CryptPad

CryptPad : a zero knowledge collaboration platform

Pass the Salt 2022

Ludovic Dubost,
XWiki SAS/CryptPad

Who am I ?

- Ludovic Dubost, President of XWiki SAS
- Creator of XWiki - Entreprise Wiki used by 7000 companies including big ones (Amazon, Lenovo)
- 17 years of Open Source
- 40 employees paid to contribute or help fund it
- XWiki SAS has launched CryptPad 6 years ago

Why encryption ?

- « There is no Cloud, just other people’s computers »
- In the Cloud, data has more and more value and is leveraged by providers
- RGPD application is a joke
- Data are not secured properly

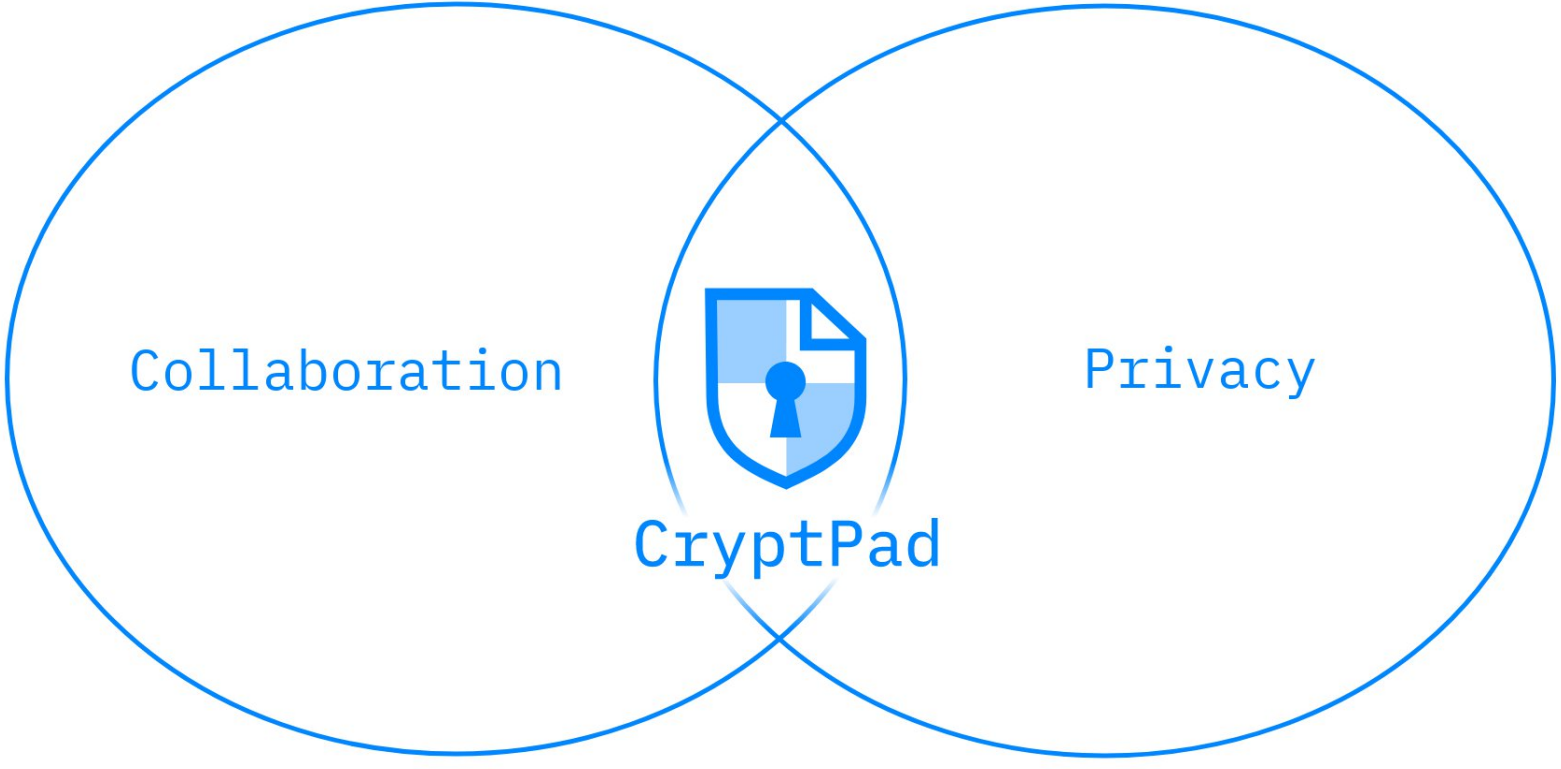
A new approach to securing web application -> CryptPad

Security before e2ee

- It’s all about trust
  - Administrators can access everything
  - Situation has been widely accepted (let’s sign contracts instead)
- Impossible to guarantee confidentiality of data in the Cloud
  - The manager of the Cloud service has access
  - Companies like it because they can leverage it for analytics and marketing

