INTEGRATE COLLECTIVE CERTIFICATE MANAGEMENT ON SKIPCHAINS AND ON CROSS PLATFORM MOBILE APPLICATION

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

RESPONSIBLE

PROF. BRYAN FORD

DEDIS/EPFL

CLAUDIO LOUREIRO

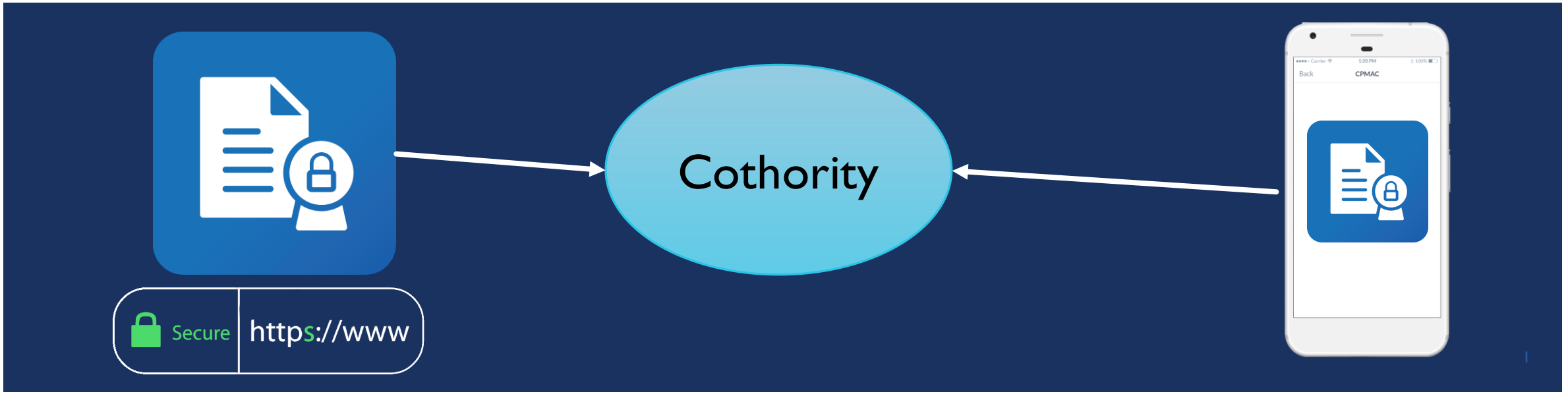
MASTER SEMESTER PROJECT

DECENTRALIZED AND DISTRIBUTED SYSTEMS LAB

