

# Cryptpad

## An Open-Source Encrypted Collaborative Office Suite

---

Fabrice Mouhartem

December 20th, 2023

AMAC/CAS<sup>3</sup>C<sup>3</sup> Seminar, Grenoble

XWiki (CryptPad)



# Collaborative Editing

**Goal:** allow users to simultaneously edit the same file

# Collaborative Editing

**Goal:** allow users to simultaneously edit the same file

Solution	Example	Pros	Cons
Synchronised folder	Syncthing	Easy to use	Conflicts
Version System	Git	Conflict management	Learning curve
Dedicated software	Overleaf	Easy to use and conflict management	Can only be used for this purpose

# Collaborative Editing

**Goal:** allow users to simultaneously edit the same file

Solution	Example	Pros	Cons
Synchronised folder	Syncthing	Easy to use	Conflicts
Version System	Git	Conflict management	Learning curve
Dedicated software	Overleaf	Easy to use and conflict management	Can only be used for this purpose

- ▶ CryptPad is a dedicated software for collaborative document editing

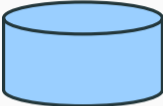
# Collaborative Editing

**Goal:** allow users to simultaneously edit the same file

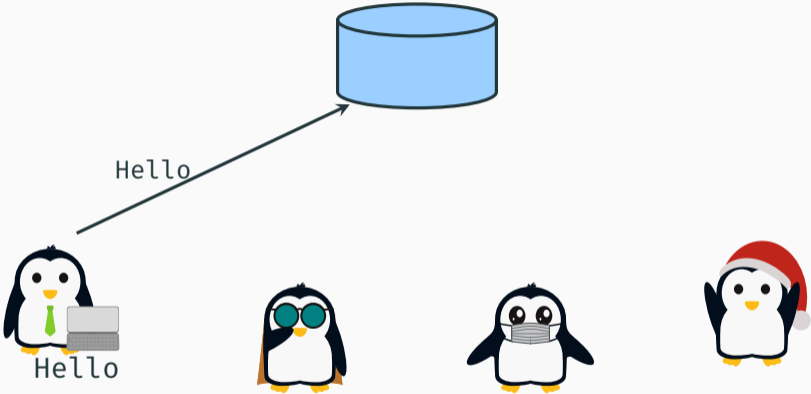
Solution	Example	Pros	Cons
Synchronised folder	Syncthing	Easy to use	Conflicts
Version System	Git	Conflict management	Learning curve
Dedicated software	Overleaf	Easy to use and conflict management	Can only be used for this purpose

- ▶ CryptPad is a dedicated software for collaborative document editing
- ▶ More than that: a collaborative office suite