Encryption can change this

CryptPad - Key Principles



Yes, you can have both

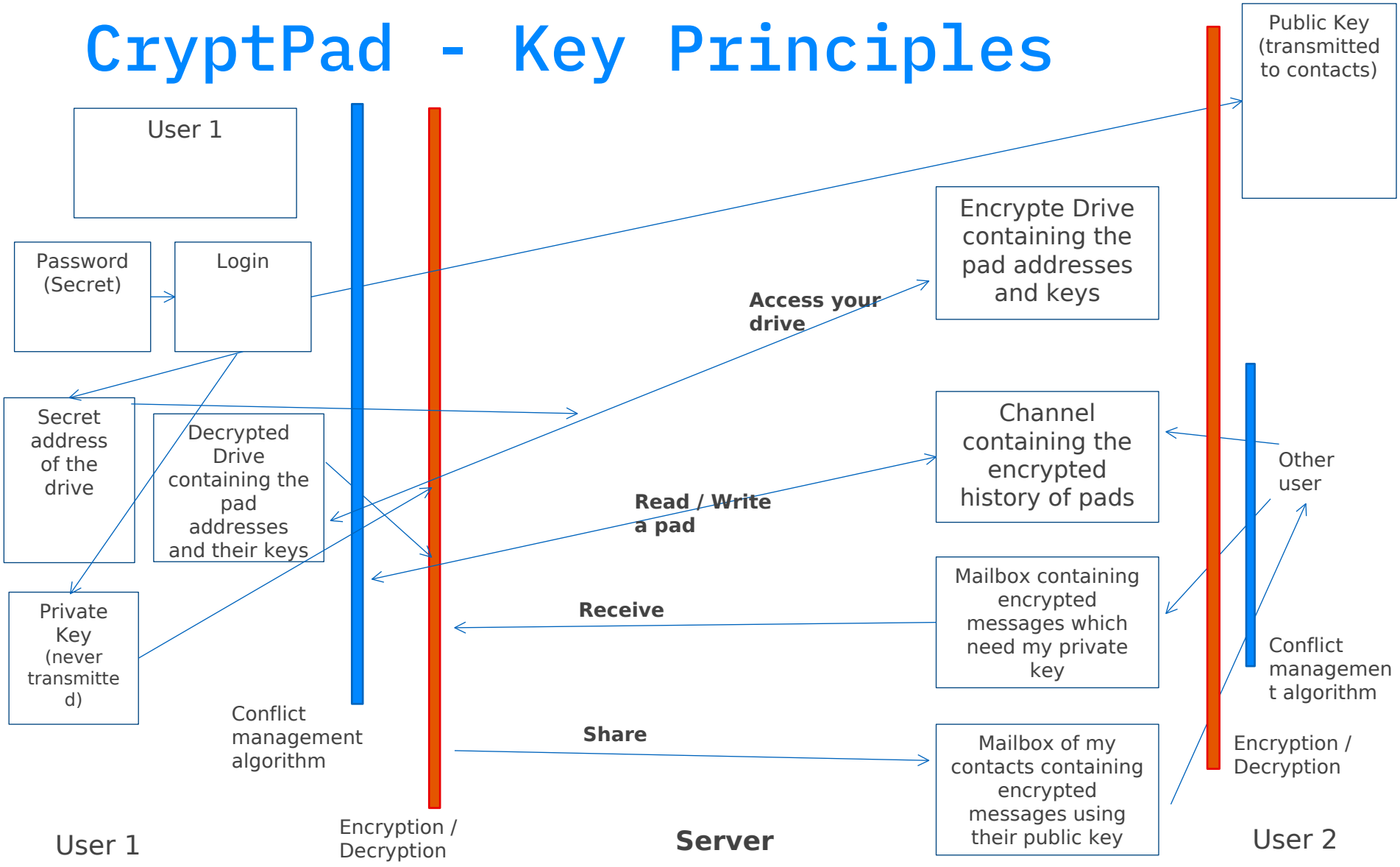
CryptPad - Key Principles

- Encrypted Documents **which can be edited in realtime**
- (**Real**) end-to-end encryption
- Key Management with secure and private key sharing

The manager of the server cannot read the data

and also not recover it

CryptPad - Key Principles



With encryption

- ZeroTrust Security
- Self-hosting : High level of confidentiality towards your system administrators
- Cloud : reduce the trust level needed of your cloud provider
- The Client code still needs to be verified for integrity and security issues

