universidade de aveiro

QUANTUM KEY RECONCILIATION APPLICATION

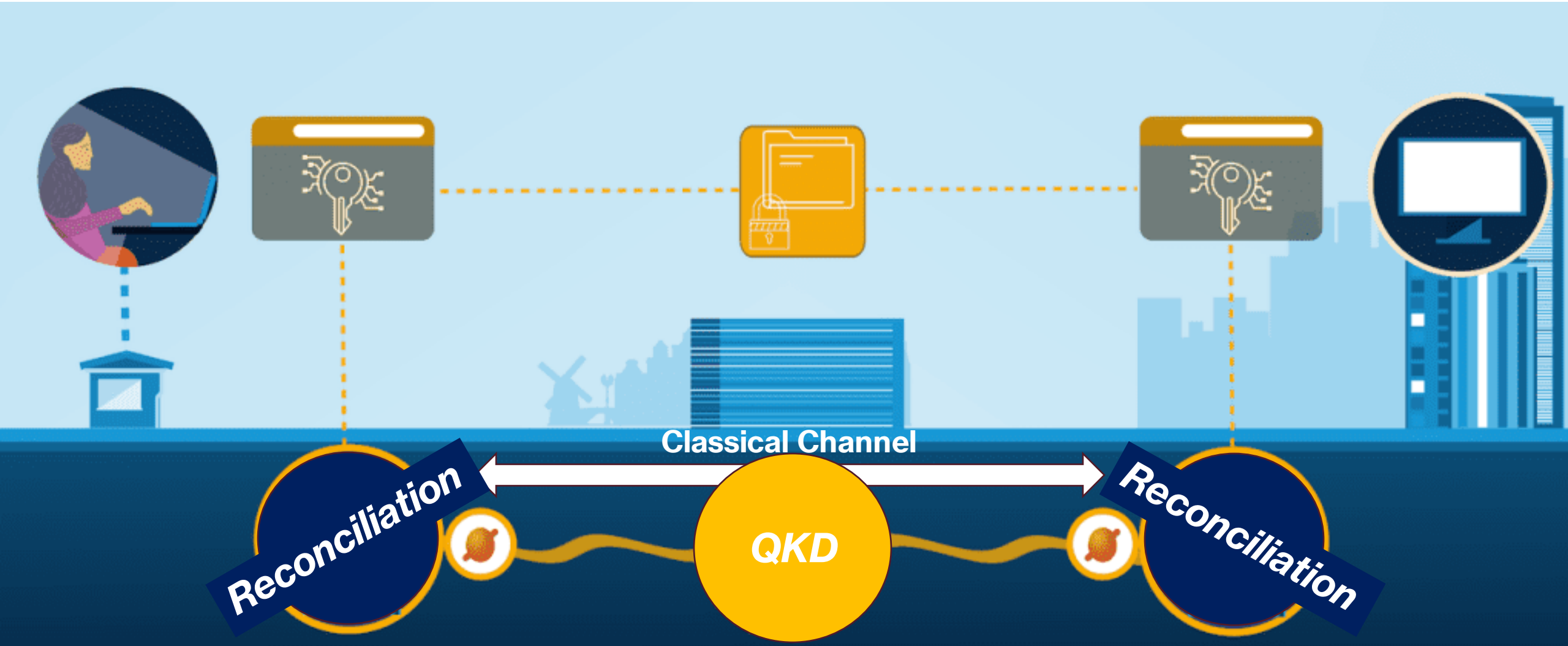
Milestone 2 **–** Elaboration

Group 14

Diogo Marto	108298
David Cobileac	102409
Tiago Pereira	108546
Tiago Portugal	103931
Vítor Santos	107186

