- **Messaging** - sending simple text with attached media - all actors
- **Device linking** - loading message history onto different devices - all actors

Non-functional

Of note:

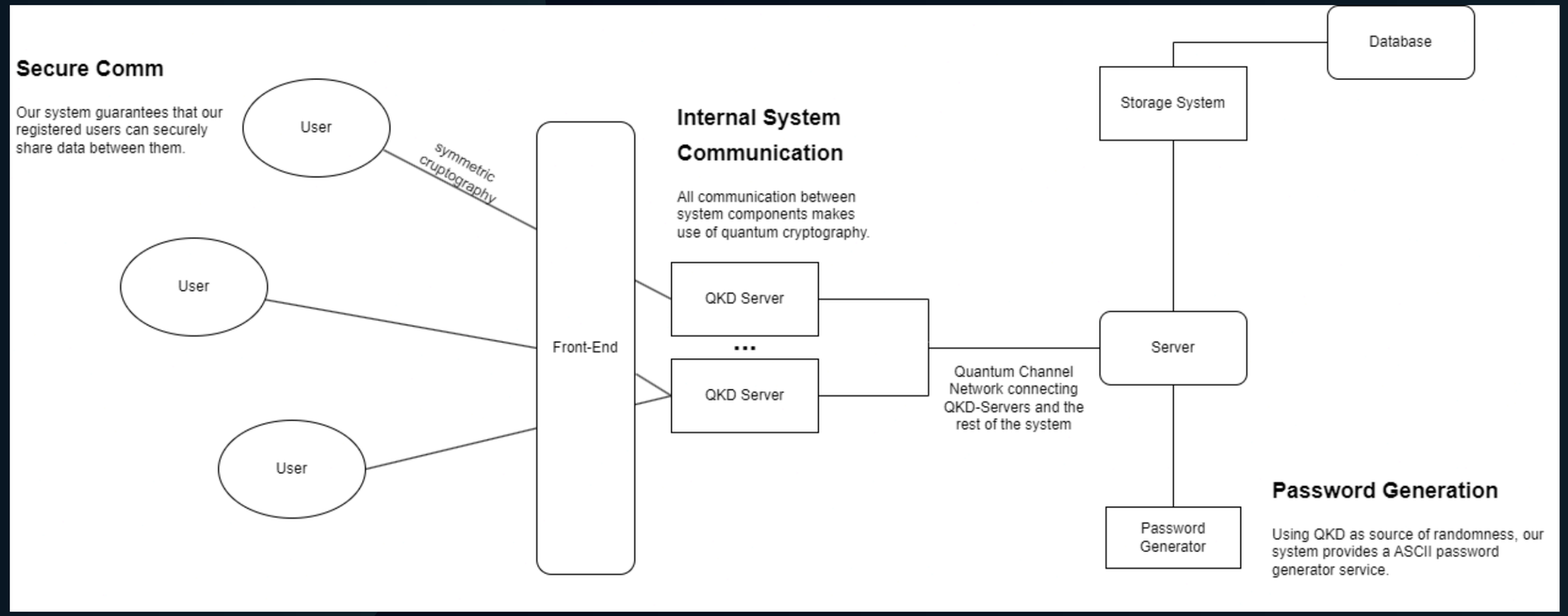
- **Security**: Elephant in the room
  - Focus of the project and extremely critical given the context
- **Usability**: A lesson from WhatsApp vs Signal
  - The less cumbersome one wins. Balance with the previous point.
- **Reliability**: High usage rates