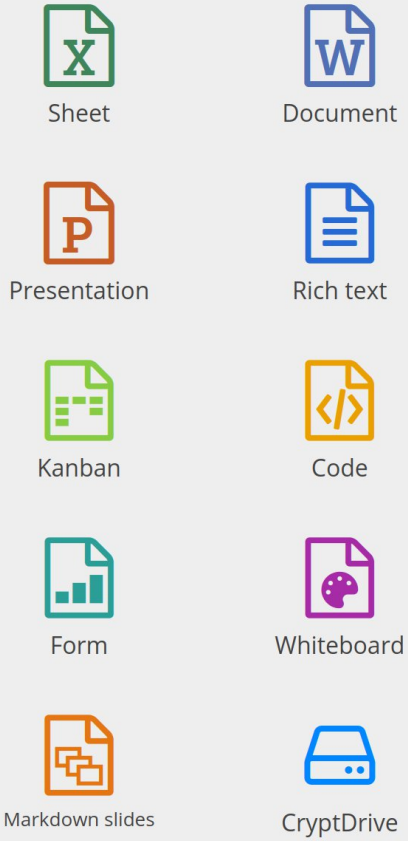
CryptPad: fonctionnalities

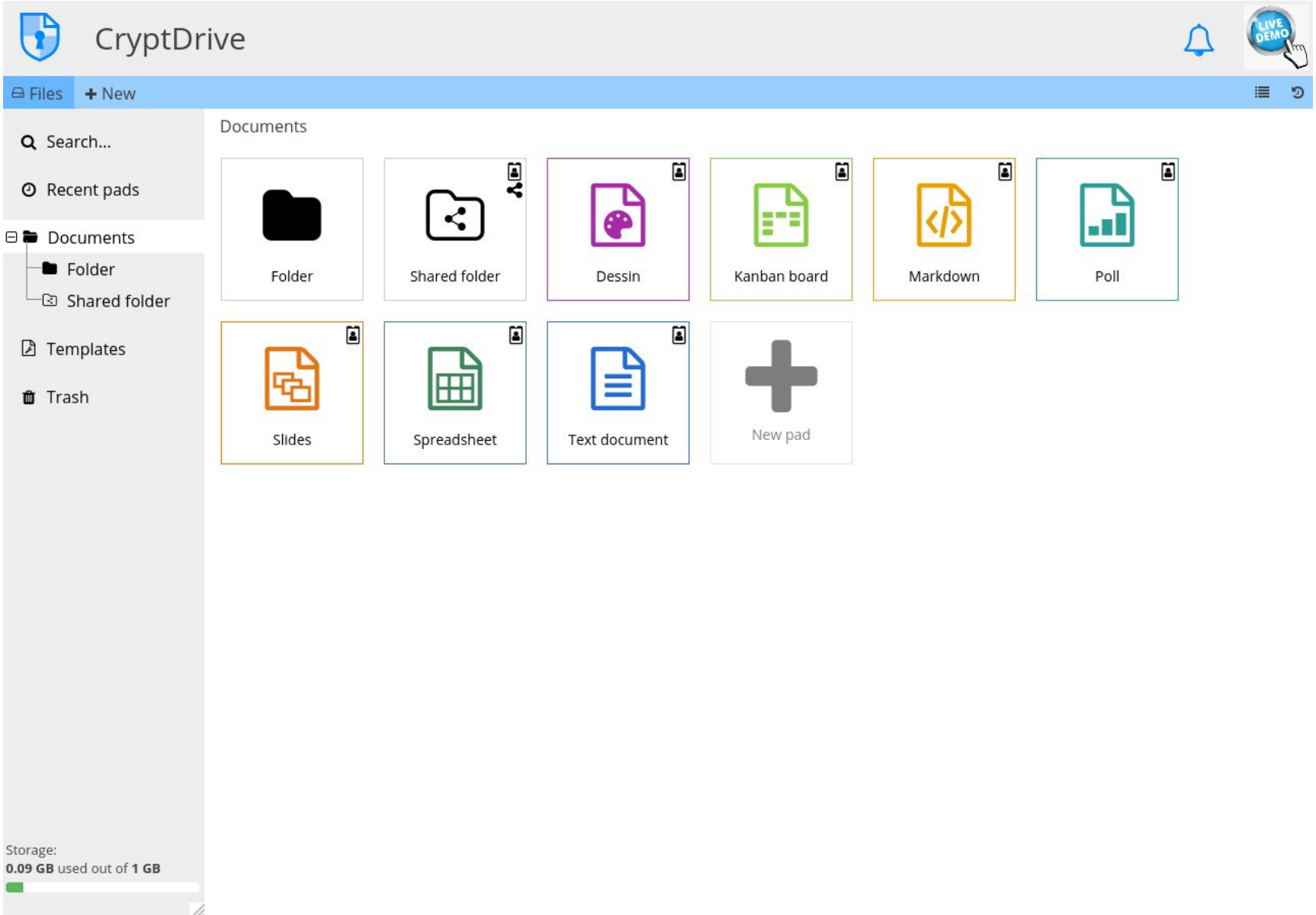
- Many applications:
  - Pad Wysiwyg / HTML
  - Document (compatible with Word / OnlyOffice)
  - Sheet(compatible with Excel / OnlyOffice)
  - Presentation (compatible with Powerpoint / OnlyOffice)
  - Kanban
  - Code (Markdown)
  - Forms
  - Whiteboard
  - Calendar
- CryptDrive
- Sharing functions
- Teams