Index

Context



State of the Art

Usage: Securely Generate and Distribute Keys

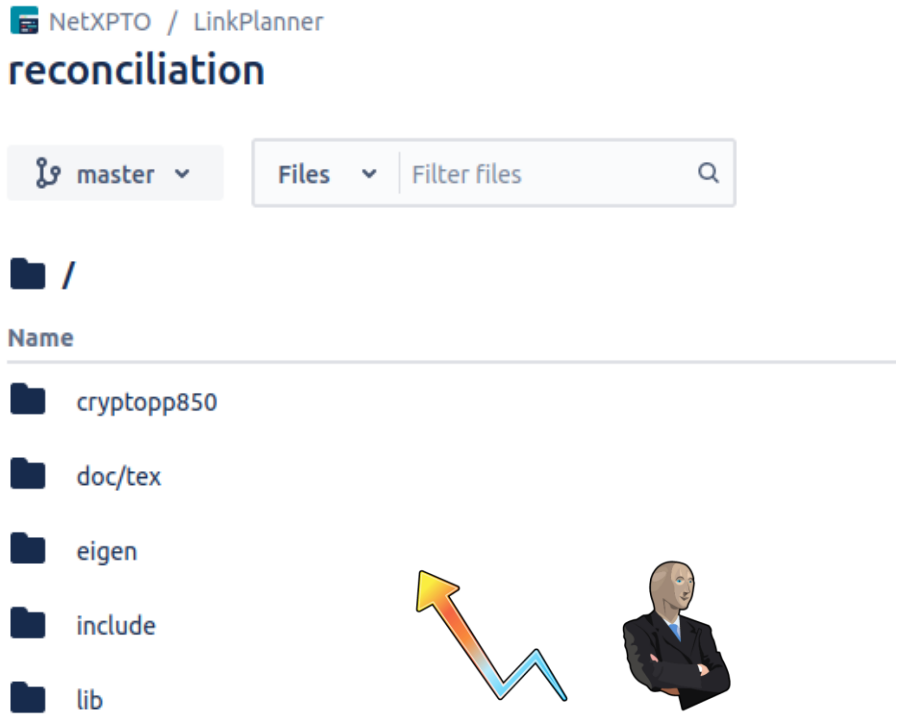
Current State of Reconciliation Layer:

- Process **symmetric** or o**blivious keys**
  - **Cooperative Communication** between parties (local-hosted).
  - **Key derivation from raw key Material**

Expected work:

- Communication interfaces
- Library
- Real-Data consumption

evolution



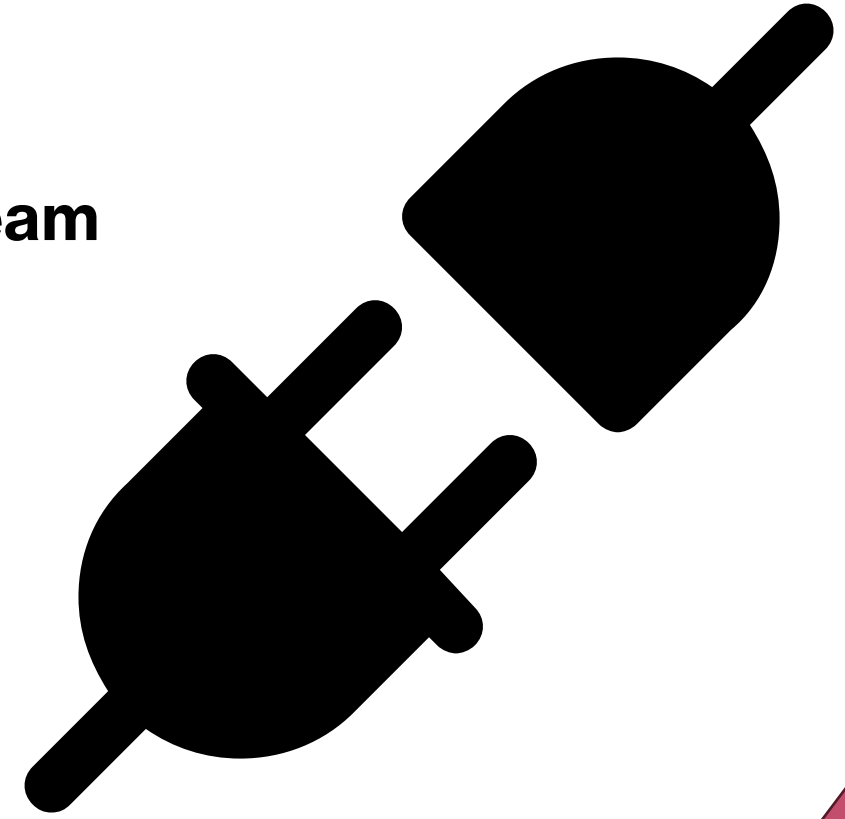
Requirement elicitation

Methodology

- **Documentation reviews**
  - QKDN documentation
  - Regulatory documentation
- **Domain modelling**
- **Use-case analysis**
  - Determine actors from external software components
  - No real human actors directly involved in system use
- **Meetings** with general QKDN project leaders and coordinators

Actors

- **QKD Key Management System layer team**
- **QKD device layer team**



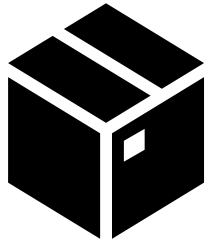
Use cases

ID	0	1
Name	Generate a key	Diagnose and calibrate QKD devices network
Description	Process raw keys into oblivious/symmetric keys	Log anomalies, measure metrics and check the reliability of the QKD device layer
Actors	• QKD Key Storage Management layer • QKD device layer	• QKD device layer

Functional Requirements

ID	Description	Use Case	Priority
0	Layer communication protocol based on ETSI GS.	0;1	High
1	APIs	0;1	High
1.1	Bottom Layer API	0;1	High
1.2	Upper Layer API	0;1	High
2	Testing environment	0;1	High
2.1	Raw key generator	0;1	High
2.2	Logging and metrics tools	1	Medium
3	Reconciliation module	0;1	High
3.1	Syndrome decoding submodule	0;1	High
3.2	Syndrome reconciliation submodule	0;1	High

