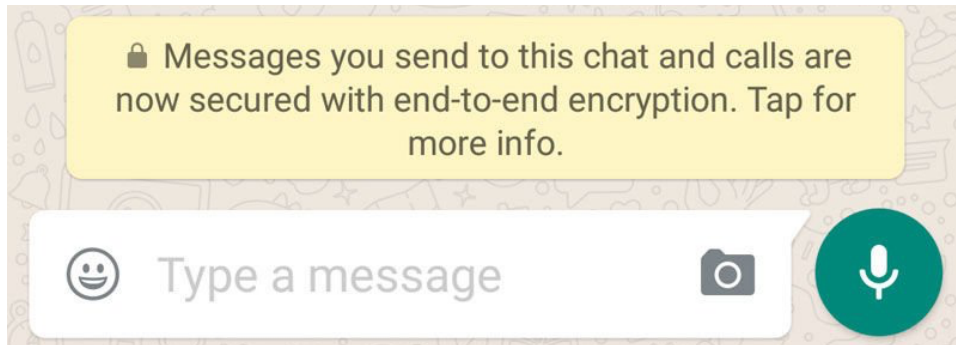
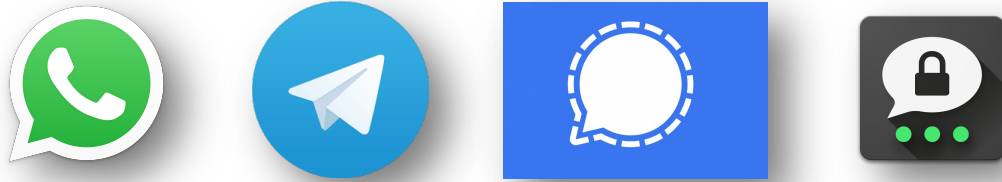


# ABEBox: end-to-end encryption for file sharing cloud services

*E. Raso, L. Bracciale, G. Bianchi, P. Loreti*

Pierpaolo Loreti, Emanuele Raso  
University of Rome "Tor Vergata"

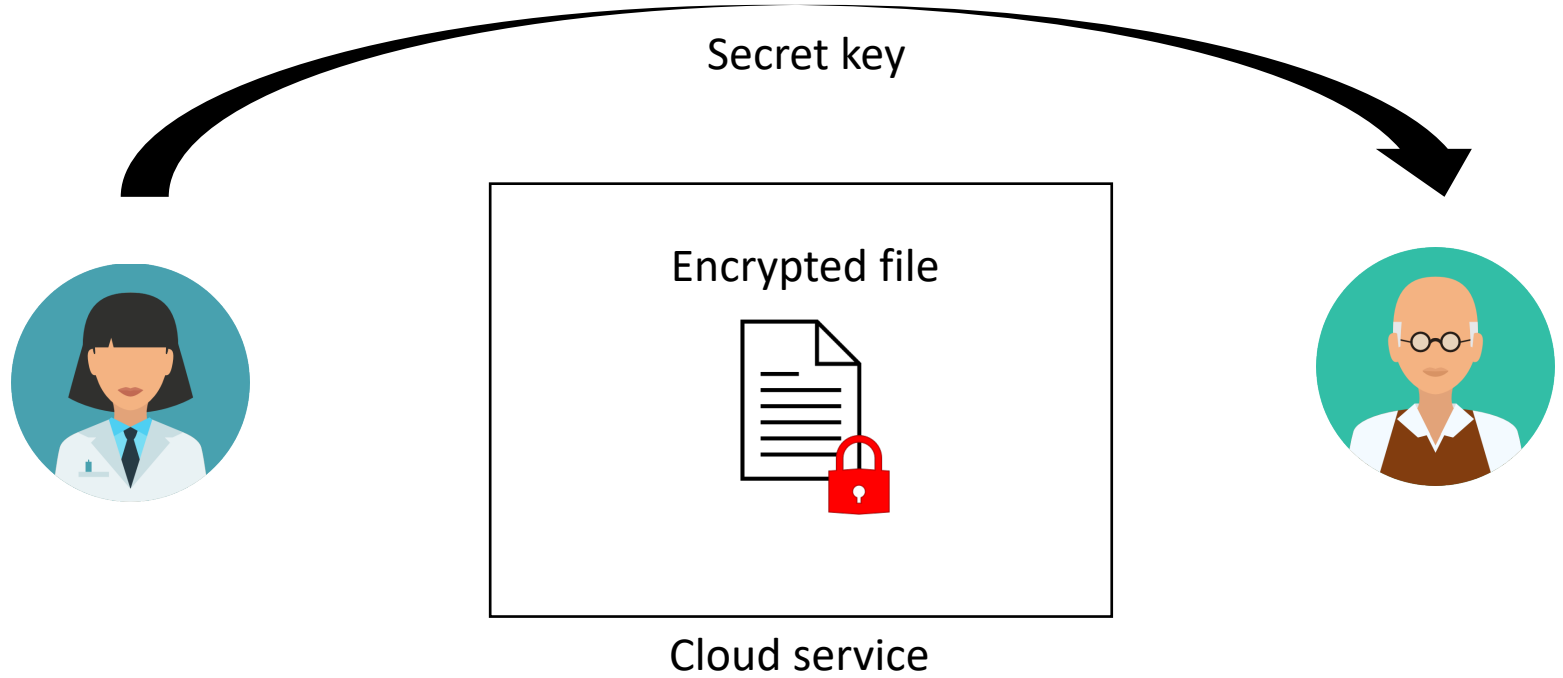
# End to end encryption in file sharing



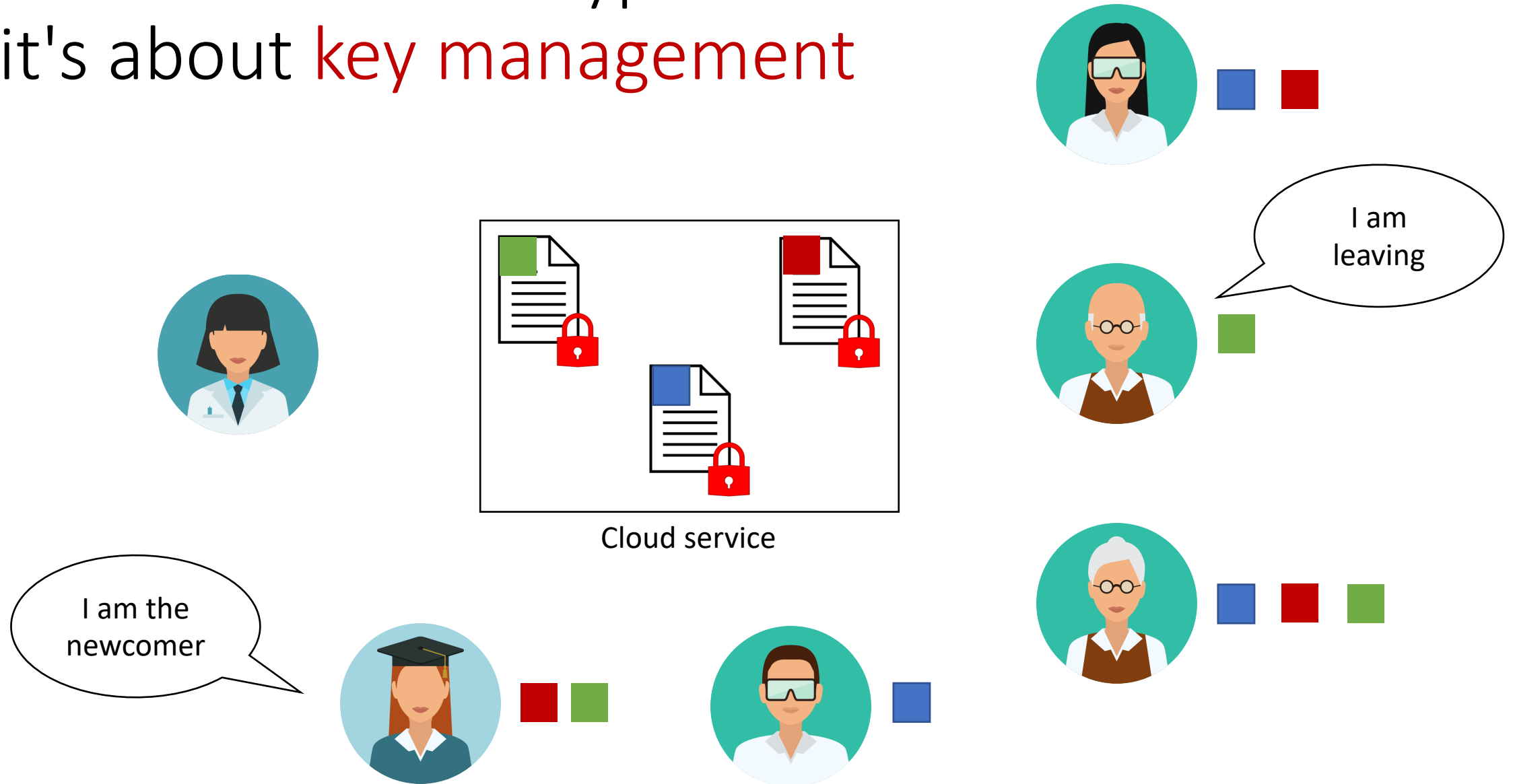
*Ownccloud EE2E*  
*Nordlocker*  
*Boxcryptor*  
*CryFs*