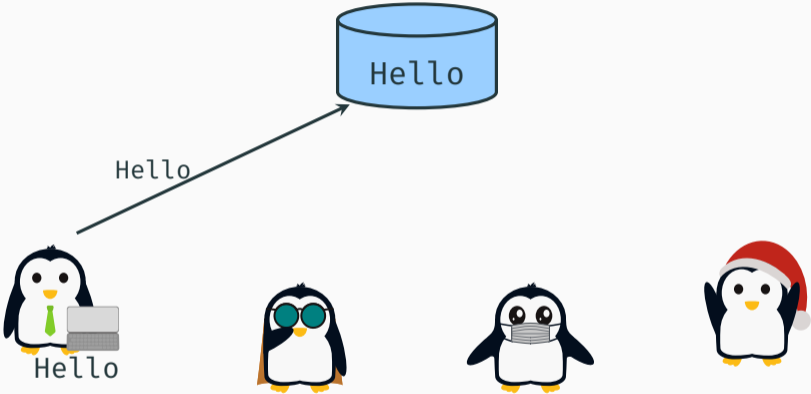
# Collaborative Editing



# Collaborative Editing

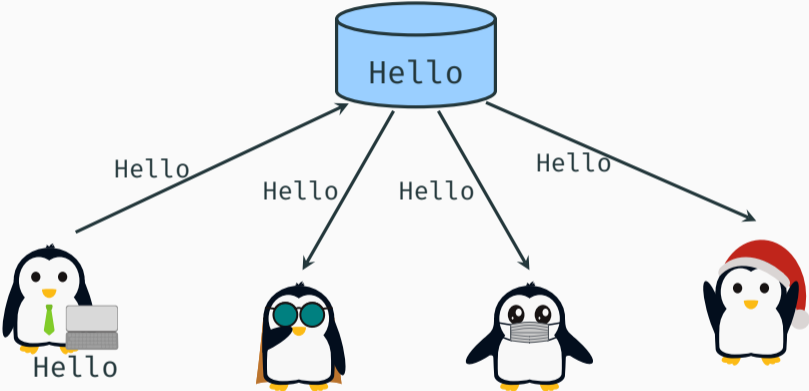


# Collaborative Editing

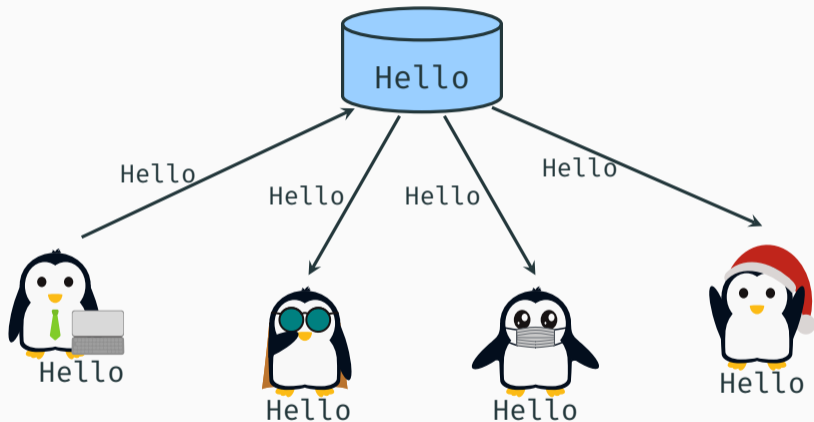




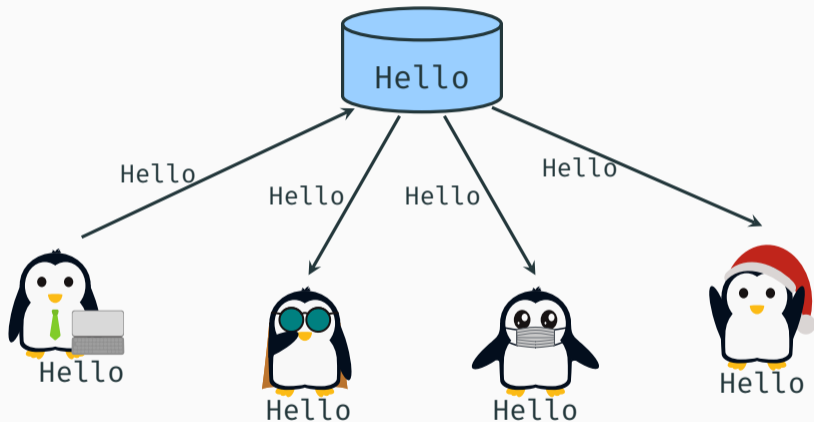
# Collaborative Editing



# Collaborative Editing



# Collaborative Editing



**Issue:** the broadcast server knows everything

The  
Intercept\_

NAOMI  
\_KLEIN



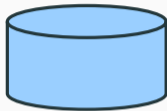
## India Targets Climate Activists With the Help of Big Tech

Tech giants like Google and Facebook appear to be aiding and abetting a vicious government campaign against Indian climate activists.

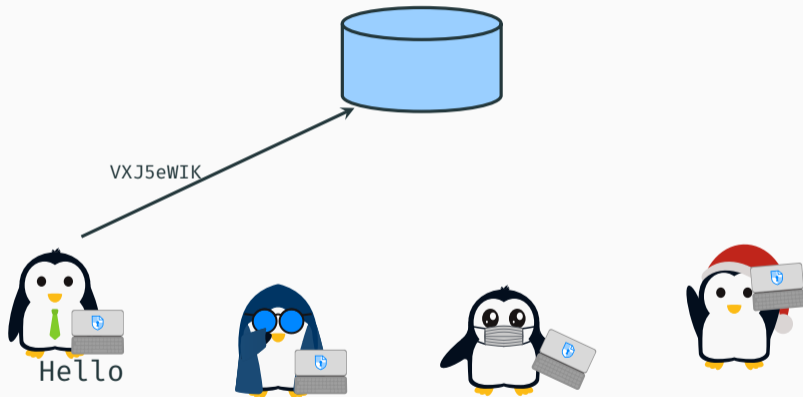
[Naomi Klein](#)

February 27, 2021, 9:00 a.m.