Non-functional Requirements

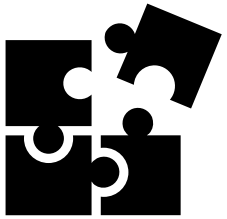


Portability

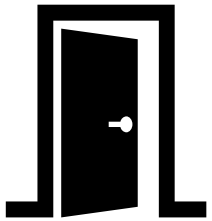
Performance

Reliability

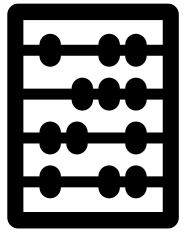
Security



Compatibility



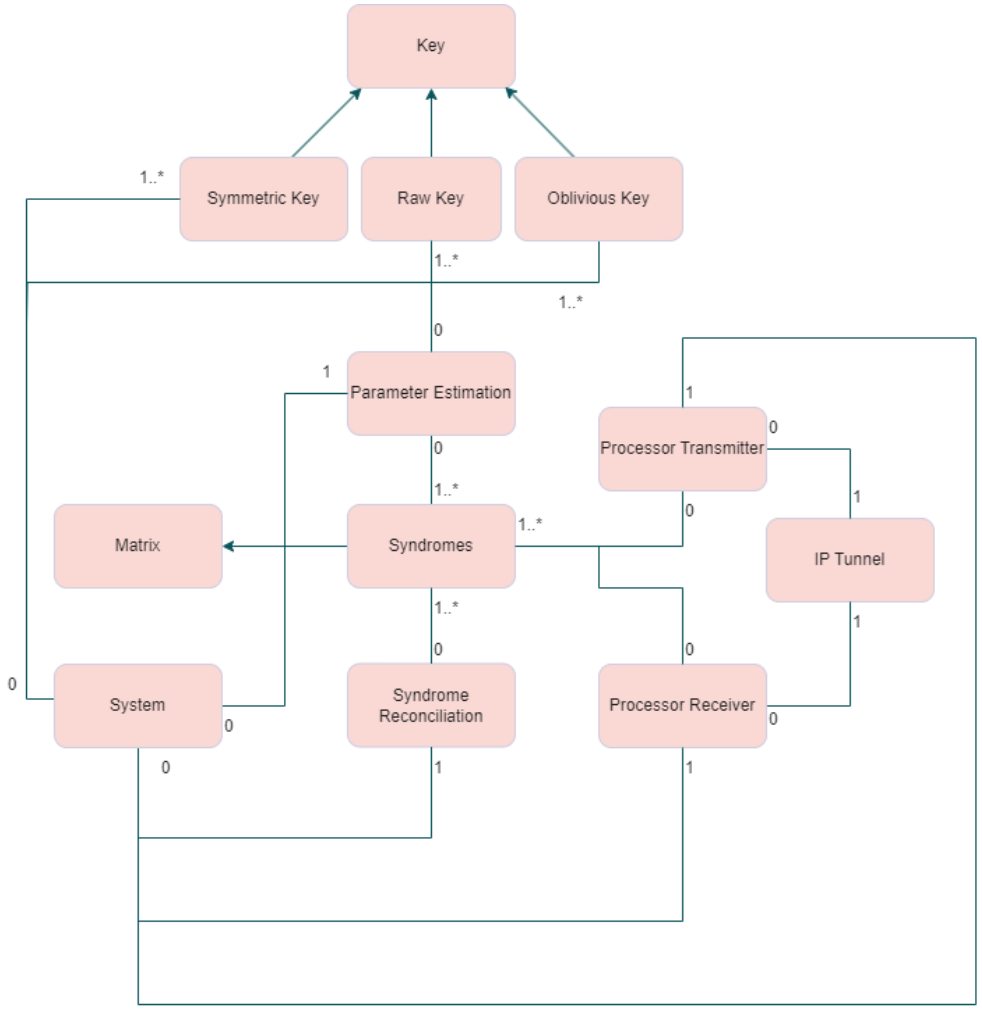
Availability



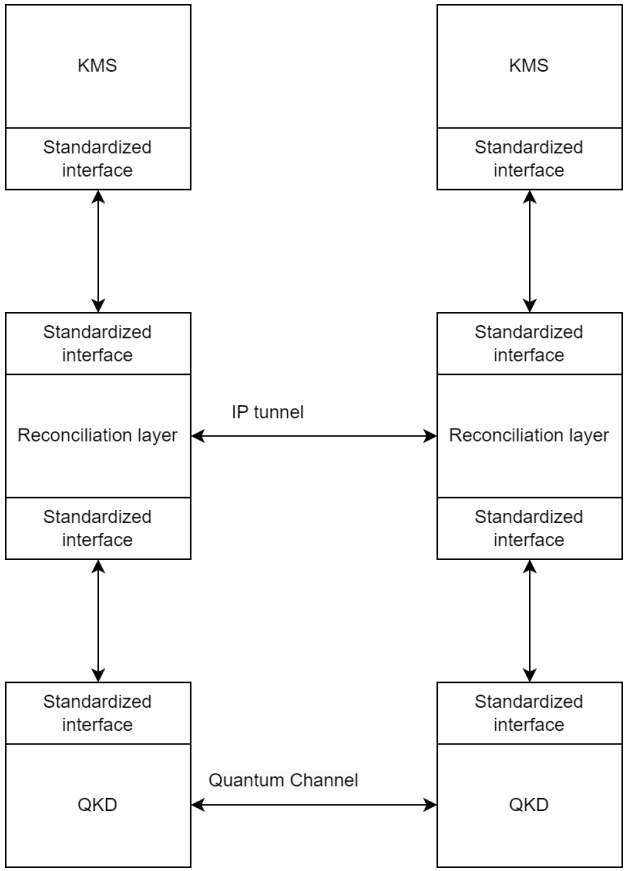
Usability

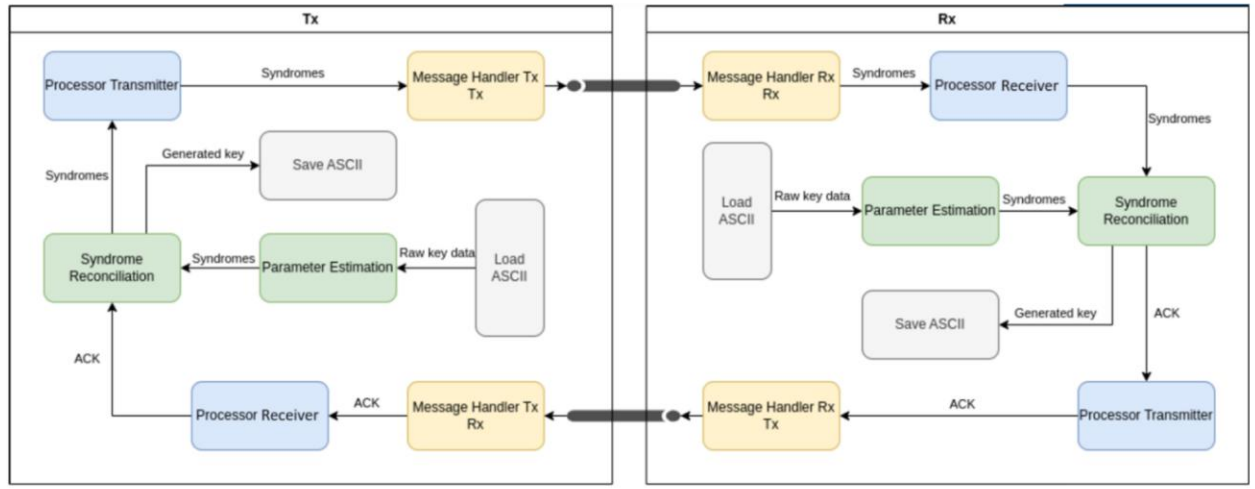
Regulatory

Domain

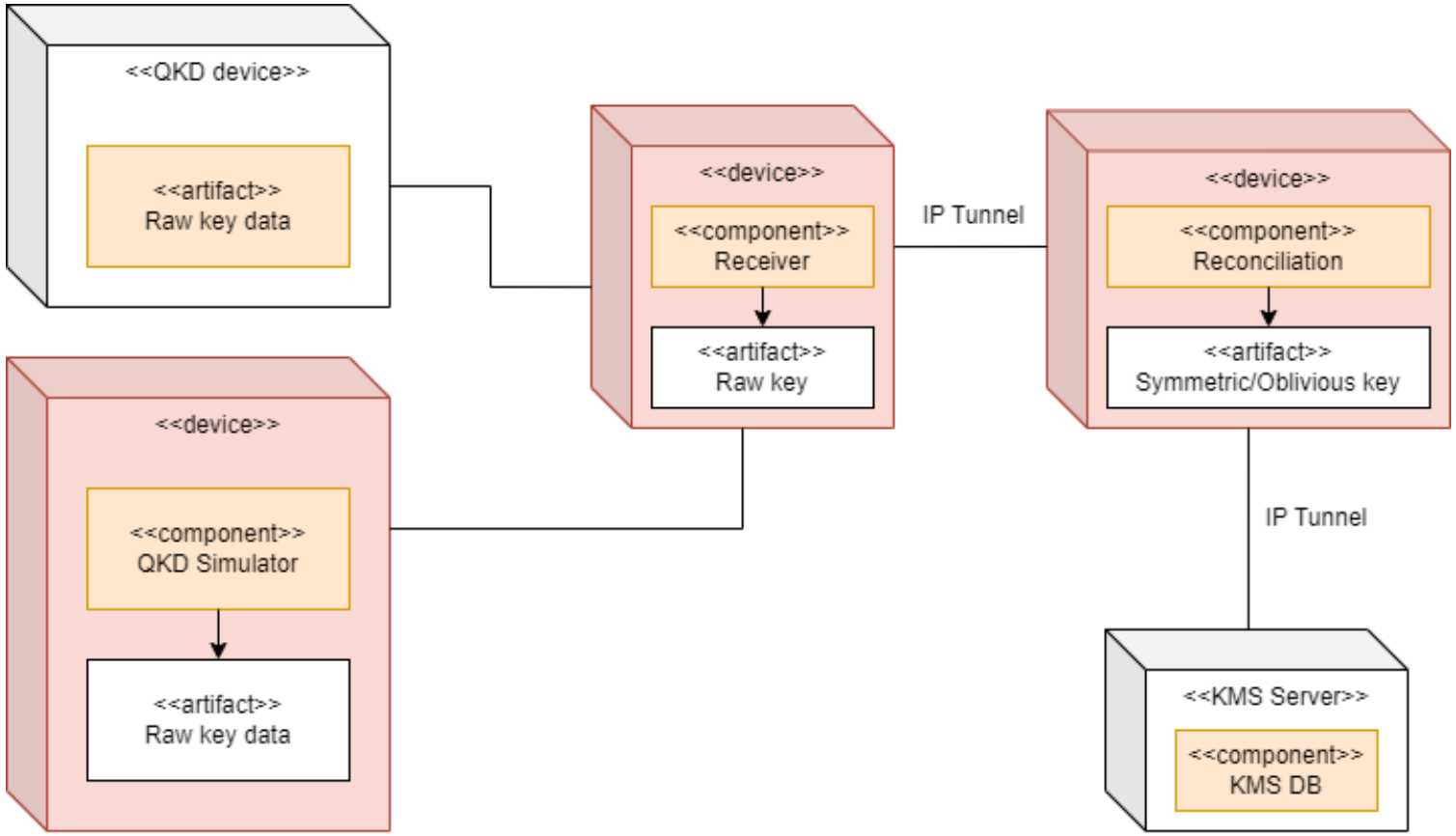

Key
Symmetric Key
Raw Key
Oblivious Key
Parameter Estimation
Processor Transmitter
Matrix
Syndromes
IP Tunnel
System
Syndrome Reconciliation
Processor Receiver
1..*
0
1

Architecture