# A trivial exercise?



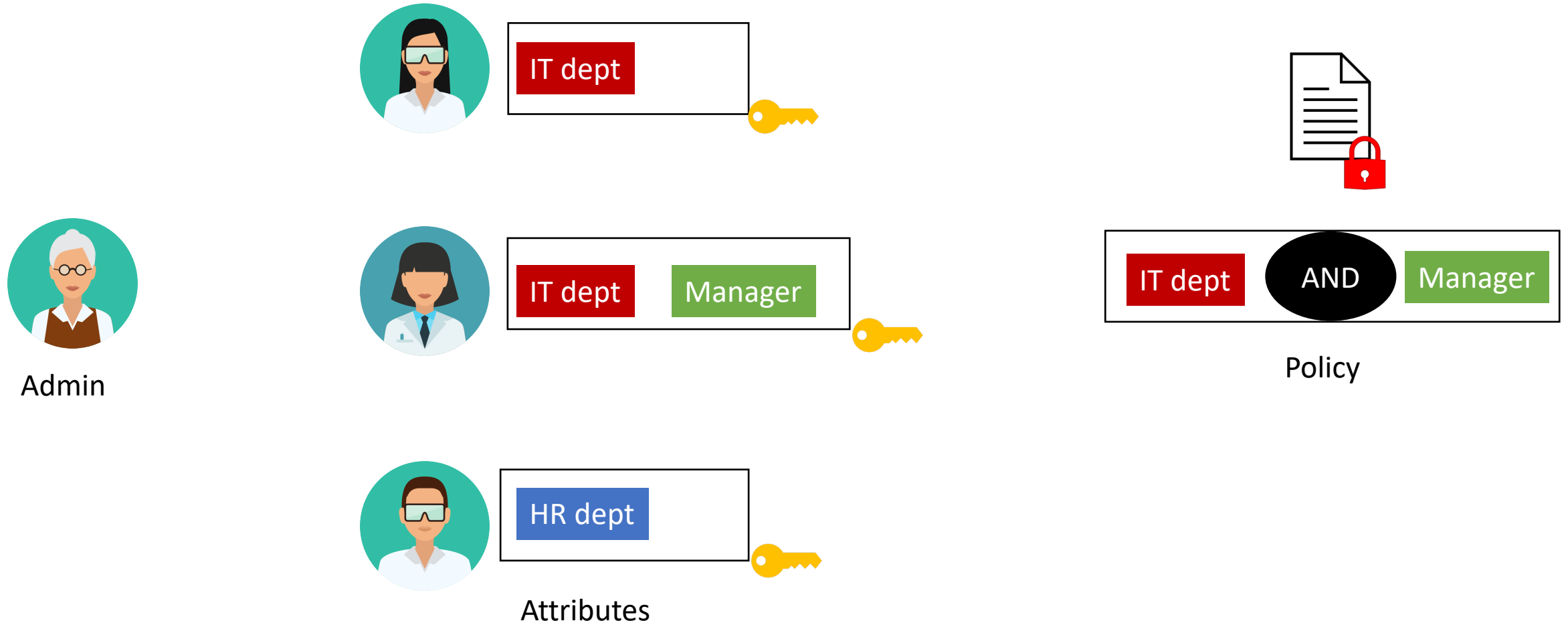
# It's not about encryption it's about **key management**



# ABEBox

- **Key management system** to bring privacy on cloud shared files
  - Without any Trusted Third Party
- It **decouples** *access control* from *data transferring and synchronization*
- It runs **on top** of existing file sharing services
  - Serverless
- Provide solutions for peer **churn**
  - New users and revoked ones