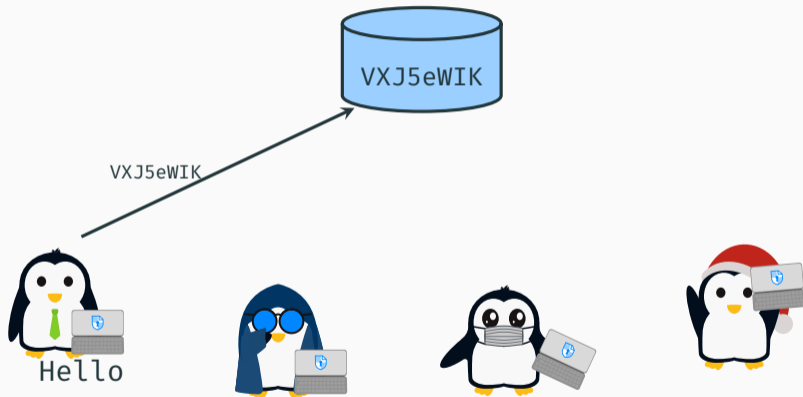
# Encrypted Collaborative Edition



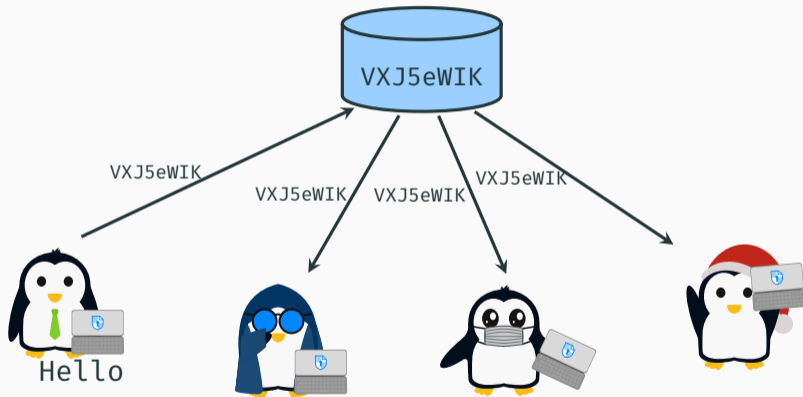
# Encrypted Collaborative Edition



# Encrypted Collaborative Edition

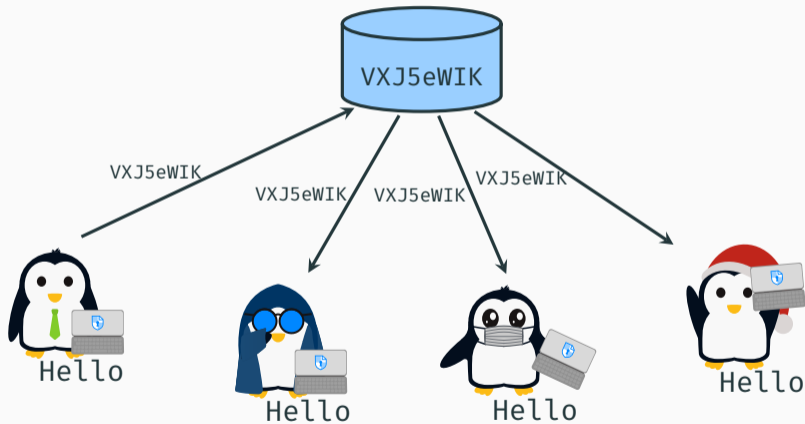


# Encrypted Collaborative Edition





# Encrypted Collaborative Edition



# Limitations of this Model

**Limitation:** the server knows metadata (IPs, connection patterns...)

#TOPTHEMA ALLGEMEIN PRESSEMITTELUNGEN

## NACH G7-LEAK: POLIZEI LEGT ÖFFENTLICHE PIRATENPARTEI-INFRASTRUKTUR LAHM

24. JUNI 2022



# Limitations of this Model

**Limitation:** the server knows metadata (IPs, connection patterns...)




A screenshot of a tweet from Greta Thunberg (@GretaThunberg) dated February 3, 2021. The tweet text reads: "Here's an updated toolkit by people on the ground in India if you want to help. (They removed their previous document as it was outdated.) #StandWithFarmers #FarmersProtest". Below the text is a link to a CryptPad document, represented by a blue icon of a document with a shield. The tweet shows 13.3K reposts, 2,445 quotes, 50.2K likes, and 318 bookmarks.