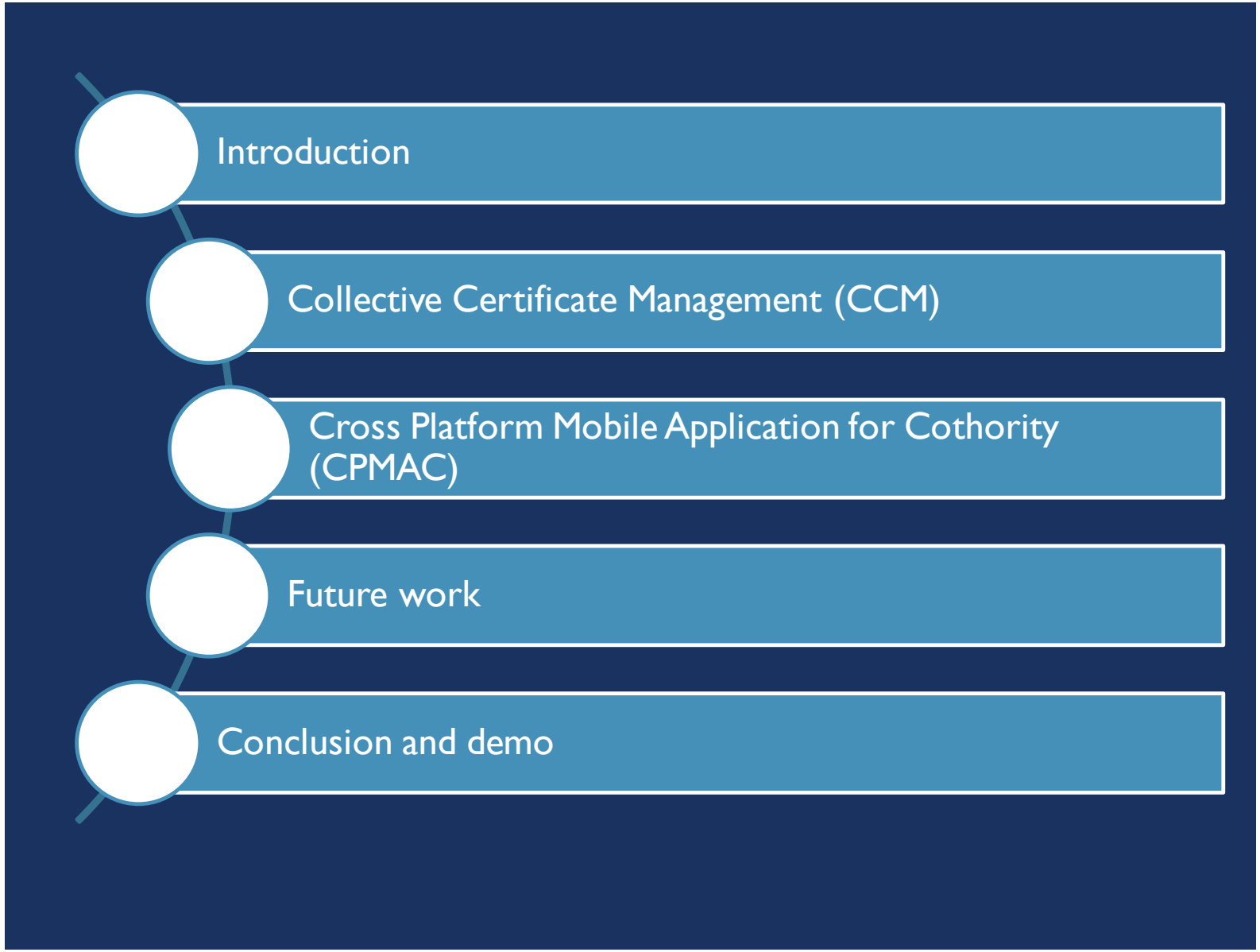
SUPERVISOR

LINUS GASSER

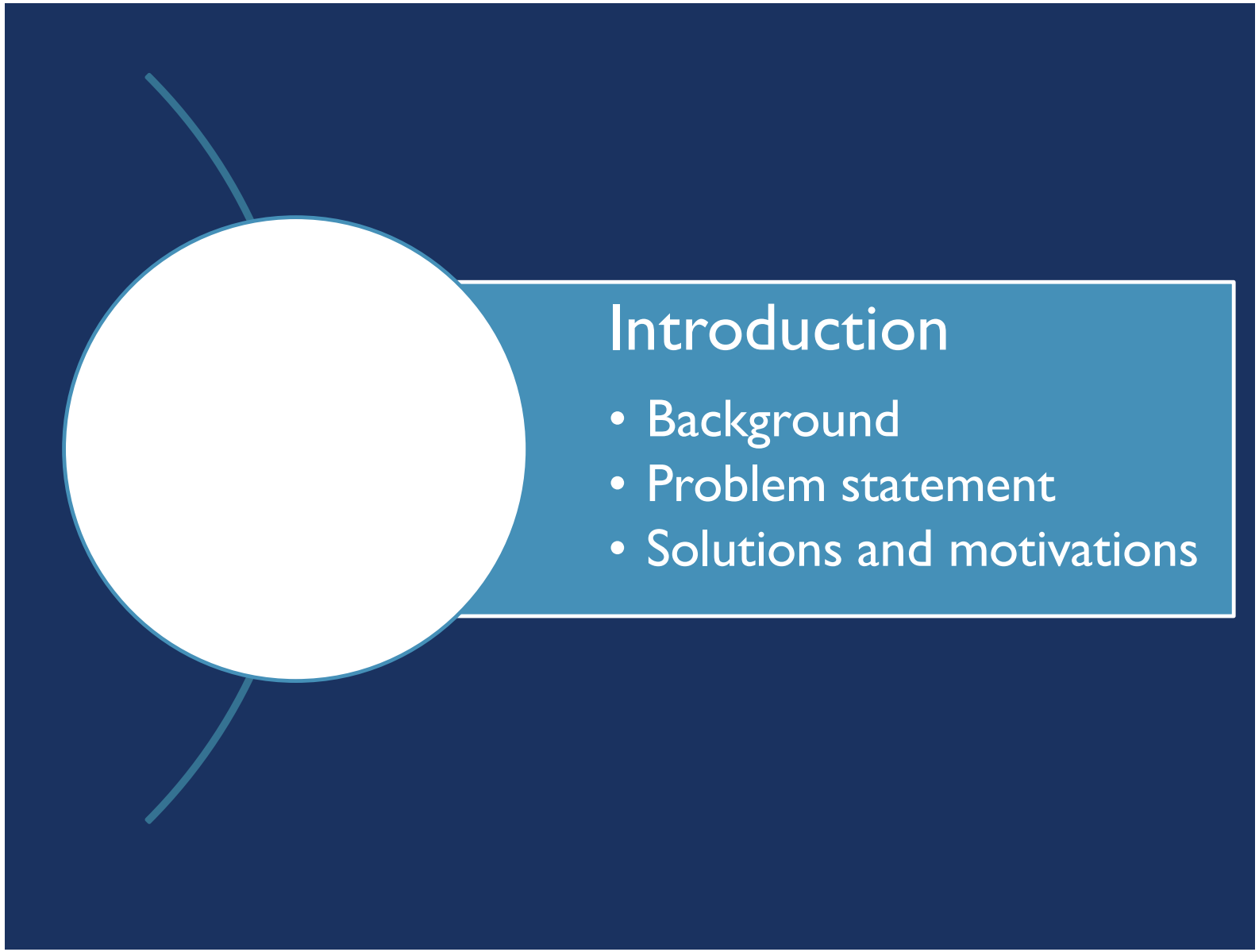
DEDIS/EPFL



SUMMARY

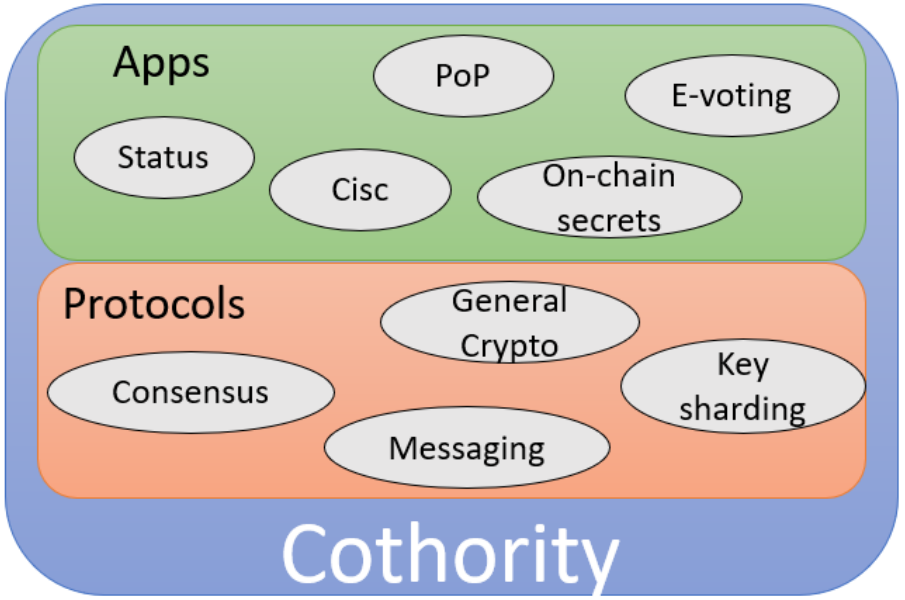

Introduction
Collective Certificate Management (CCM)
Cross Platform Mobile Application for Cothority (CPMAC)
Future work
Conclusion and demo