# CP-ABE: Ciphertext-Policy Attribute-Based Encryption



# CP-ABE for file sharing

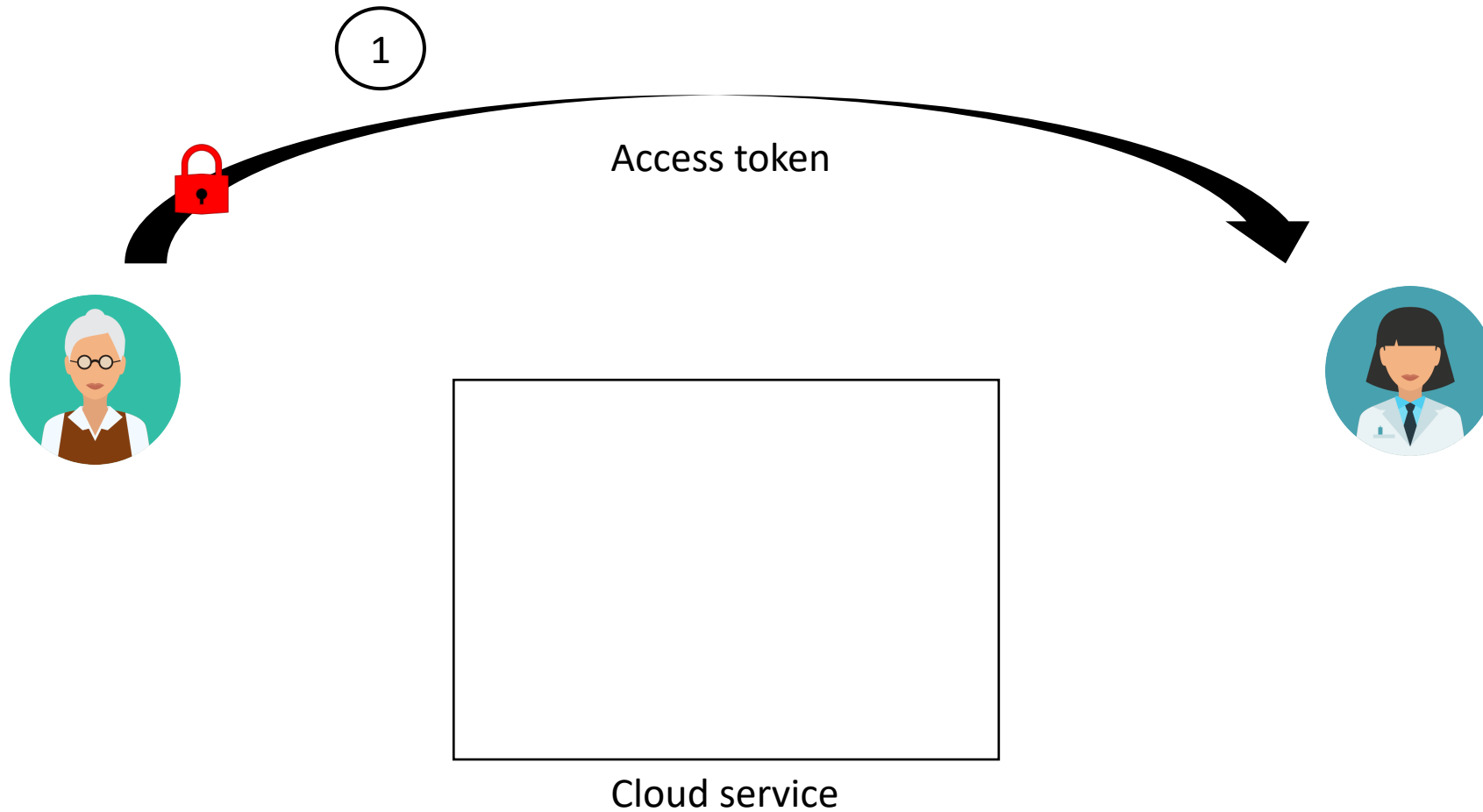
- **Pro**

- Attribute Based Access Control (ABAC) fits nice the needs for flexibility
- Newcomers can be just provided with a single key with the right set of attributes

- **Cons/Still missing**

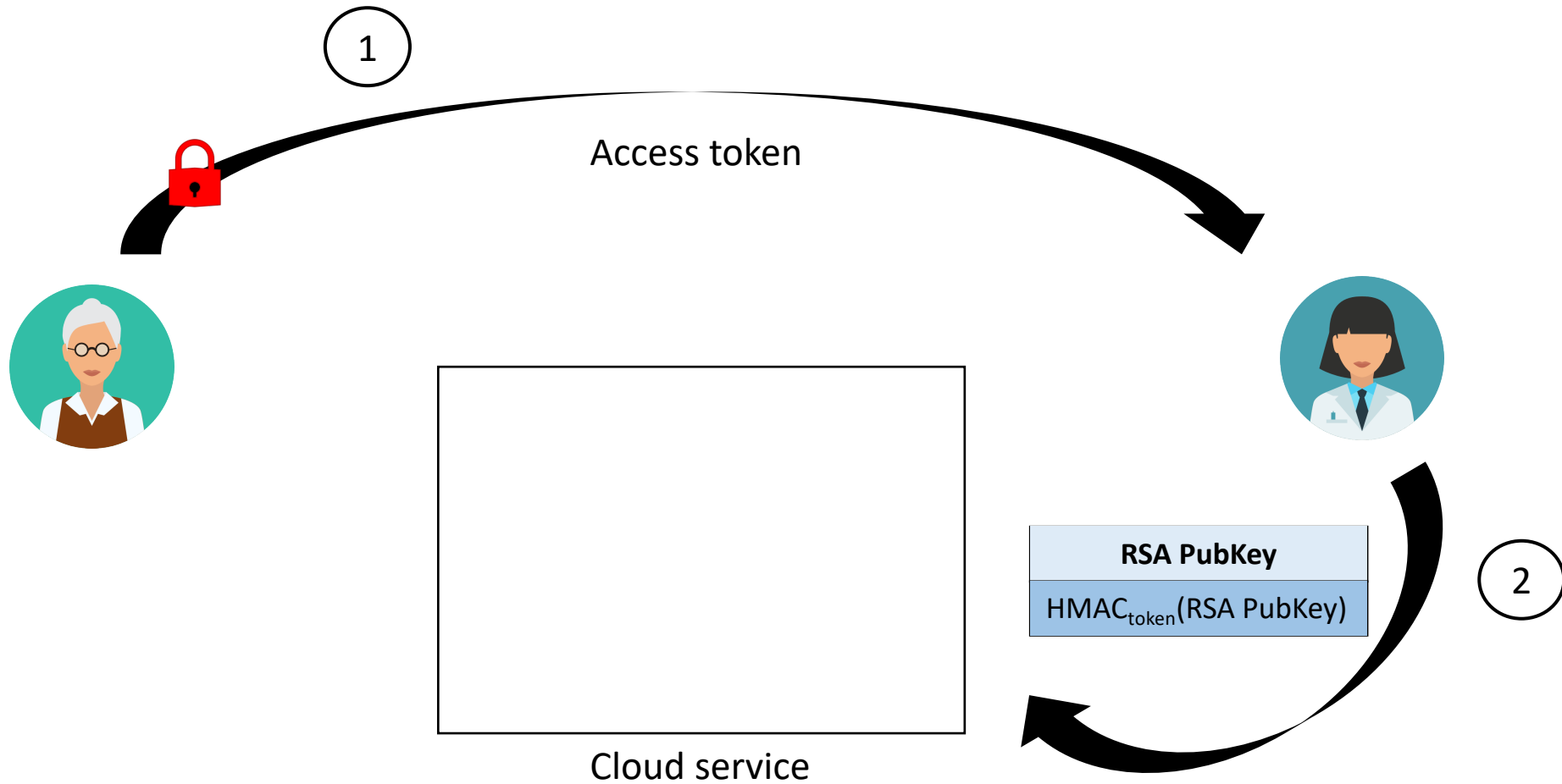
- How can we send ABE secret key to users?
- Revocation is still not addressed
- CP-ABE is tremendously SLOW (~1000 times slower than RSA)