Architecture

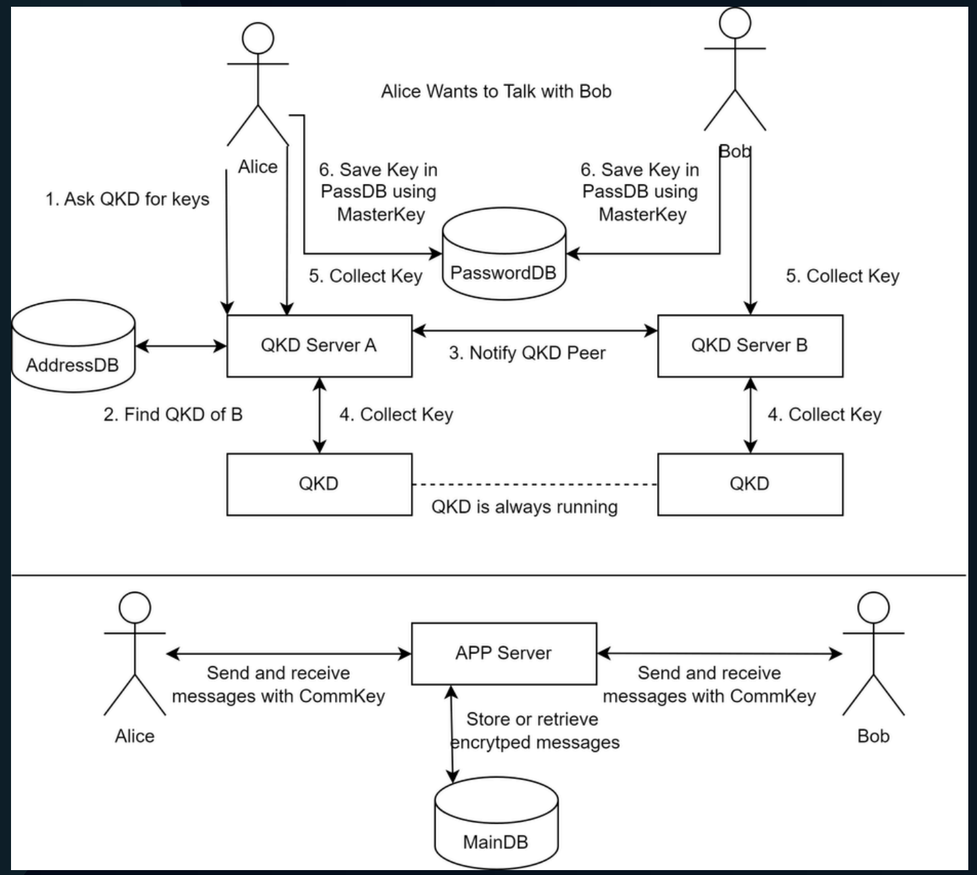
Analysis

Finding ways to better results

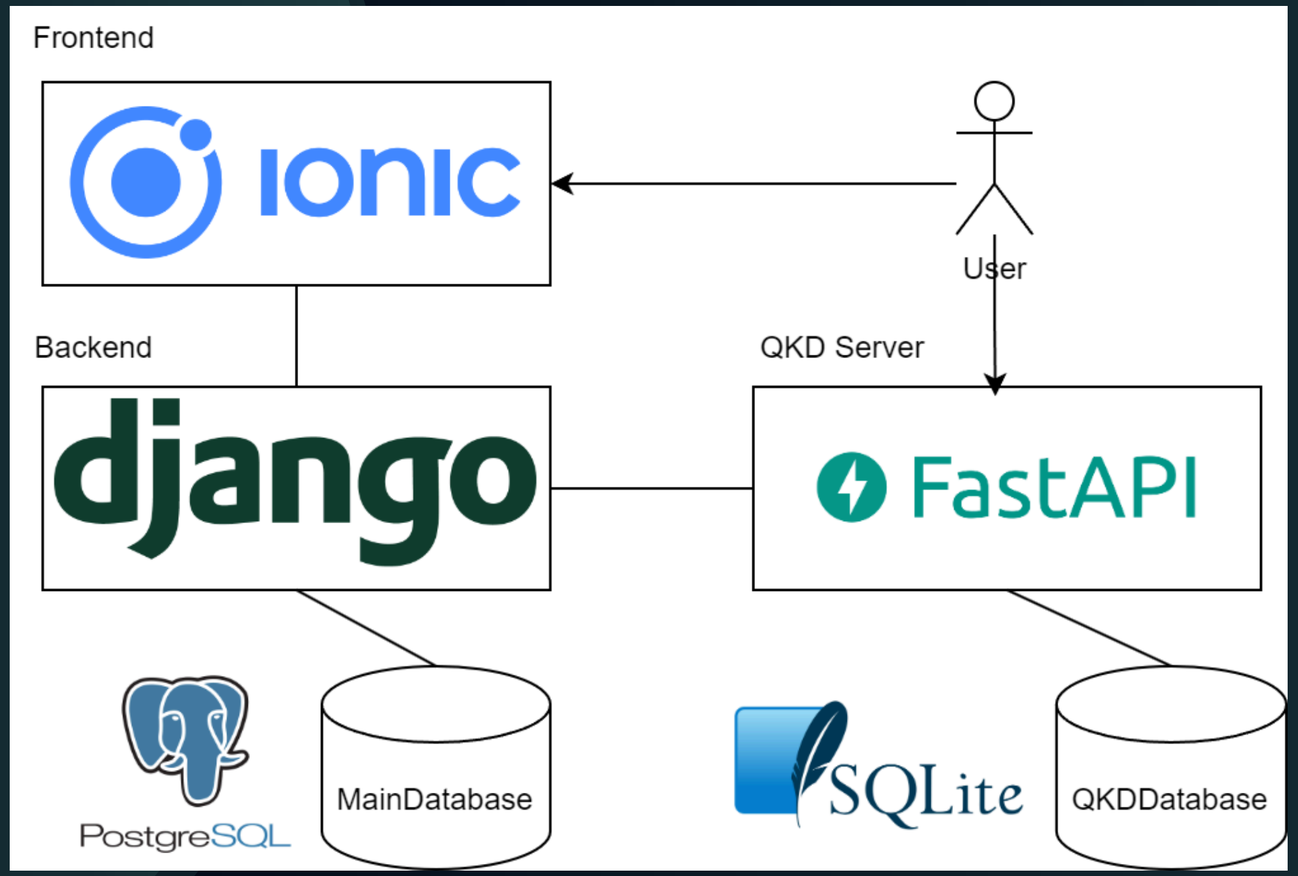
Communication



Architecture



Implementation

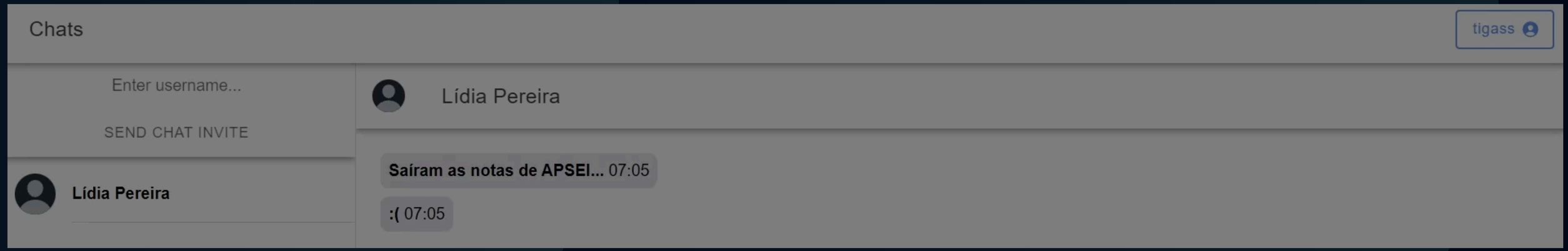


Results

& Outcomes

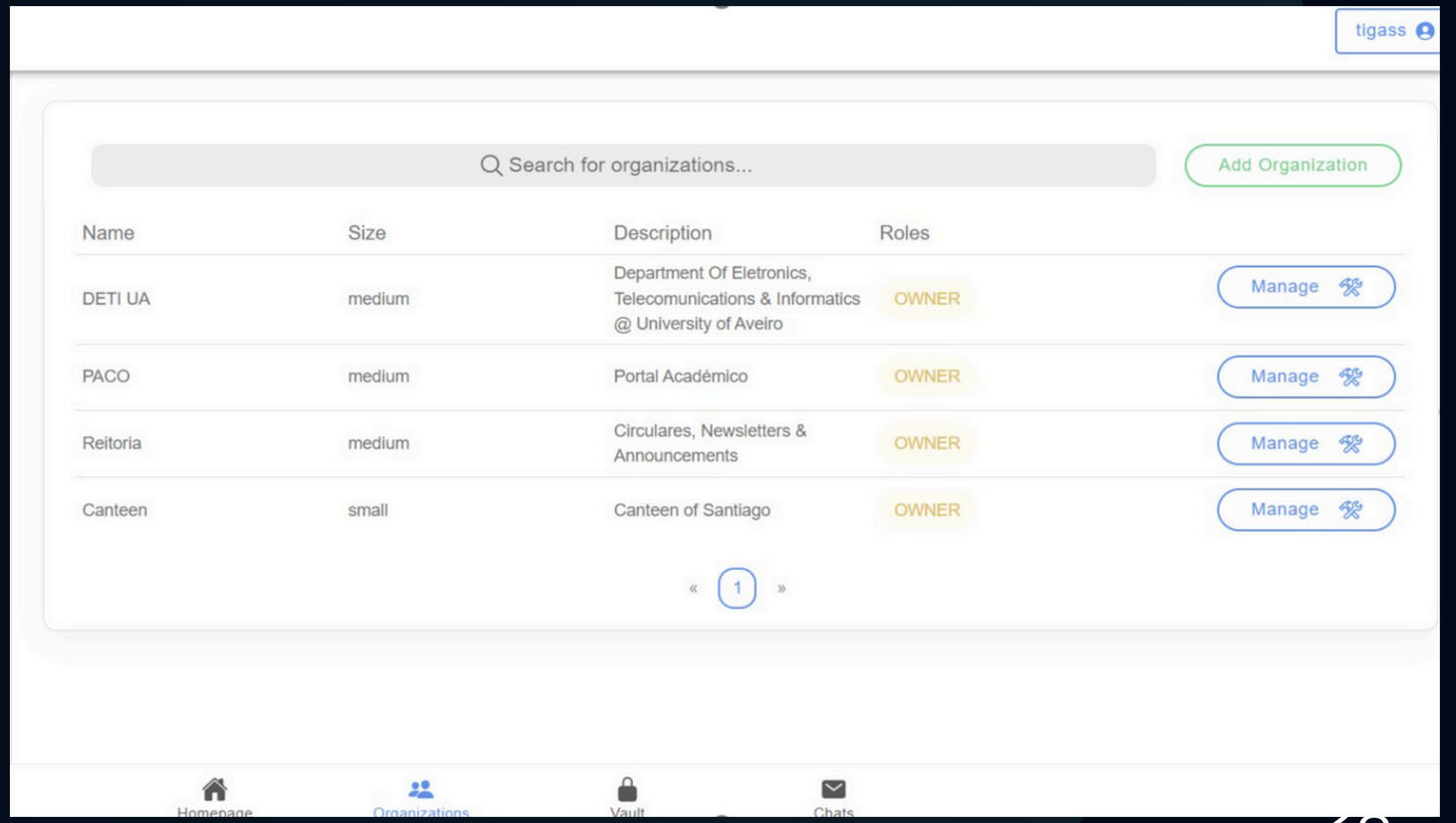
Results & Outcomes

- Quantum Chat System



Results & Outcomes

- Quantum Vaults
- Highly-Modular Secret Data Management Ecossystem



Main Challenges

Project management issues:

- **Insufficient** and **inefficient** communication with advisor during initial phase - significant delay in development.
- Consensus on design issues was **turbulent** up until the end.
- In this time-sensitive, rapidly shifting scenario, the UP methodology started to **fall short**.

- Missing member...

Conclusions

- Real project value was started too late -> Increased Challenge
- Implementing and testing novel security mechanisms is a time-consuming and constantly shifting venture.
- Fundamental takeaway: the value of communication and negotiation.

MS4: Final Presentation

Quantum Key Reconciliation Application

Team:

Diogo Marto	108298
David Cobileac	102409
Tiago Pereira	108546
Vítor Santos	107186

Orientadores:

Armando Pinto, IT

Diogo Matos, IT