CryptPad: Demo

CryptPad

Collaboration suite
end-to-end encrypted and open-source




CryptDrive
LIVE DEMO
Files
+ New
Search...
Recent pads
Documents
Folder
Shared folder
Templates
Trash
Storage:
0.09 GB used out of 1 GB
Documents
Folder
Shared folder
Dessin
Kanban board
Markdown
Poll
Slides
Spreadsheet
Text document
New pad

Rich Text document

Saved

File | Insert | Tools | Outline | Share | Access | Chat | 1 | 0

Styles | Format | Arial | 16 | Words: 116

Contents

CryptPad Encryption Algorithms

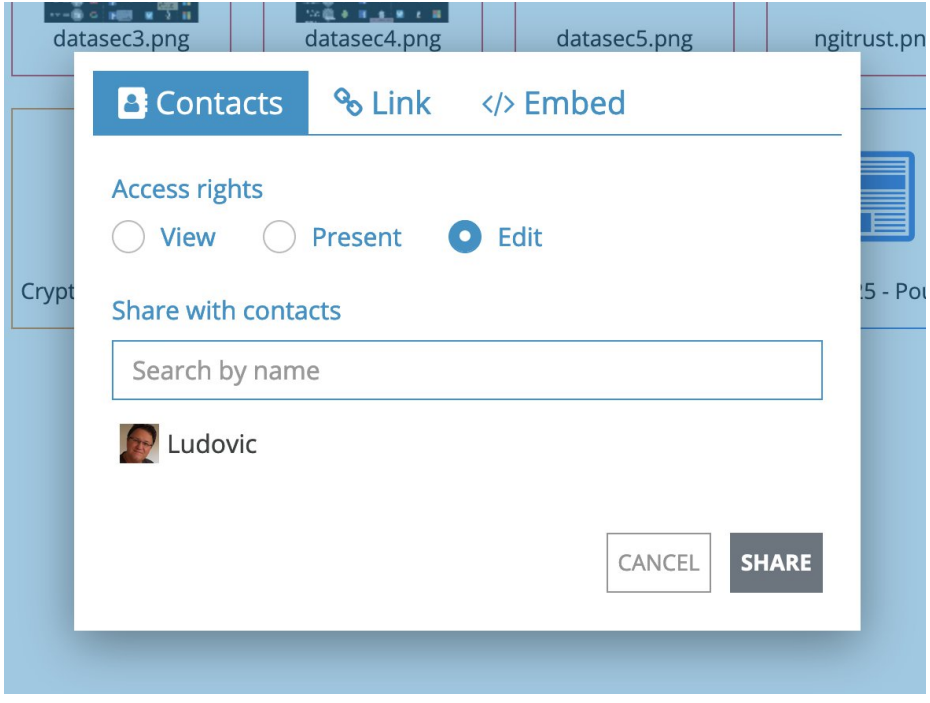
- Threat model is an "honest but curious" cloud server.
- 100% client side (in the browser using JavaScript).
- Key derivation from username and password using scrypt.
- Pads are encrypted using salsa20-poly1305 (tweetnacl.js) with randomly generated symmetric keys.
  - Technically what is encrypted is a sequence of patches, thus precluding known plaintext type attacks on changing cyphertext.
- Sharing a pad by URL facilitated by putting the pad key into the URL after the # mark (HTTP spec says this is never sent to the server).
- Changes to a pad are also signed using ed25519 and the signing public key is known to the server, thus allowing "read-only access".