# Providing ABE secret key

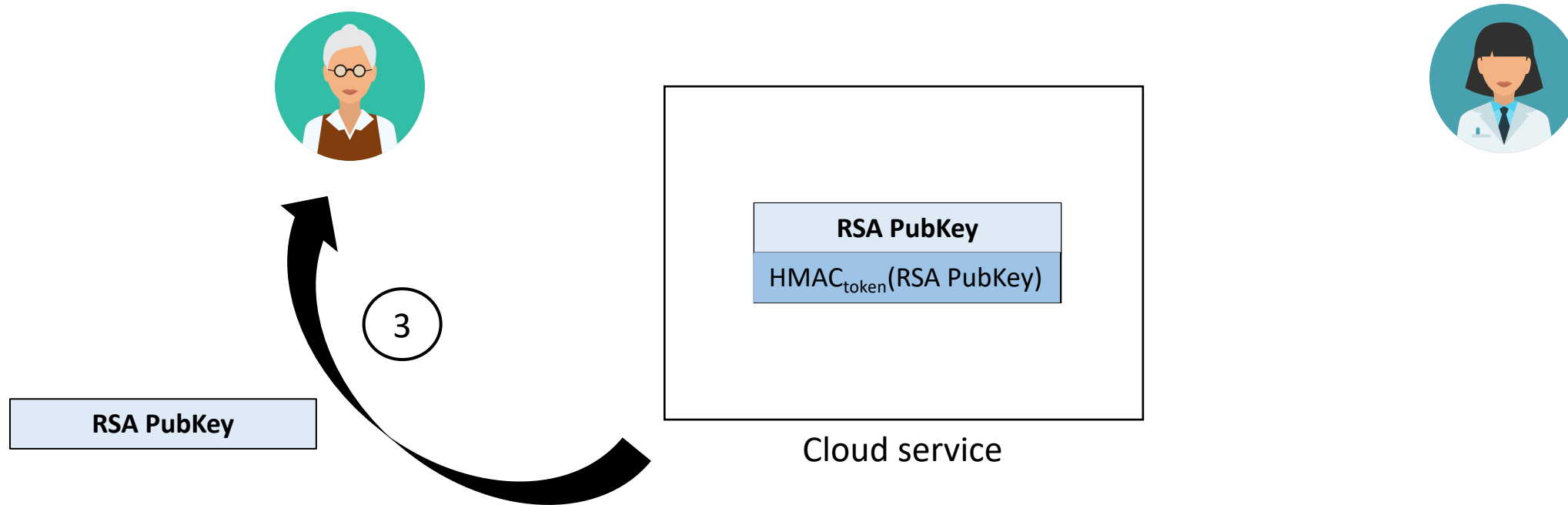




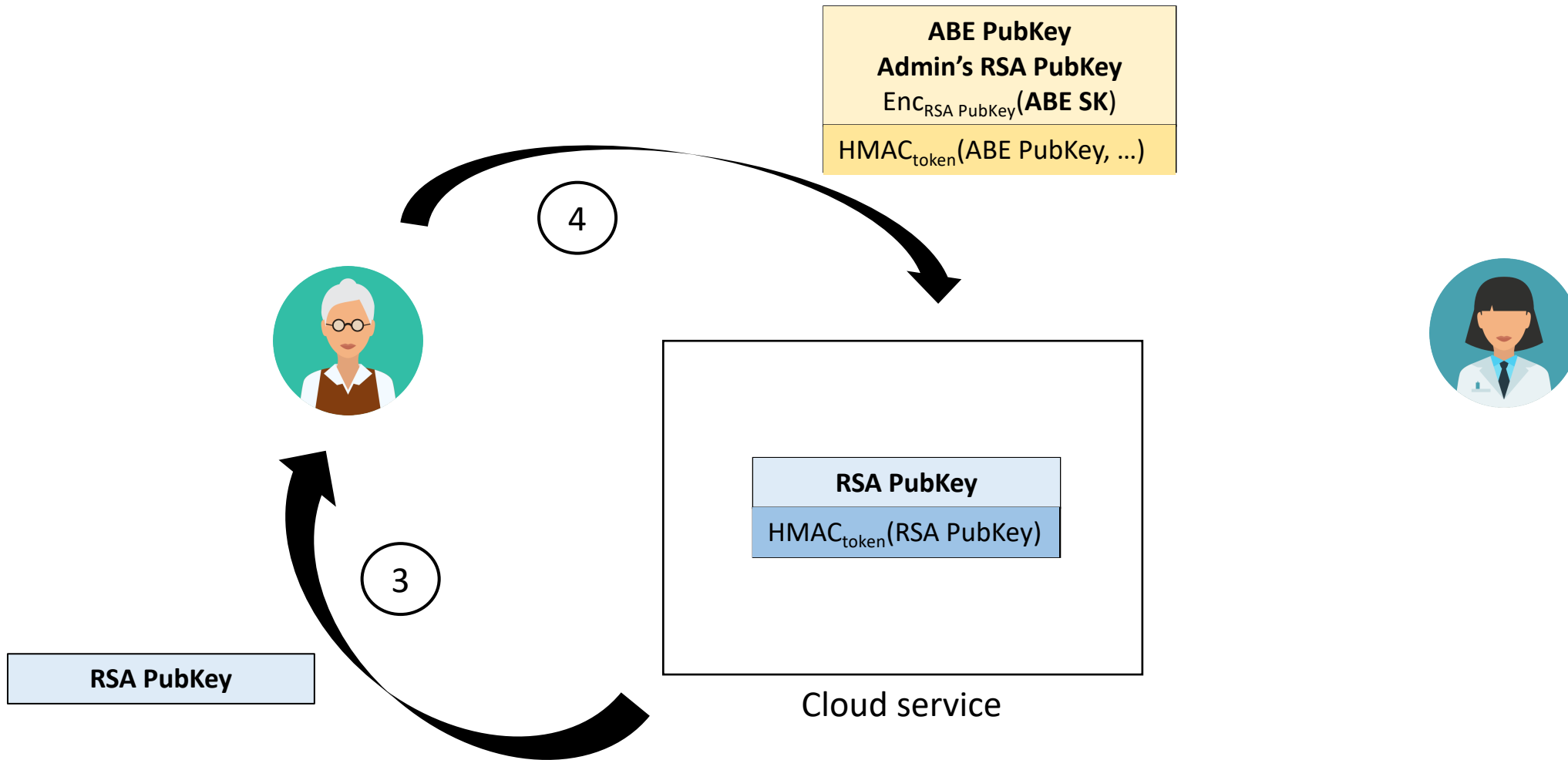
# Providing ABE secret key



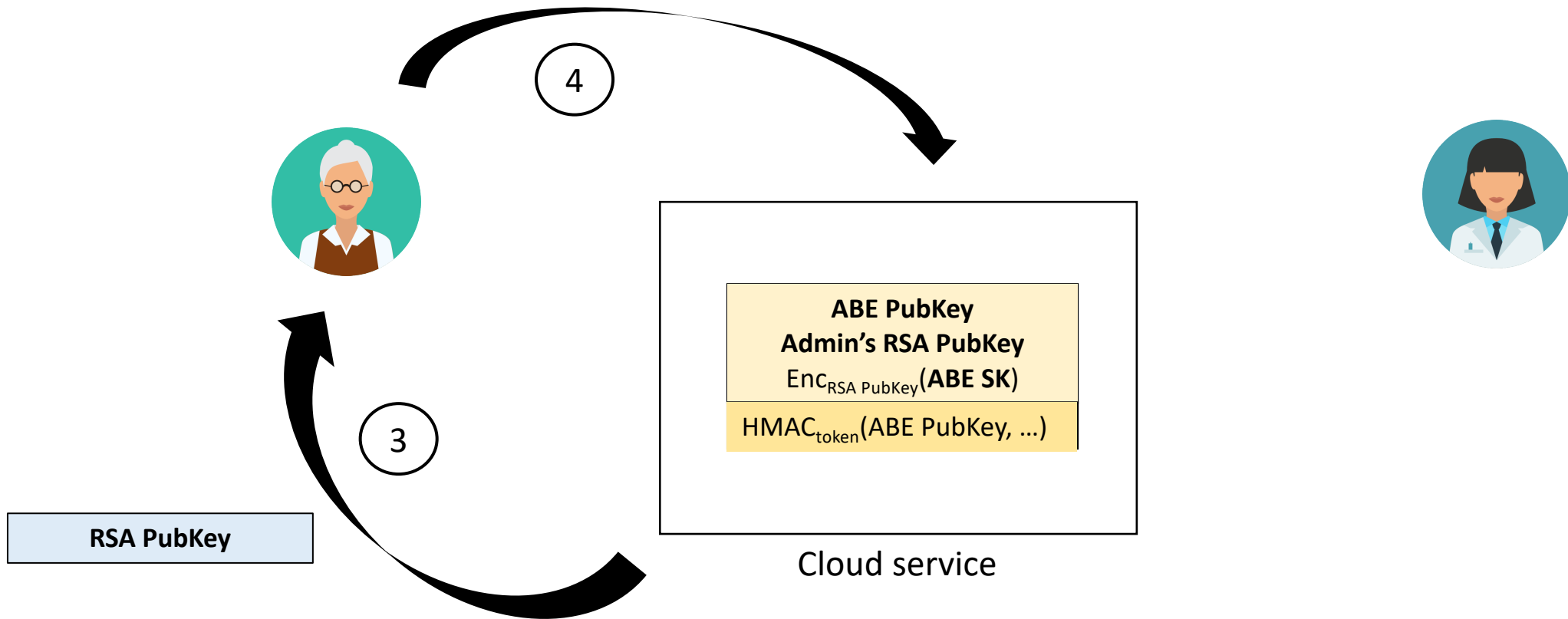
# Providing ABE secret key



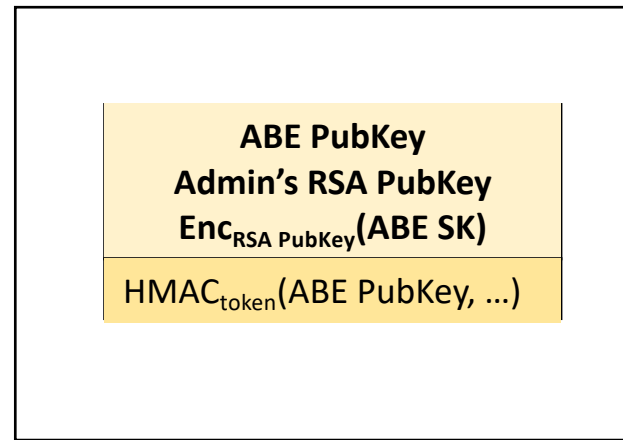
# Providing ABE secret key



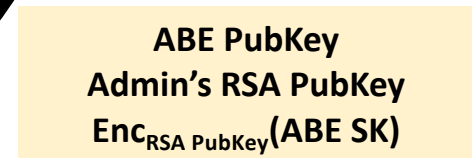
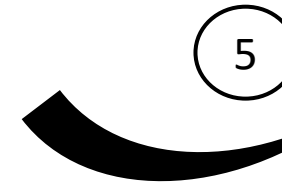
# Providing ABE secret key



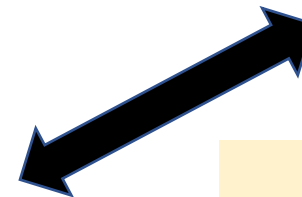
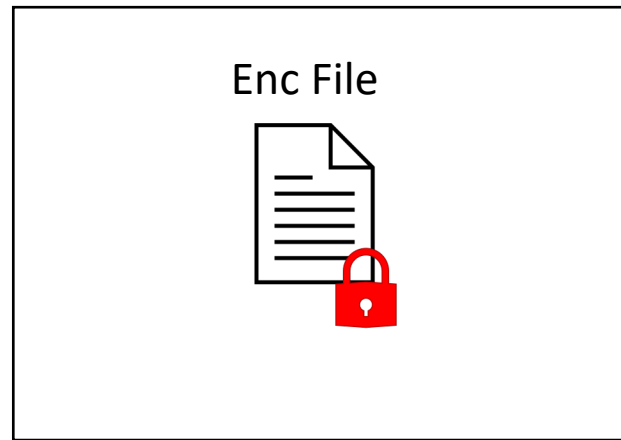
# Providing ABE secret key



Cloud service

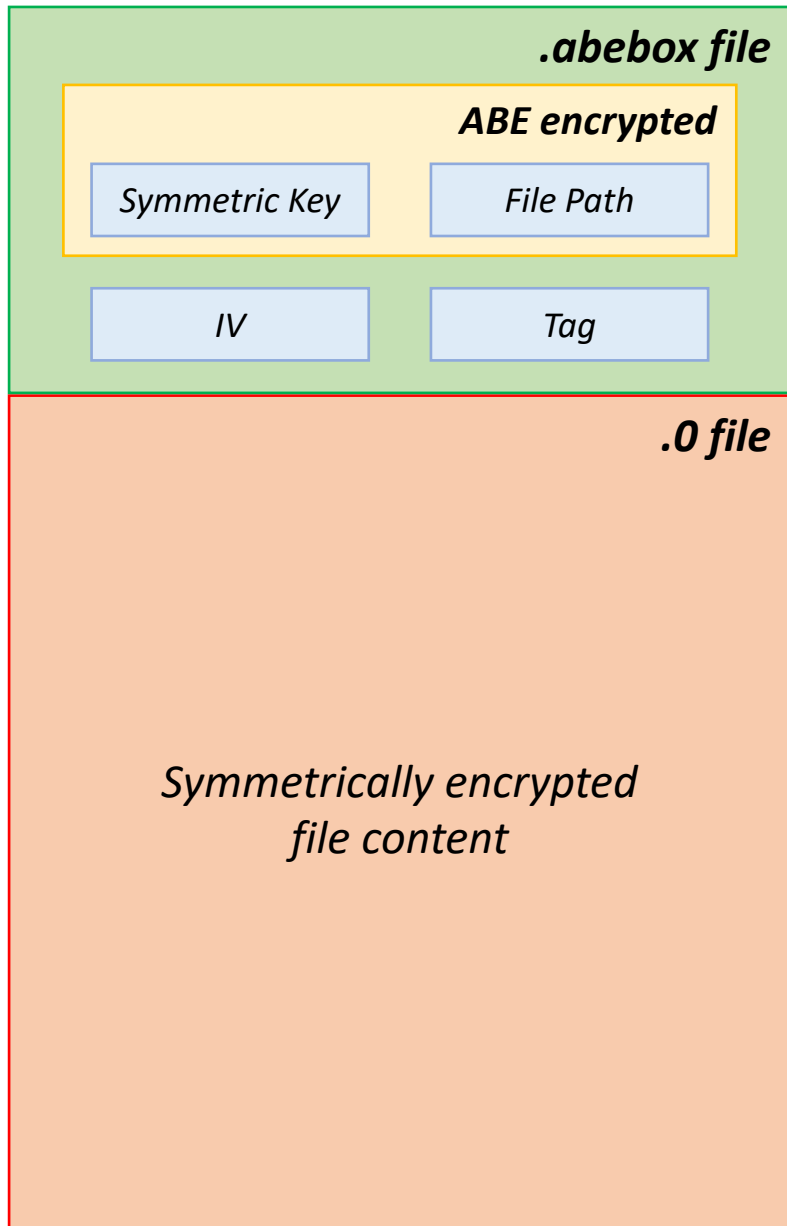



# Share Files



**ABE PubKey**  
**ABE SK**



Cloud service



```
{  
  enc metadata:  
    {  
       sym_key: Symmetric Key,  
      file_path: File Path  
    },  
  iv: IV,  
  tag: Tag (AES-GCM)  
}
```












# Protected Data File Structure

# ABEBox

Name	
 myfile1.png	
 myfile2.json	

Plaintext files local folder



Name	
▼ repo	
 8382162a-7749-45b3-903d-4297afaf2dde.abebox	
 8382162a-7749-45b3-903d-4297afaf2dde.0	
 0110cc21-7364-4154-b630-58fab6b0464a.abebox	
 0110cc21-7364-4154-b630-58fab6b0464a.0	
 27a10020-97e8-4cb8-8d86-1ac96e60118e.abebox	
 27a10020-97e8-4cb8-8d86-1ac96e60118e.0	
▼ pub_keys	
 826ba2465fd23d46ad20...ba75298876b94f7324cf	
 7a9ac3d62f4eeaf2c0946...9349ddabeb4a411318df	
▼ keys	
 826ba2465fd23d46ad20...75298876b94f7324cf.sk	
 7a9ac3d62f4eeaf2c0946...49ddabeb4a411318df.sk	
▼ attributes	
 attributes_list.json	