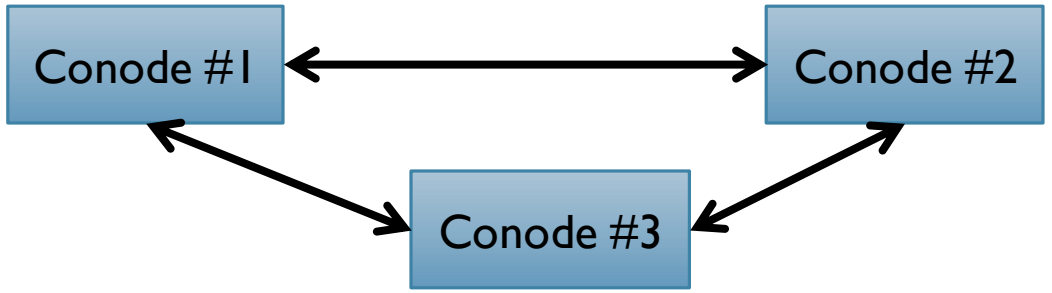
INTRODUCTION



BACKGROUND - COTHORITY

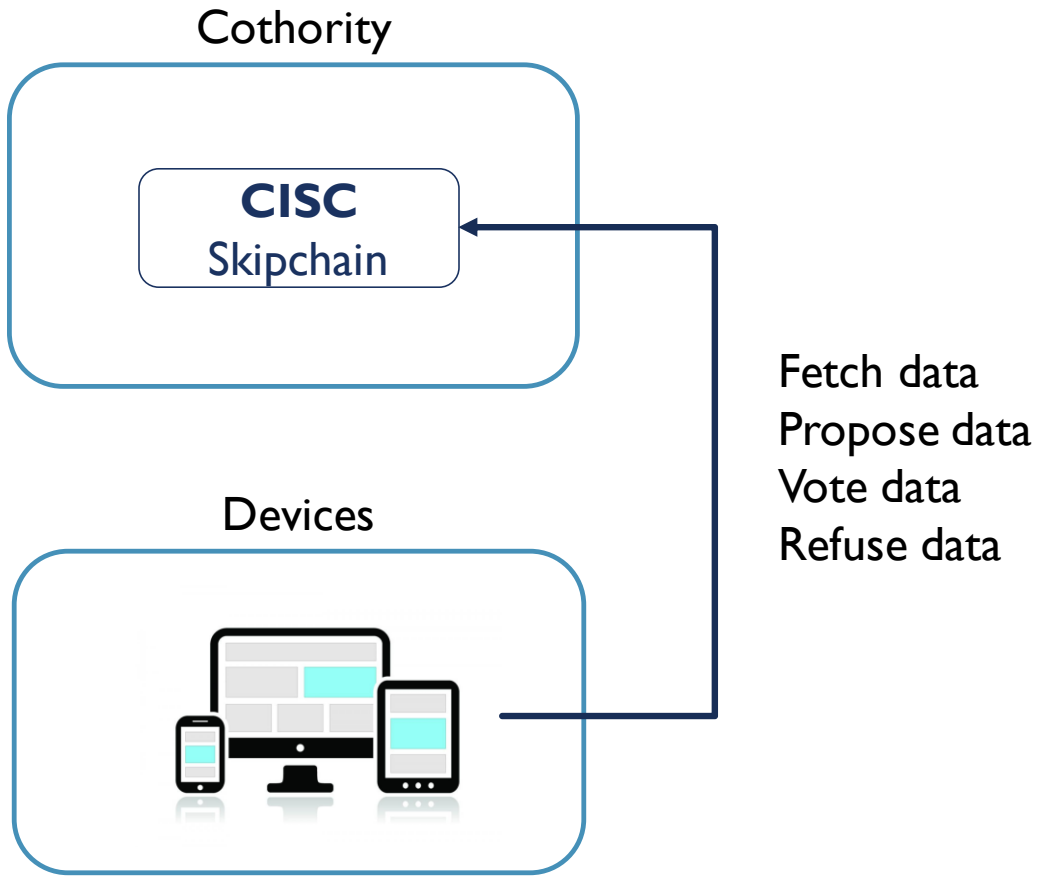
- Cothority framework
  - Protocols between conodes
  - Apps (PoP, Cisc…)
  - Services, (CoSi, Status,…)