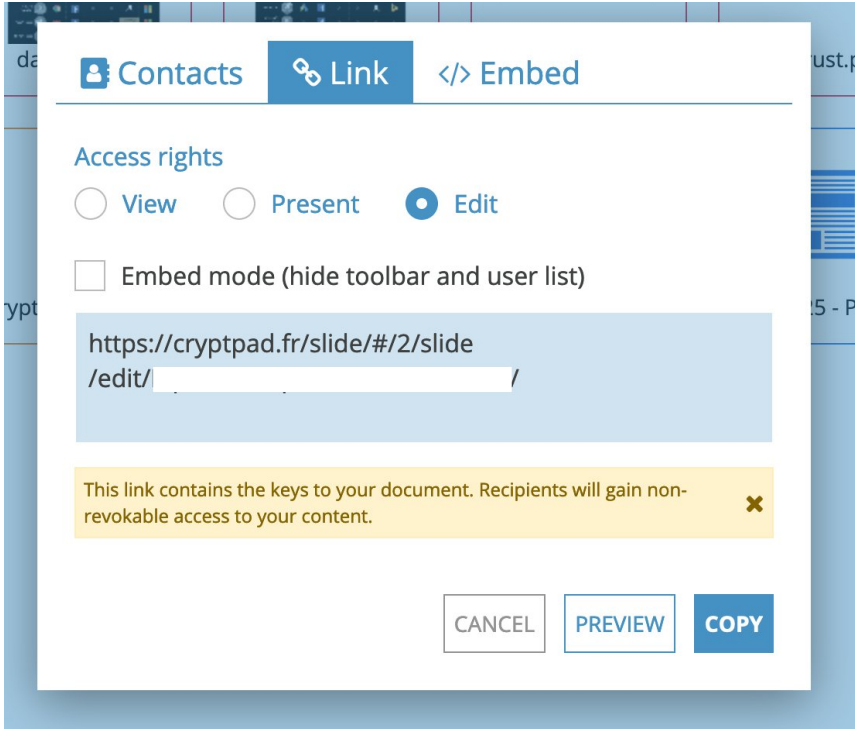
David
11/01/2021, 15:02:25
a document

billy
11/01/2021, 15:03:29
The link

David
11/01/2021, 15:03:37
ah ok thanks

Share


datasec3.png
datasec4.png
datasec5.png
Contacts
Link
Embed
Access rights
View
Present
Edit
Share with contacts
Search by name
Ludovic
CANCEL
SHARE


Contacts
Link
Embed
Access rights
View
Present
Edit
Embed mode (hide toolbar and user list)
https://cryptpad.fr/slide/#/2/slide
/edit/
This link contains the keys to your document. Recipients will gain non-revokable access to your content.
CANCEL
PREVIEW
COPY

Markdown Guide: Extensions

Saved

File Theme Insert Tools Share Access Preview Chat 1 0

```
## Mermaid

See the [Mermaid Documentation](https://mermaid-js.github.io/mermaid/#/)
for more examples and in depth demonstrations.

### Flowchart

```mermaid
graph TD

A --- B & C -.-> D ==> E
```

Pie charts

```mermaid
pie title pewpewpew

"dogs": 5
"cats": 3
```

GANTT

```mermaid
gantt
    title A Gantt Diagram
    dateFormat  YYYY-MM-DD

section Section
    A task           :a1, 2014-01-01, 30d
    Another task     :after a1  , 20d

section Another
    Task in sec      :2014-01-12  , 12d
    another task      : 24d
```

Sequence diagram

```mermaid
sequenceDiagram
    participant John
    participant Alice
    Alice->>John: Hello John, how are you?
    John-->>Alice: Great!
```

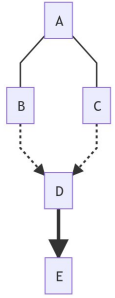
Class diagram

```mermaid
```

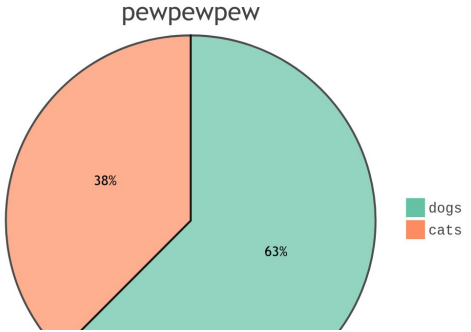
Mermaid

See the Mermaid Documentation for more examples and in depth demonstrations.

Flowchart



Pie charts



https://docs.cryptpad.fr/en/user_guide/apps/code.html#markdown
```

Kanban

Saved

File | Share | Access | Chat | 1 | 0

Filter by tag: a tag | branding | feature

BUGS

- there are some
- they can be reported
- On Github
- or via support tickets
- or on Matrix chat

Ideas

- Make static pages more readable
- Federation
- Calendar Support
  Will come with a redesign of the Polls app and Forms.
  feature
- Redesign contacts app
  - multi-user chats
  - mentions across the platform
- test
  branding | feature

To Do

- Slides theme
- Documentation
  - for users
  - for admins
  - for instance install
- Password policy
- Improve accessibility
  aiming for AA across the platform
- Visual identity
  - [ ] de-clutter
  - [ ] lighten
  - [ ] simplify

  branding

In progress

- Share dialog
  Lorem Ipsum with **markdown** support.
  - list
  - of
  - things

  a tag
- New toolbar UI
  Make functionality easier to discover. Lighten the top-heavy design.
- copywriting
- writing some JavaScript

Done

- Color By Author
- Rich Text Comme
- Usage bar
- Burn After Readir
  Sharing a pad that sel is opened by the recip
- Migrate Todo list board
- Profile page
- tooltip cleanup