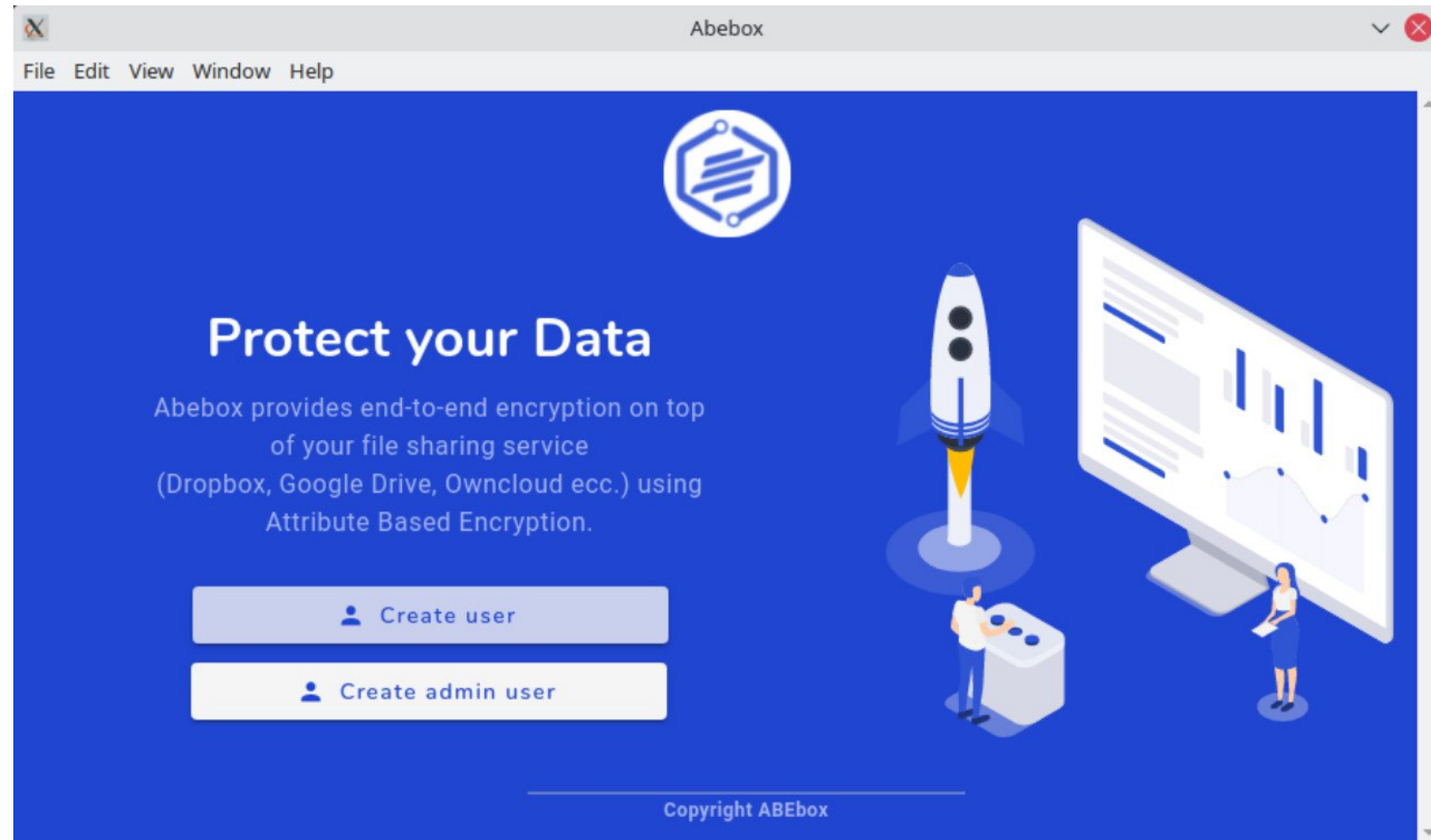
Shared folder



# Electron version

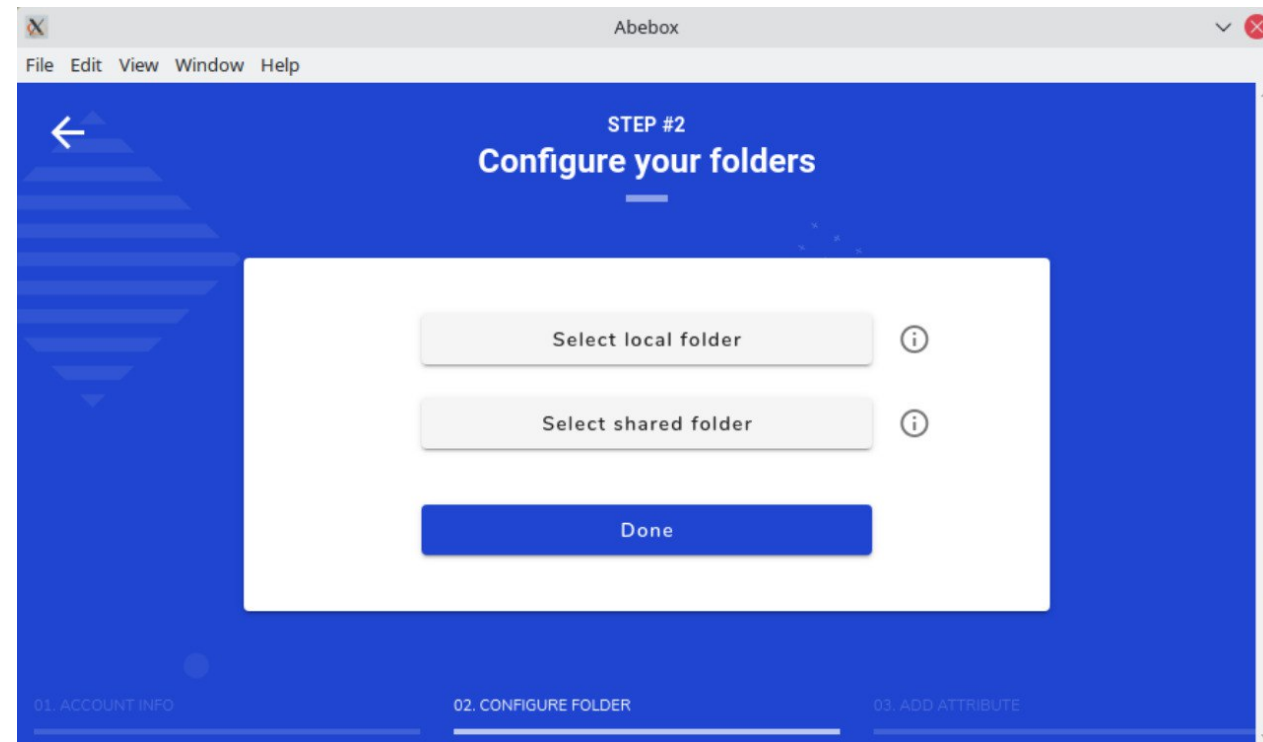


- Multi platform app
  - Win, linux, mac
- GUI for configuration
  - policies, attributes, users