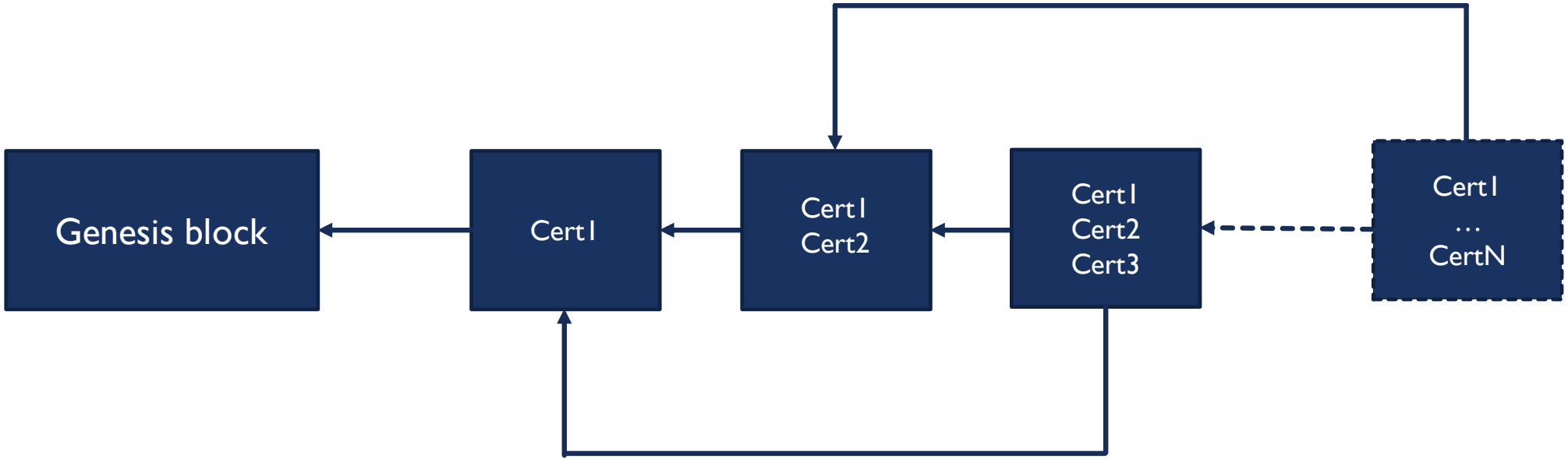


BACKGROUND - CISC

- Application providing a simple way to store data
- Storing based on blockchain principle (Skipchains)
- System of cryptographic vote
  - New data needs to be accepted by a threshold of devices
  - Proposal list for data to be voted on
  - If accepted a new block is added to the Skipchain
- Data storage
  - Key/value pairs
  - SSH public keys
  - Webpages
  - **Certificates**



BACKGROUND - SKIPCHAIN



Skipchain structure

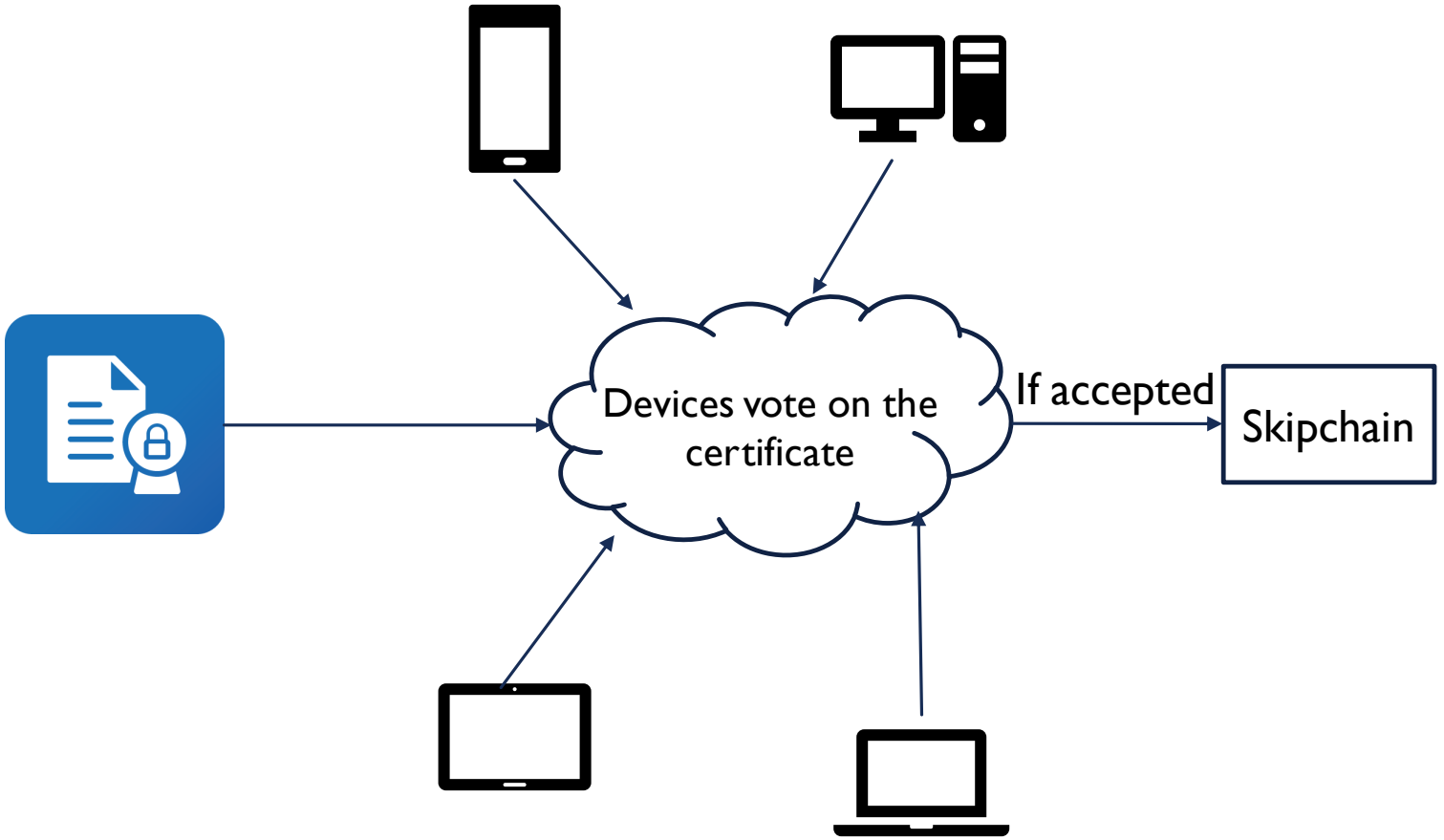
PROBLEM STATEMENT

- **Problem**
  - Certification Authority can validate or give fake certificates (even intentionally)
    - WoSign incident in 2015 [1]
    - Trustwave incident in 2012 [1]
- **Consequences**
  - Impersonation of web server
  - Man-in-the-middle : spying communications or stealing valuable information

[1] https://www.enisa.europa.eu/publications/info-notes/certificate-authorities-the-weak-link-of-internet-security

SOLUTION

- Using our Skipchains to store and vote on certificates
  - Multiple entities decide together if certificates are considered valid
  - Accepted certificates are stored in the Skipchain
  - Any modification on the certificate should be collectively approved