CryptPad Sales and Revenues 2016-2020

Saved

File | Share | Access | Chat | 1 | 0

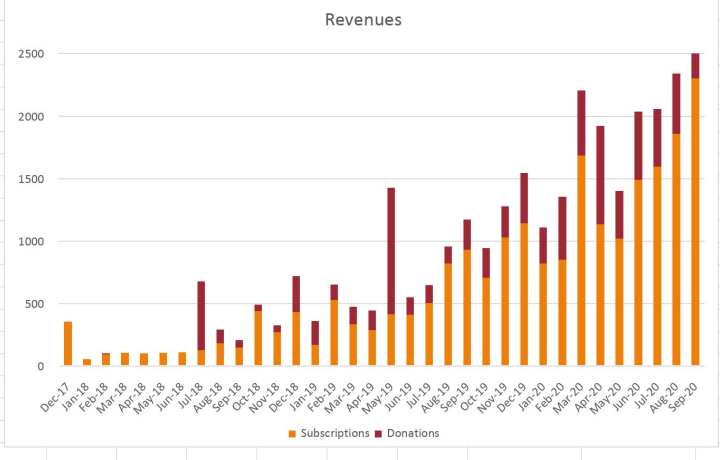
ONLYOFFICE

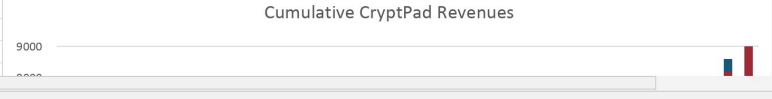
File | Home | Insert | Layout | Formula | Data | Pivot Table | Collaboration | View

Normal | Neutral | Bad | Good | Input | Output | Calculation

G108 =SUM('CryptPad Revenues Summary'!F27:F38)

Period	Refunds (Quaderno Credit Notes)	Stripe Fees	Quaderno Fees	Total	Total Revenue	Last 12 month
Dec-17		12.22	218	125	355	
Jan-18		3.12	27	25	55	
Feb-18		4.32	27	68	100	
Mar-18		5.85	27	72	105	
Apr-18		4.98	27	474	506	
May-18		5.92	27	72	105	
Jun-18		5.92	27	77	110	
Jul-18		19.97	27	629	676	
Aug-18		17.2	27	246	290	
Sep-18		13.36	27	164	205	
Oct-18		23.38	27	441	492	
Nov-18		14.96	27	283	325	3324
Dec-18		44.14	27	649	720	3689
Jan-19	49	20.11	27	263	311	3944
Feb-19		30.85	27	593	651	4495
Mar-19		27.77	27	419	474	4865
Apr-19		22.4	27	394	444	4802
May-19	6	62.5	27	1330	1420	6117
Jun-19		31	27	493	551	6558
Jul-19	25	32.91	27	564	624	6506
Aug-19	27	48.58	27	853	929	7144
Sep-19	6	61.18	27	1077	1165	8105
Oct-19		47.55	27	868	942	8555
Nov-19	110	60.42	27	1080	1168	9398
Dec-19		81.62	27	1436	1545	10224
Jan-20		62.82	27	1020	1110	11023
Feb-20		82.19	27	1245	1354	11726
Mar-20		105.2	27	2076	2209	13461
Apr-20		115.61	27	1782	1925	14942
May-20		80.1	27	1296	1403	14925
Jun-20		114.68	27	1895	2037	16411
Jul-20		106.63	27	1927	2061	17848