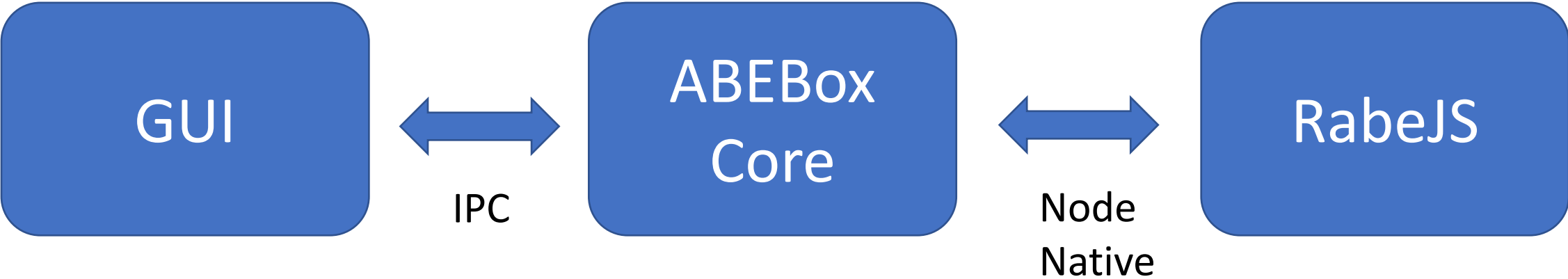


# ABEBox operational flow

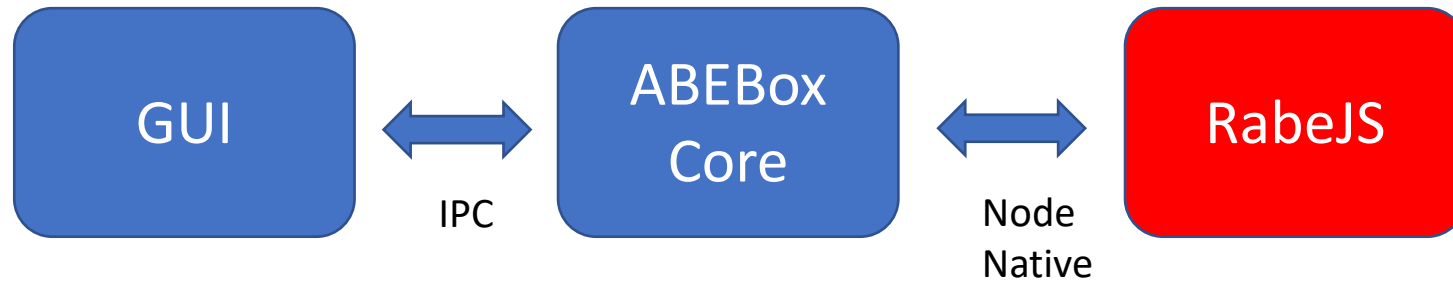
- Invited User or Admin?
- Users
  - Select folders
  - Insert token
- Admin
  - Set attributes
  - Add users, assign them attributes and get their tokens
  - Select folders



# The ABEBox App



# The ABEBox App



- **First** port of Attribute Based Encryption on Web (JS)
  - We started from the Fraunhofer's RABEJS Rust ABE library and create web-assembly
  - Then we develop interfaces to import the modules in JS as Node Native

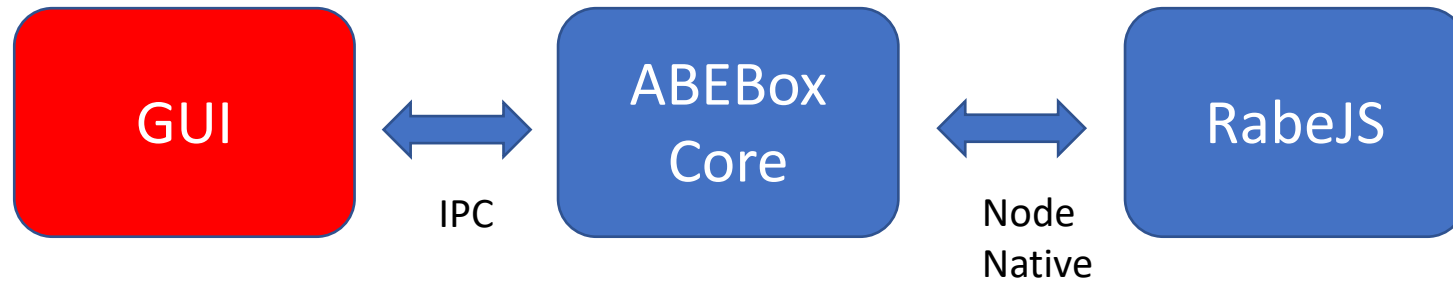
# The ABEBox App



- Key management
- Encryption and decryption
- File synchronization and handling (chokidar)
- User management

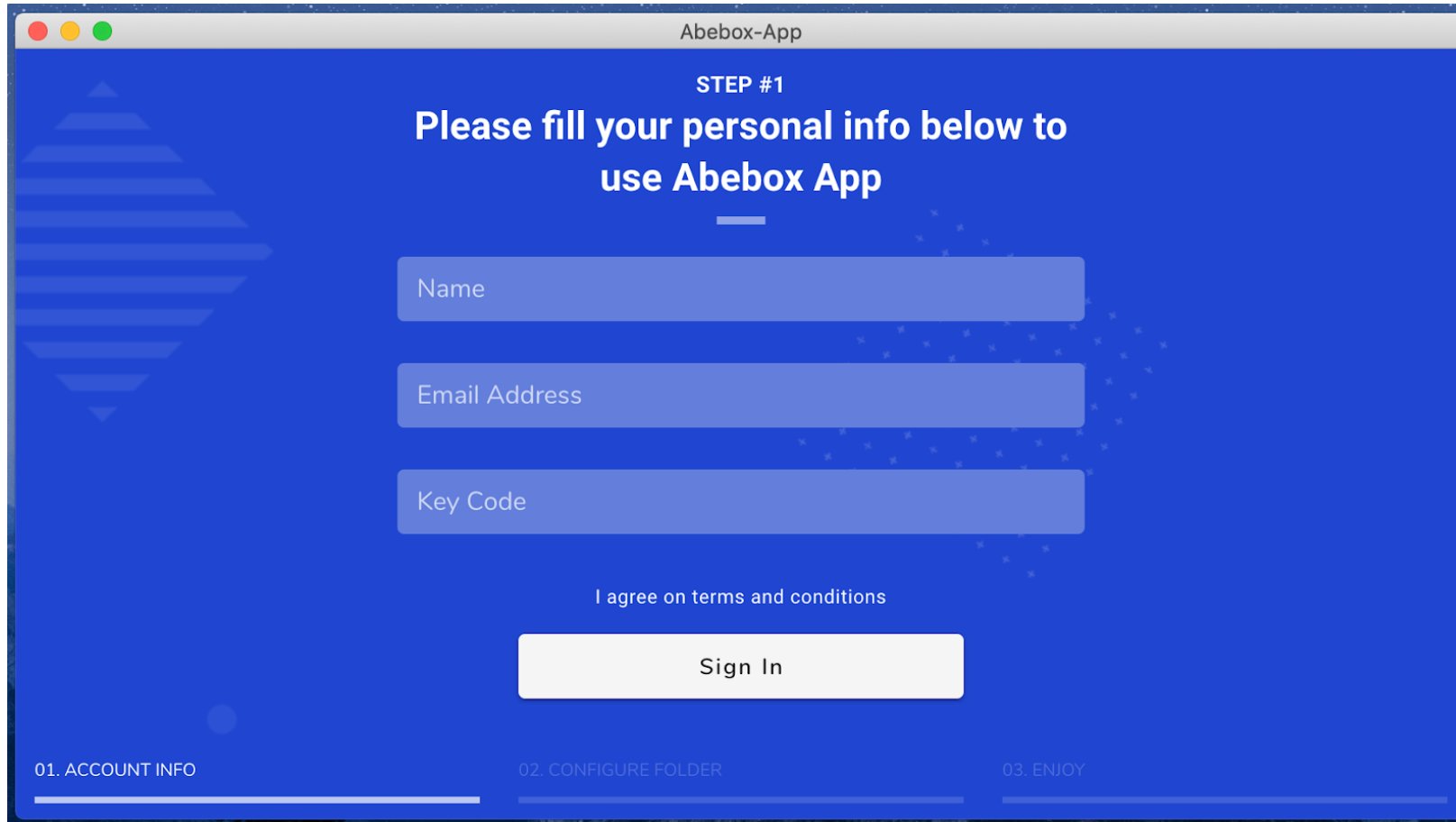
Number of Node modules	11
Lines of Code	2007
Tests	32
Line of Code (tests)	966