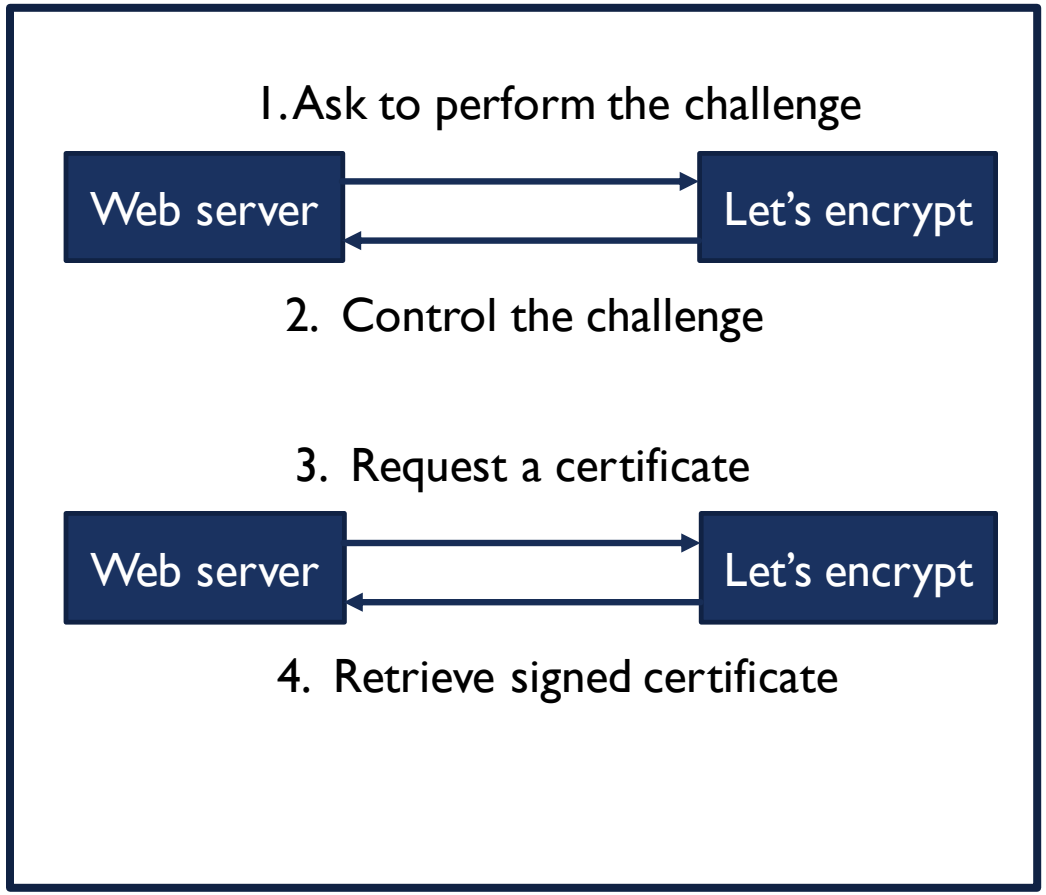
MOTIVATIONS AND GOALS

- Integration of Collective certificate management on Skipchains (Command Line Interface)
  - Previous implementation not supported by multiple Skipchains
  - Commands robustness improved
- Integration of this functionality on the Cross Platform Mobile Application (CPMAC)
  - Command line interface is not a user-friendly interface
  - Offers a better visualization and interaction with the certificates stored

COLLECTIVE CERTIFICATE MANAGEMENT

OVERVIEW

- Cisc commands (CLI)
  - **Request** : Request a certificate from Let's Encrypt and add it to the Skipchain if the proposition is accepted
  - **Add** : Add an existing certificate to the list proposal
  - **List** : Display the stored certificates
  - **Retrieve** : Retrieve the physical certificate
  - **Renew** : Renew the certificate
  - **Revoke** : Revoke a certificate by deleting it from the Skipchain if the proposition is accepted