**Greta Thunberg** @GretaThunberg

Here's an updated toolkit by people on the ground in India if you want to help. (They removed their previous document as it was outdated.)  
[#StandWithFarmers](#) [#FarmersProtest](#)

 CryptPad



8:52 PM · Feb 3, 2021

13.3K Reposts 2,445 Quotes 50.2K Likes 318 Bookmarks

## Kerckhoff's principle

A cryptosystem should be secure, even if everything about the system, except the secret keys, is public knowledge.

## Kerckhoff's principle

A cryptosystem should be secure, even if everything about the system, except the secret keys, is public knowledge.

### ► AGPLv3 License:

The GNU Affero General Public License is a free, copyleft license for software and other kinds of works, specifically designed to ensure cooperation with the community in the case of network server software.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, our General Public Licenses are intended to guarantee your freedom to share and change all versions of a program—to make sure it remains free software for all its users.

## Kerckhoff's principle

A cryptosystem should be secure, even if everything about the system, except the secret keys, is public knowledge.

- ▶ AGPLv3 License:  
you can reuse and modify our code, but users must have access to the source code they are running.

## The privacy we want (informal)

No **untrusted authority** can infer personal information, document content, or collaborators.

## The privacy we want (informal)

No **untrusted authority** can infer personal information, document content, or collaborators.

- ▶ The server is a passive adversary (honest-but-curious)
  - Cannot do much if it serves a different code
  - Administrators can always delete a file
- ▶ We want to protect users' data even if the server becomes corrupt



## Goals:

- ▶ Synchronous document edition
- ▶ Conflicts management
  - Secure communications
  - User-friendliness

## Goals:

- ▶ Synchronous document edition
- ▶ Conflicts management
  - Secure communications
  - User-friendliness

**Relations:** • and ▶ are separated while ■ depends on •

- ▶ A broadcast protocol: Netflux
  - Each client sends patches of their change
  - The server relays messages in the same order to everyone
  - Each client decrypts these patches and apply them

# Collaboration Layer

- ▶ A broadcast protocol: Netflux
  - Each client sends patches of their change
  - The server relays messages in the same order to everyone
  - Each client decrypts these patches and apply them
- ▶ No offline editing is possible (read-only remains possible)

# Collaboration Layer

- ▶ A broadcast protocol: Netflux
  - Each client sends patches of their change
  - The server relays messages in the same order to everyone
  - Each client decrypts these patches and apply them
- ▶ No offline editing is possible (read-only remains possible)
- ▶ Storage: ChainPad
  - Documents are a list of patches + checkpoints
  - Everything is a document

## ► Identification

- Authenticated public-key encryption keys ( $pk, sk$ ), and a symmetric encryption key  $k$  are derived from username + password

# Cryptography Layer

- ▶ Identification
  - Authenticated public-key encryption keys ( $pk, sk$ ), and a symmetric encryption key  $k$  are derived from username + password
- ▶ Create a document
  - Upon creation generate a random string `editKeyStr`
  - Encrypt `editKeyStr` + the URL of the document under  $k$  to store it

# Cryptography Layer

- ▶ Identification
  - Authenticated public-key encryption keys ( $pk, sk$ ), and a symmetric encryption key  $k$  are derived from username + password
- ▶ Create a document
  - Upon creation generate a random string editKeyStr
  - Encrypt editKeyStr + the URL of the document under  $k$  to store it
- ▶ Edit a document
  - (editKeyStr || pwd) is used to derive a document key  $k_d$  and a document signature key pair ( $vk_d, sk_d$ )
  - Encrypt a patch of your change under  $k_d$
  - Sign the patch under  $vk_d$  and send it to the server



## ► Right managements

- To share a read-only document, share only  $k_d$  + URL. As the receiver doesn't have  $sk_d$ , it cannot send modifications
- Registered users only: use an access list that embeds into the document metadata the verification keys of allowed users