# The ABEBox App



- Electron + VUE + Vuetifyjs
- Admin and User views
- Interface for policy creation
- User and file management

# The ABEBox App (User view)



The screenshot shows a web browser window titled "Abebox-App". The page has a dark blue background with a subtle pattern of white stars and a large, faint, stylized arrow graphic on the left. The main heading reads "STEP #1 Please fill your personal info below to use Abebox App". Below this are three input fields: "Name", "Email Address", and "Key Code". A checkbox labeled "I agree on terms and conditions" is positioned above a white "Sign In" button. At the bottom, a progress bar shows three steps: "01. ACCOUNT INFO" (highlighted with a white line), "02. CONFIGURE FOLDER", and "03. ENJOY".

Abebox-App

STEP #1

Please fill your personal info below to use Abebox App

Name

Email Address

Key Code

I agree on terms and conditions

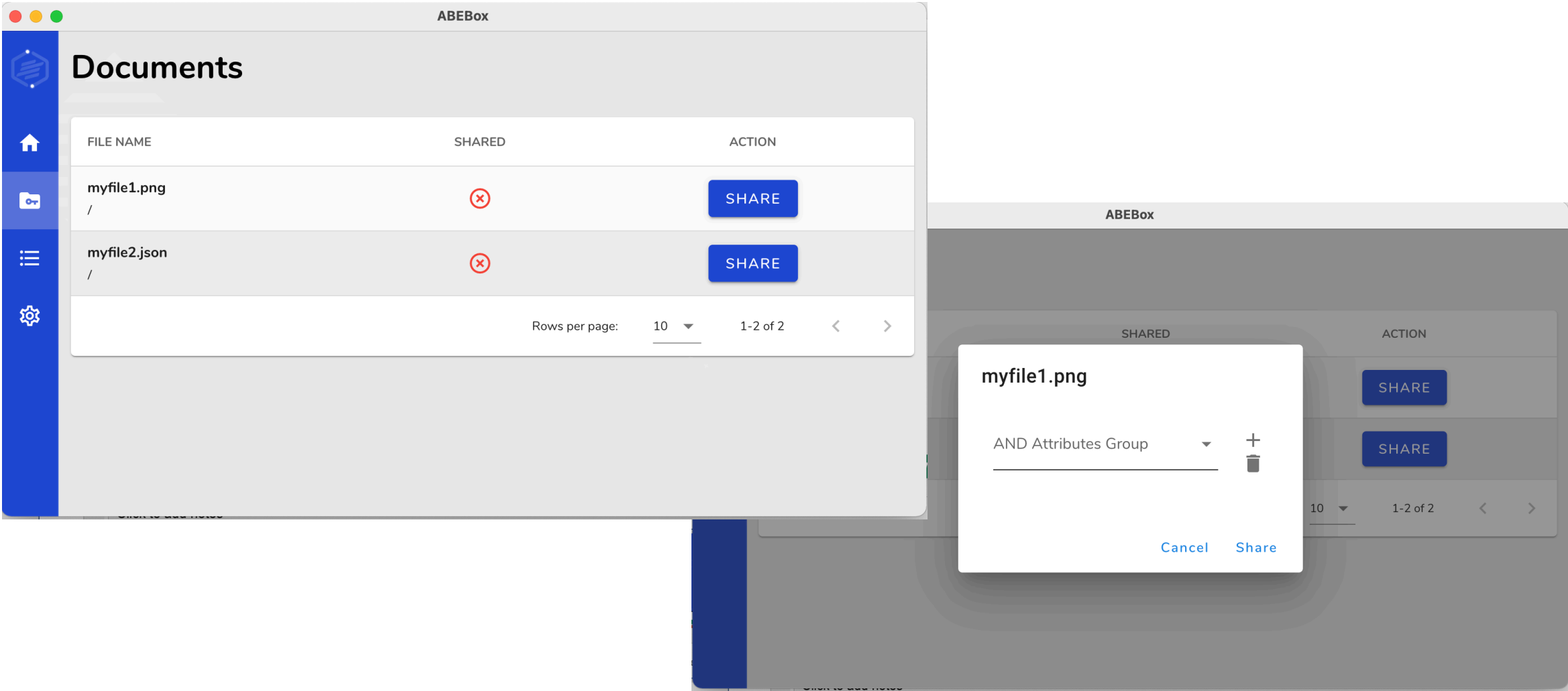
Sign In

01. ACCOUNT INFO

02. CONFIGURE FOLDER

03. ENJOY

# The ABEBox App (Documents and share)





# Website

<http://abebox.netgroup.uniroma2.it/>



[HOME](#)

[HOW DOES IT WORK](#)

[SOURCE](#)

[DOWNLOAD](#)

[Download](#)

## Protect your Data

Abebox provides end-to-end encryption on top of your file sharing service (Dropbox, Google Drive, Owncloud ecc.) using Attribute Based Encryption.

[Download](#)

[Github](#)



# Testing

- Testing groups:
  - 50 Computer Science 101 students (Electronic and Internet Engineering)
  - 6 e-health students (Electronic Engineering)
- Testing methodology
  - Interview & Questionnaires
- Result (summary)
  - Almost all succeeded in accessing a shared file
  - Setup problems installing a new (uncertified) app on some OSs (OS security policies)
  - Major bug reported and patched

# Follow up

- Invitation to SRE Conference (Paris 1-2 March, cancelled for FORCE MAJEURE)  
<https://www.sre2022.eu/>
- Deep dive with Owncloud engineers about E2E Encryption of EFSS (Online 22 Feb)

# Conclusion

- E2E encryption for cloud file sharing systems is more a **key management problem** than an "encryption" problem
- **Attribute Based Encryption** can solve part of problems
- We propose some solutions for the **revocation** problem
- We implemented such solution on a **multi-platform application** and release the code as **open-source**

<http://abebox.netgroup.uniroma2.it/>

*binaries*

<https://github.com/netgroup/abebox-electron>

*code*

# Thanks!

Pierpaolo Loreti

*[pierpaolo.loreti@uniroma2.it](mailto:pierpaolo.loreti@uniroma2.it)*

*Pierpaolo Loreti*

*Emanuele Raso*

*Giuseppe Bianchi*



*Innovation programme*



*Horizon 2020 innovation programme  
grant agreement No.787149*