Request procedure

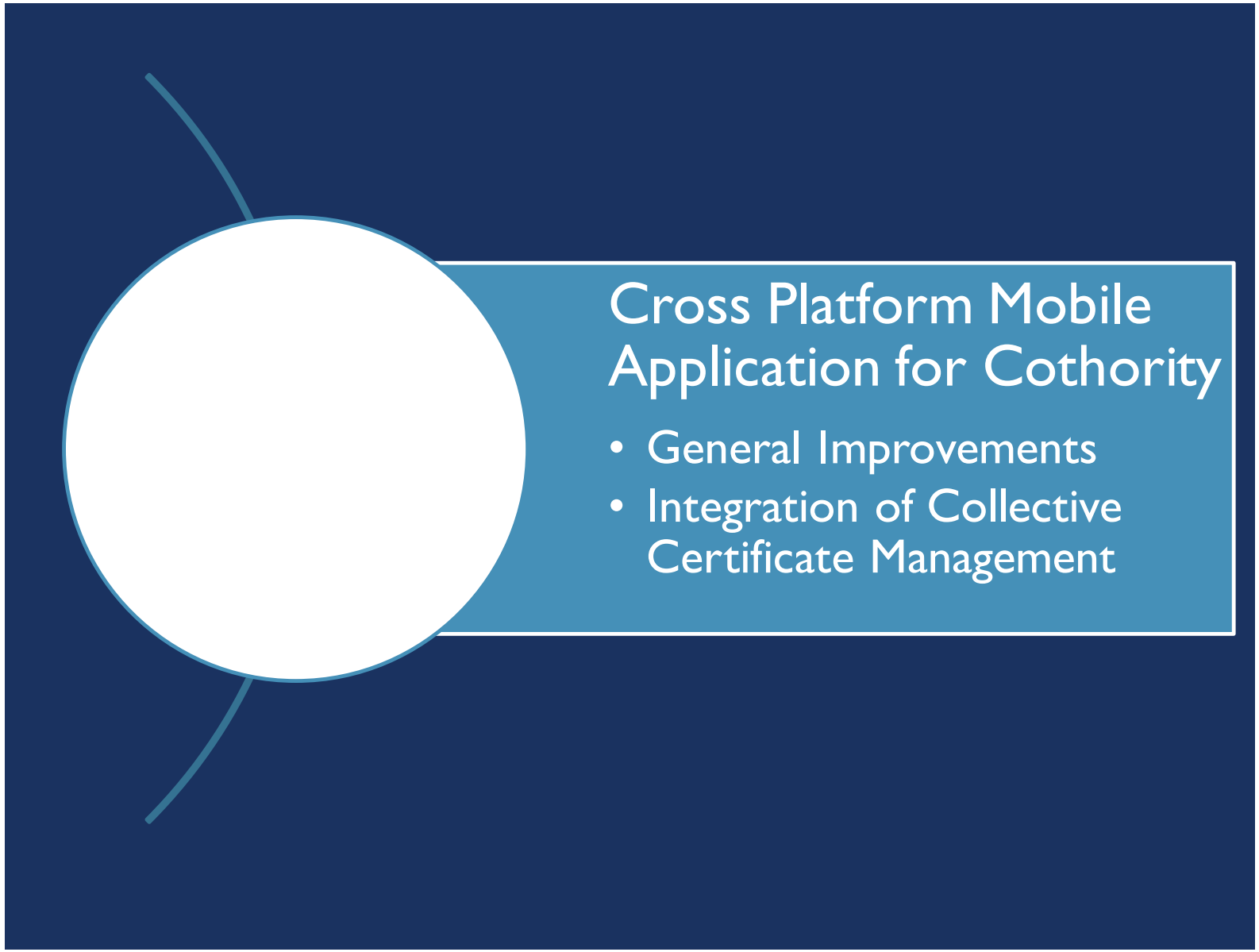
IMPROVEMENTS AND CHANGES

- Skipchain ID has to be given together with the commands if multiple Skipchains available
- Improved robustness and clarity of the Cisc certificate commands
  - Code cleaning
  - Paths to directories have to be given more often (avoiding storing private keys in public folder) and to control where the core data is stored in the device
  - When listing certificates more information is shown
  - Renew certificate automatically replaces the old certificate (locally and in the Skipchain)

ROBUSTNESS IMPROVEMENT

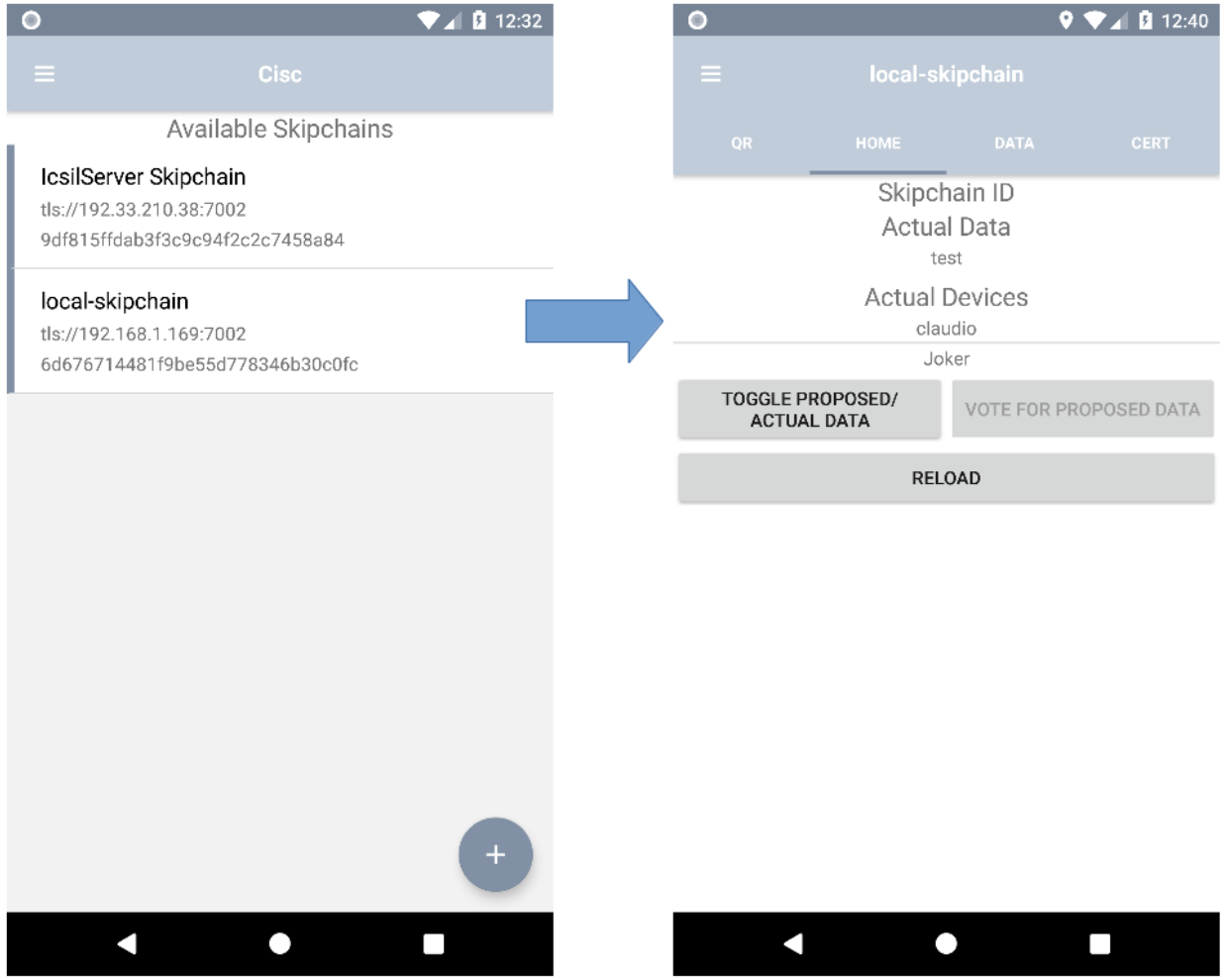
- **Before** Cisc request takes only the domain as argument (keys and certificates are stored locally in the current folder)
- **Problem** private keys could be stored accidentally public folder
- **After** Cisc request takes as arguments
  - Requested domains (cothority.net)
  - Certificate path (cert)
  - Public folder (www)

CROSS PLATFORM MOBILE APPLICATION FOR COTHORITY (CPMAC)