## ▶ Right managements

- To share a read-only document, share only  $k_d$  + URL. As the receiver doesn't have  $sk_d$ , it cannot send modifications
- Registered users only: use an access list that embeds into the document metadata the verification keys of allowed users

## ▶ Share a document

- To a registered user
  - Encrypt keys + URL under respective receivers'  $pks$
  - Use of Netflix to send it to respective receivers
- To anyone
  - Generate URL with keys suffixed after a # sign

# A Special Case: Forms

Xmas Dinner 🎅

This form cannot be submitted anonymously

Please fill this form with your preference for Xmas Dinner! 🌟

1. Preferred Menu Required

Vegetarian 🍌

Vegan 🌱

Turkey 🦃

2. Do you have any other food restrictions? (allergies 🍷, intolerances 🥛, ...)

Gluten-free

3. Your question here?

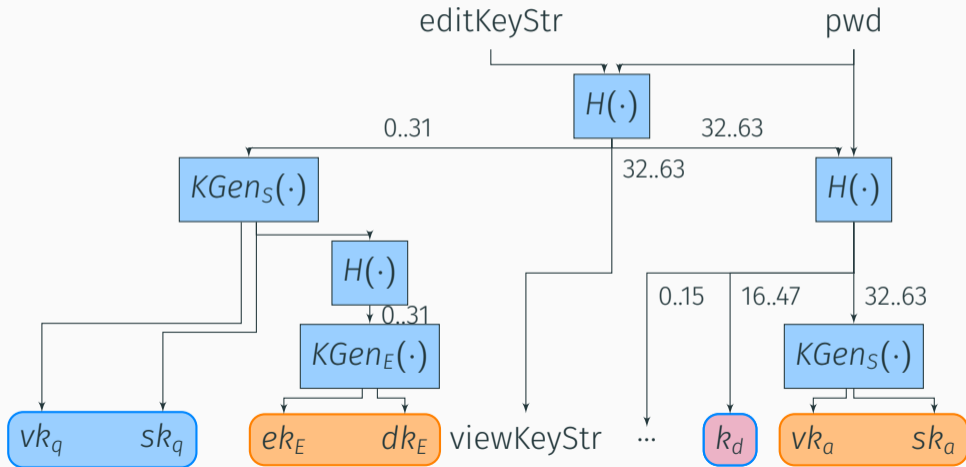
✓: Yes, ✗: No, ✓: Acceptable

SWAP AXES 🗑️	Wednesday 20/12/2023	Thursday 21/12/2023	Friday 22/12/2023
--------------	-------------------------	------------------------	----------------------

Forms are made of two documents in one, with linked right management:

- ▶ Questions
- ▶ Answers

# Forms: Our Solution



# Limitations

Our choices lead to several limitations:

## User Experience

- ▶ No password recovery
- ▶ Once a document is shared, you cannot revoke access
- ▶ Moderation issues

# Limitations

Our choices lead to several limitations:

## User Experience

- ▶ No password recovery
- ▶ Once a document is shared, you cannot revoke access
- ▶ Moderation issues
- ▶ No full-text search
- ▶ Cannot search a user from its username

# Possible solutions

**Problem:** revoke access rights of some users

# Possible solutions

**Problem:** revoke access rights of some users

**Now:**

1. Copy the document, delete the original and share the new one
2. Create a document with a document password that rotates when someone new is added



# Possible solutions

**Problem:** revoke access rights of some users

**Now:**

1. Copy the document, delete the original and share the new one
2. Create a document with a document password that rotates when someone new is added
3. Use of a document access list

# Possible solutions

**Problem:** revoke access rights of some users

**Now:**

1. Copy the document, delete the original and share the new one
2. Create a document with a document password that rotates when someone new is added
3. Use of a document access list

**Possible future solution:** key rotation

# Key Rotation

## Key idea

The document moderators can punctually request a refresh of the document keys that will overwrite the previously used key

# Key Rotation

## Key idea

The document moderators can punctually request a refresh of the document keys that will overwrite the previously used key

- ▶ **Usecase:** to share a document while hiding the history
- ▶ Provide the mechanism to upgrade toward more secure schemes
- ▶ Provide a starting point for forward secrecy
- ▶ **Drawback:** break anonymous access to new versions of the document