Deployment


<<QKD device>>
<<artifact>>
Raw key data
<<device>>
<<component>>
Receiver
<<artifact>>
Raw key
IP Tunnel
<<device>>
<<component>>
Reconciliation
<<artifact>>
Symmetric/Oblivious key
<<device>>
<<component>>
QKD Simulator
<<artifact>>
Raw key data
IP Tunnel
<<KMS Server>>
<<component>>
KMS DB

References:

- https://dl.acm.org/doi/fullHtml/10.1145/3600160.3605050
- https://elearning.ua.pt/pluginfile.php/247936/mod_resource/content/4/PI05_example.pdf
- https://www.reqview.com/doc/iso-iec-ieee-29148-templates/
- https://ieeexplore.ieee.org/document/278253
- https://www.evolutionq.com/products/basejumpqdn
- https://www.etsi.org/deliver/etsi_gs/QKD/001_099/004/02.01.01_60/gs_QKD004v020101p.pdf
- https://www.altexsoft.com/blog/non-functional-requirements/
- Domain Modeling by Example. Associating Objects with Python. https://codeburst.io/rule-your-domain-model-d4beae6806c
- A Brief Introduction to Domain Modeling. https://olegchursin.medium.com/a-brief-introduction-to-domain-modeling-862a30b38353

Thank you !

- Diogo Marto, 108298, diogo.marto@ua.pt
- David Cobileac, 102409, cobileacd@ua.pt
- Tiago Pereira, 108546, tfgp@ua.pt
- Tiago Portugal, 103931, tiago.portugal@ua.pt
- Vítor Santos, 107186, vitor.mtsantos@ua.pt