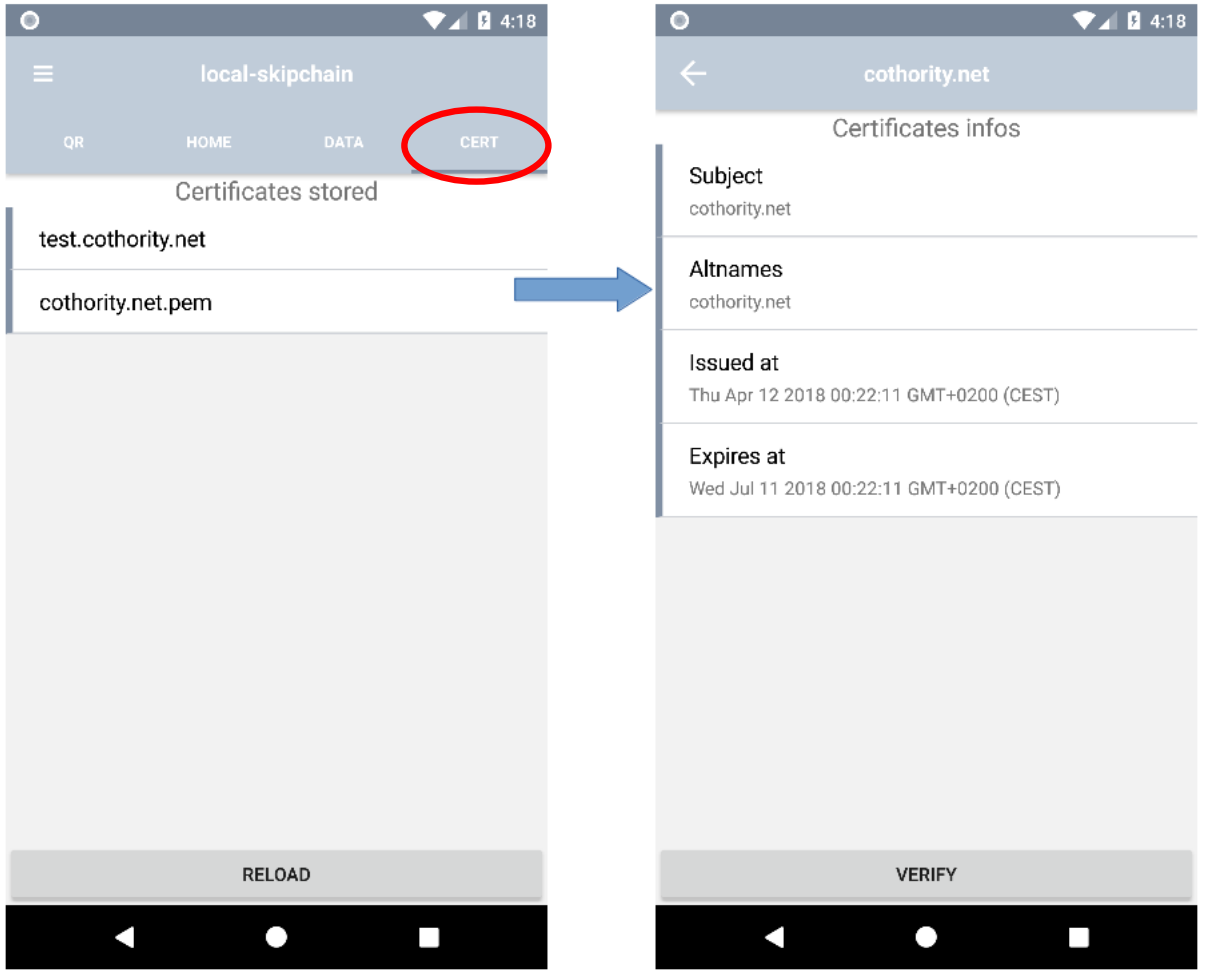
GENERAL IMPROVEMENTS

- Multiple Skipchains compatibility
  - All the Skipchains listed in the Cisc home page
  - Add button to join an existing Skipchain
- Settings update
  - User name is no longer bound to a Skipchain