# Key Rotation

## Key idea

The document moderators can punctually request a refresh of the document keys that will overwrite the previously used key

- ▶ **Usecase:** to share a document while hiding the history
- ▶ Provide the mechanism to upgrade toward more secure schemes
- ▶ Provide a starting point for forward secrecy
- ▶ **Drawback:** break anonymous access to new versions of the document

**Going further:** for registered users only, possible to adapt MLS group chat user deletion

# Key Rotation

## Key idea

The document moderators can punctually request a refresh of the document keys that will overwrite the previously used key

- ▶ **Usecase:** to share a document while hiding the history
- ▶ Provide the mechanism to upgrade toward more secure schemes
- ▶ Provide a starting point for forward secrecy
- ▶ **Drawback:** break anonymous access to new versions of the document

**Going further:** for registered users only, possible to adapt MLS group chat user deletion  $\Rightarrow$  forward secrecy

# Password recovery

## Idea

Secret share your secrets and dispatch the shares to some contacts

## Idea

Secret share your secrets and dispatch the shares to some contacts

**In practice:** secret-share the secret key of CryptPad file containing your key



## Idea

Secret share your secrets and dispatch the shares to some contacts

**In practice:** secret-share the secret key of CryptPad file containing your key

**Drawback:** not a very used method nowadays, UI/UX need some works to have something usable

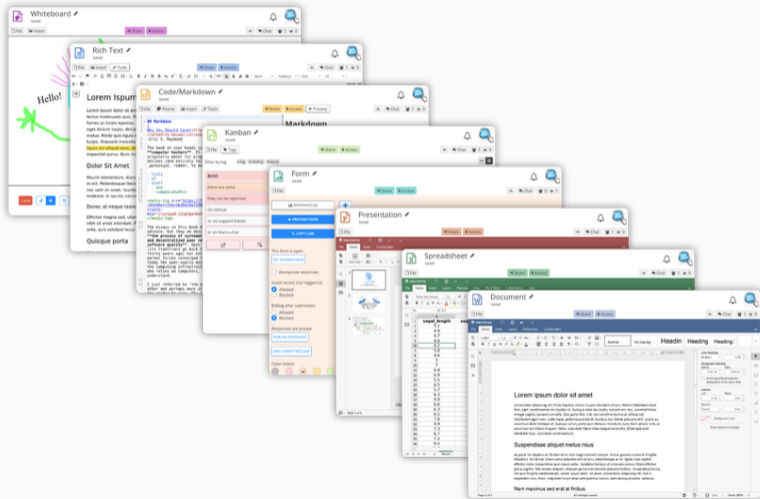
# Summary

- ▶ CryptPad is tightly intertwined with cryptography
- ▶ This use of cryptography as its core raises usability issues
- ▶ That can be solved with more cryptography

# Summary

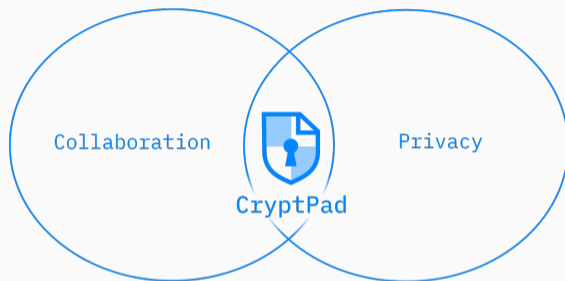
- ▶ CryptPad is tightly intertwined with cryptography
- ▶ This use of cryptography as its core raises usability issues
- ▶ That can be solved with more cryptography
- ▶ Real world limitations:
  - Computational resources (especially in mobile device)
  - Scalability
  - Libraries in javascript
  - Reliance on web browsers

# Demo



- ▶ Formalise the security of cryptpad
  - Provide an API
    - Lighter dependency on browsers
    - Provide synchronised storage
  - Post-quantum migration
- ▶ Implement & Deploy the above QoL improvements
  - nlnet Blueprints project: <https://nlnet.nl/project/CryptPad-Blueprints/>
- ▶ Security enhancement
  - Forward secrecy
  - Security against actively malicious servers

# Questions?



**Yes, you can have both**

- ▶ <https://cryptpad.org>
- ▶ <https://cryptpad.fr> for our public instance