Fill: No Fill

Borders Style | Color

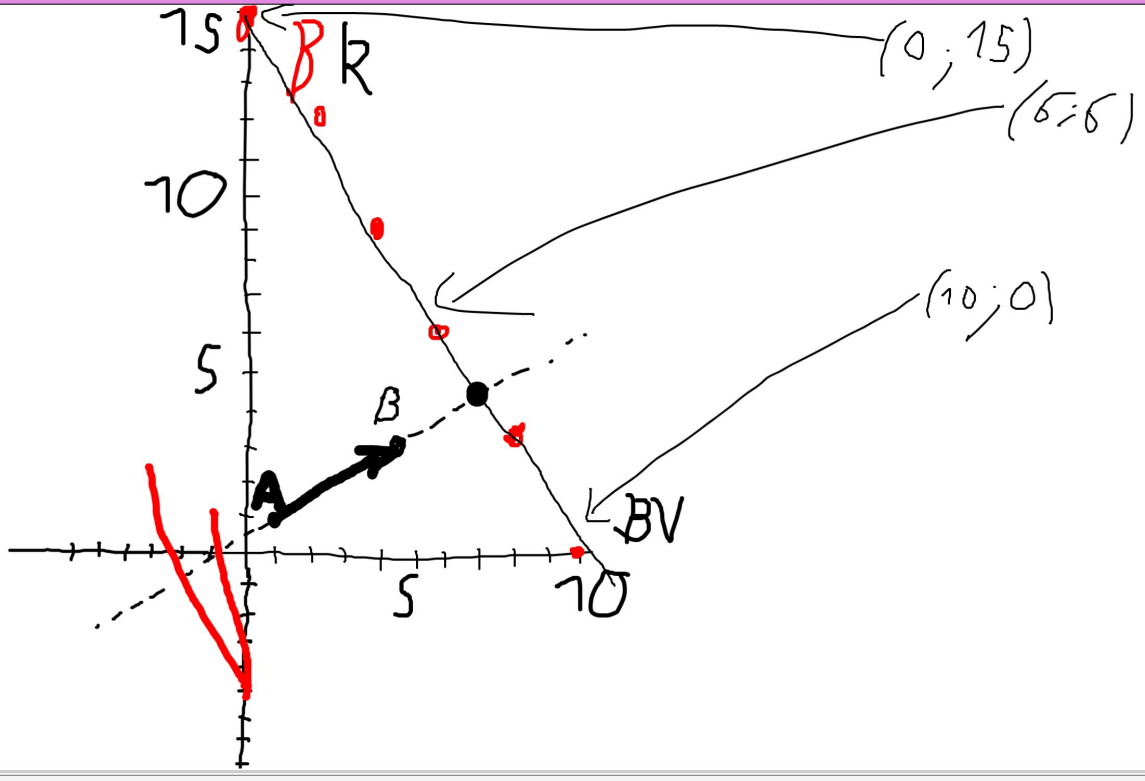
Select borders you want to change applying style chosen above

Text Orientation: Angle 0°

Text Control: Wrap text | Shrink to fit

CryptPad Revenues Summary | Manual Sales | Multi-Year Analysis | Subs Analysis

Zoom 100%



CLEAR

Width: 20px

Opacity: 100%

CryptPad: recent work

- InterOffice (better Import/Exports using WebAssembly) + Presentation and Documents based on OnlyOffice (only for subcribers or on self-hosting) & OnlyOffice 6.4.2
- Bug Bounty European Community (security fixes)
- Instances Directory (https ://cryptpad.org/instances/) with security checks
- CryptPad 5.0 : new look

cryptpad.fr: quite a ride !