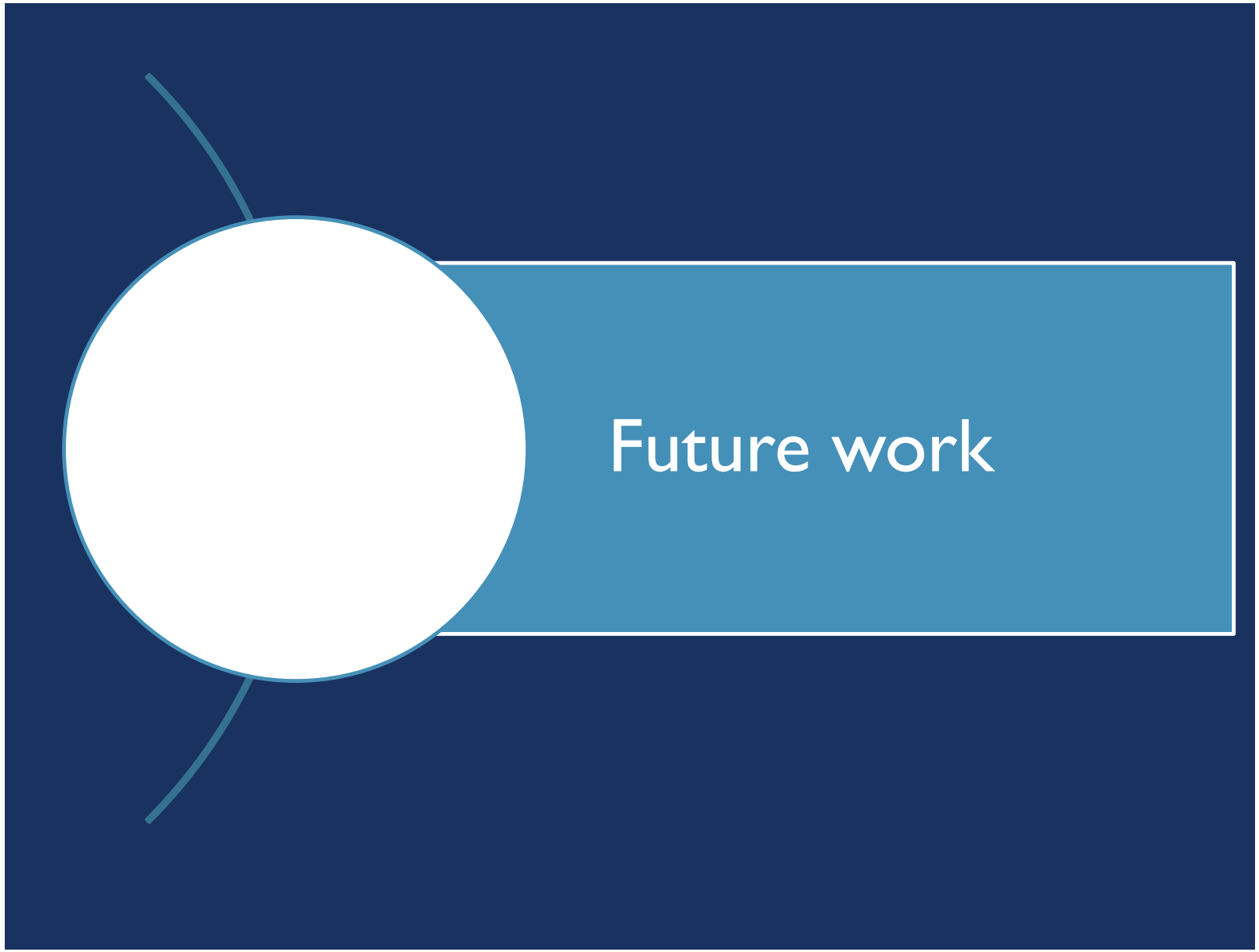


INTEGRATION OF COLLECTIVE CERTIFICATE MANAGEMENT

- Cert tab added
- Lists stored certificates with their names
- Clicking on a certificate shows additional information
- Possibility to verify the clicked certificate
  - Check the validity
  - Check it was signed by its parent
  - Check certificate issuer name matches the parent's subject name



FUTURE WORK



FUTURE WORK

Collective Certificate Management

- Automated voting and renew system

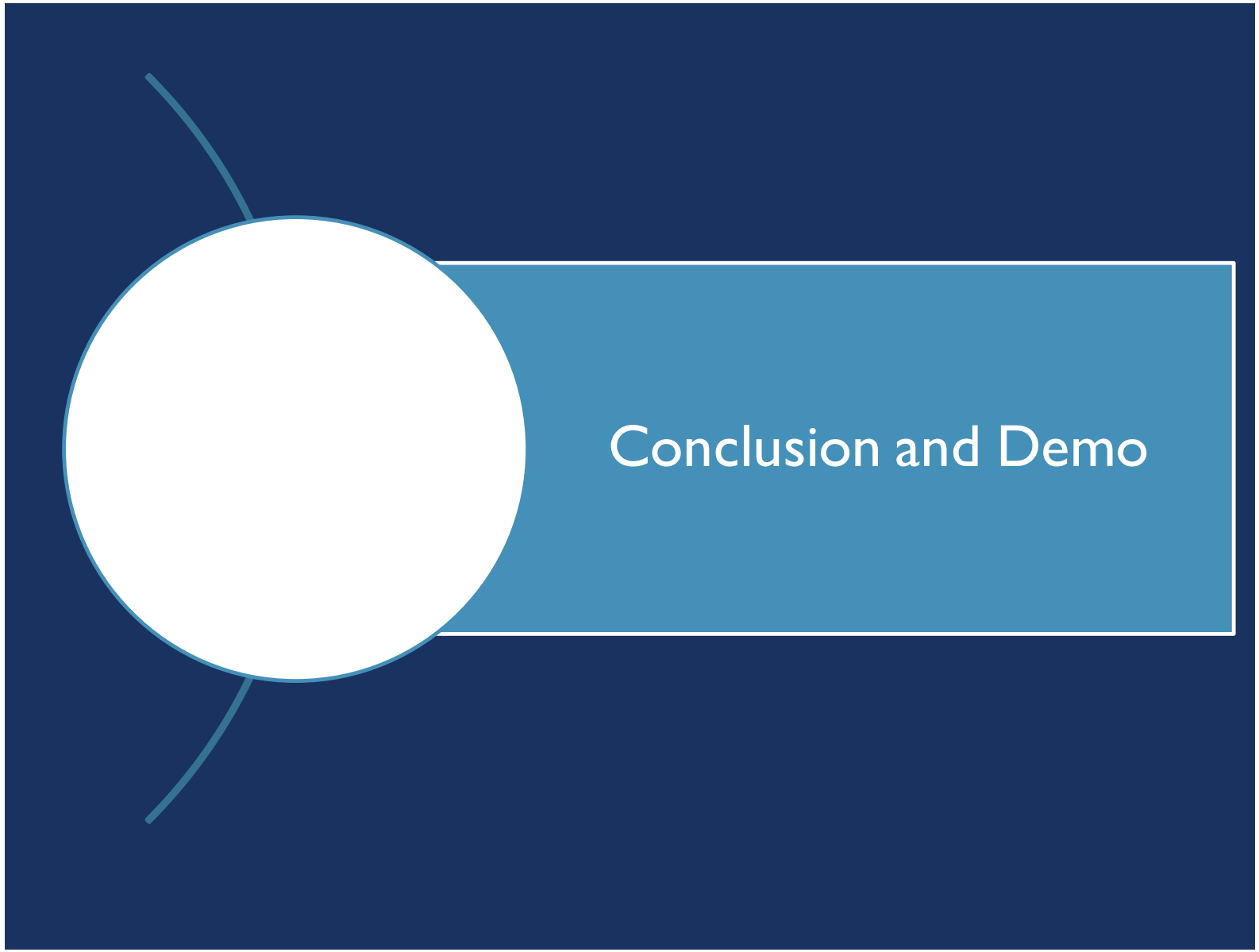
CPMAC

- At the moment a certificate can only be requested with the command line interface Cisc user

Other features

- Adding a plugin to the browser to verify if the certificate is on the Skipchain

CONCLUSION AND DEMO



CONCLUSION AND DEMO