COVID Wave 1

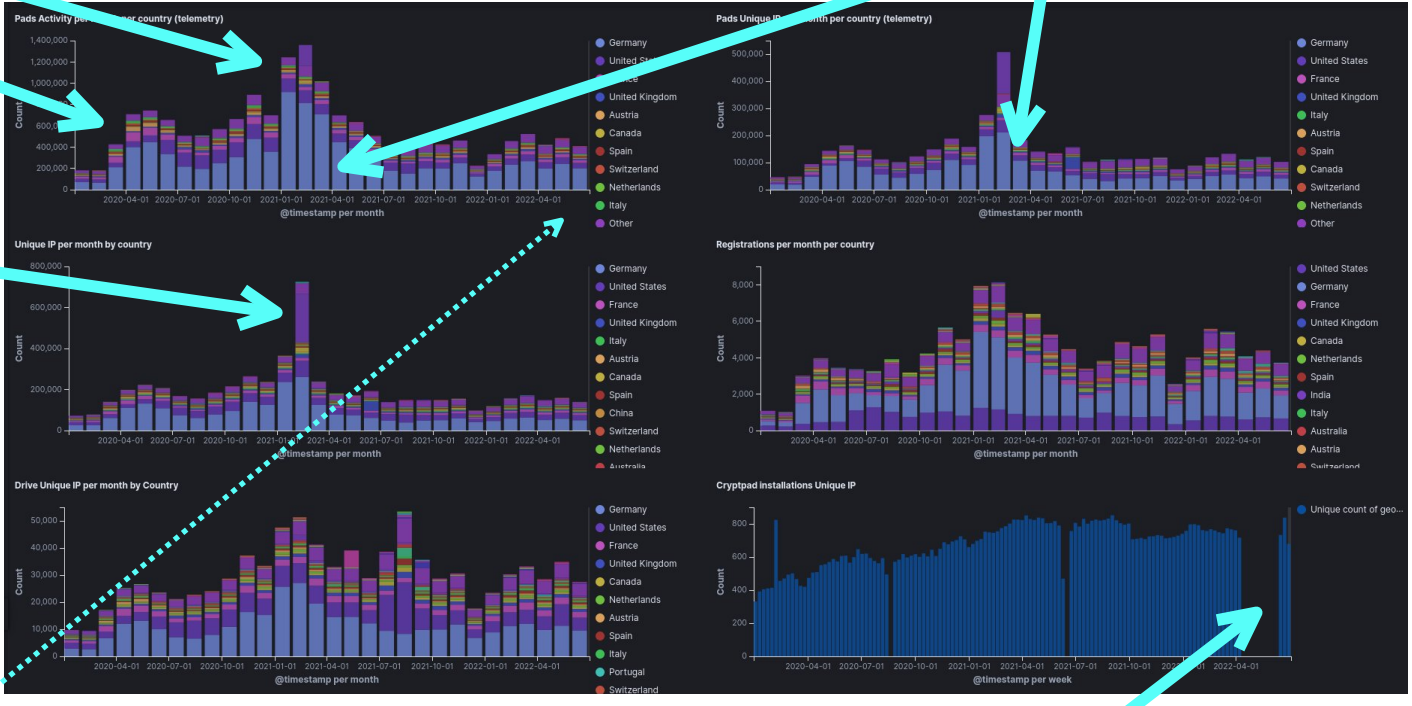
COVID lockdown of schools

High usage in Germany

Greta Thunberg shares a pad in India

450000+ pads / month

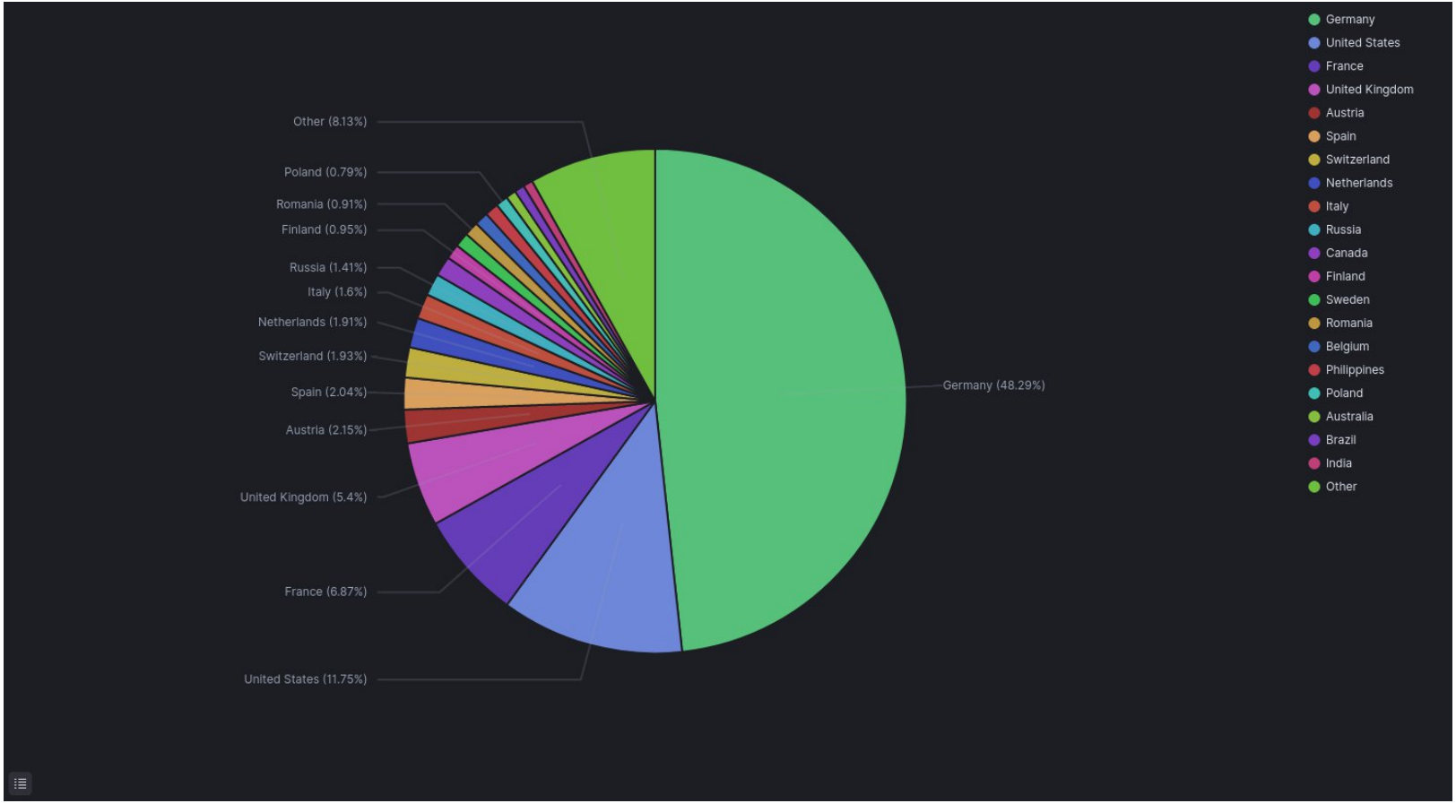
100000+ users / month



30000 drive users / month

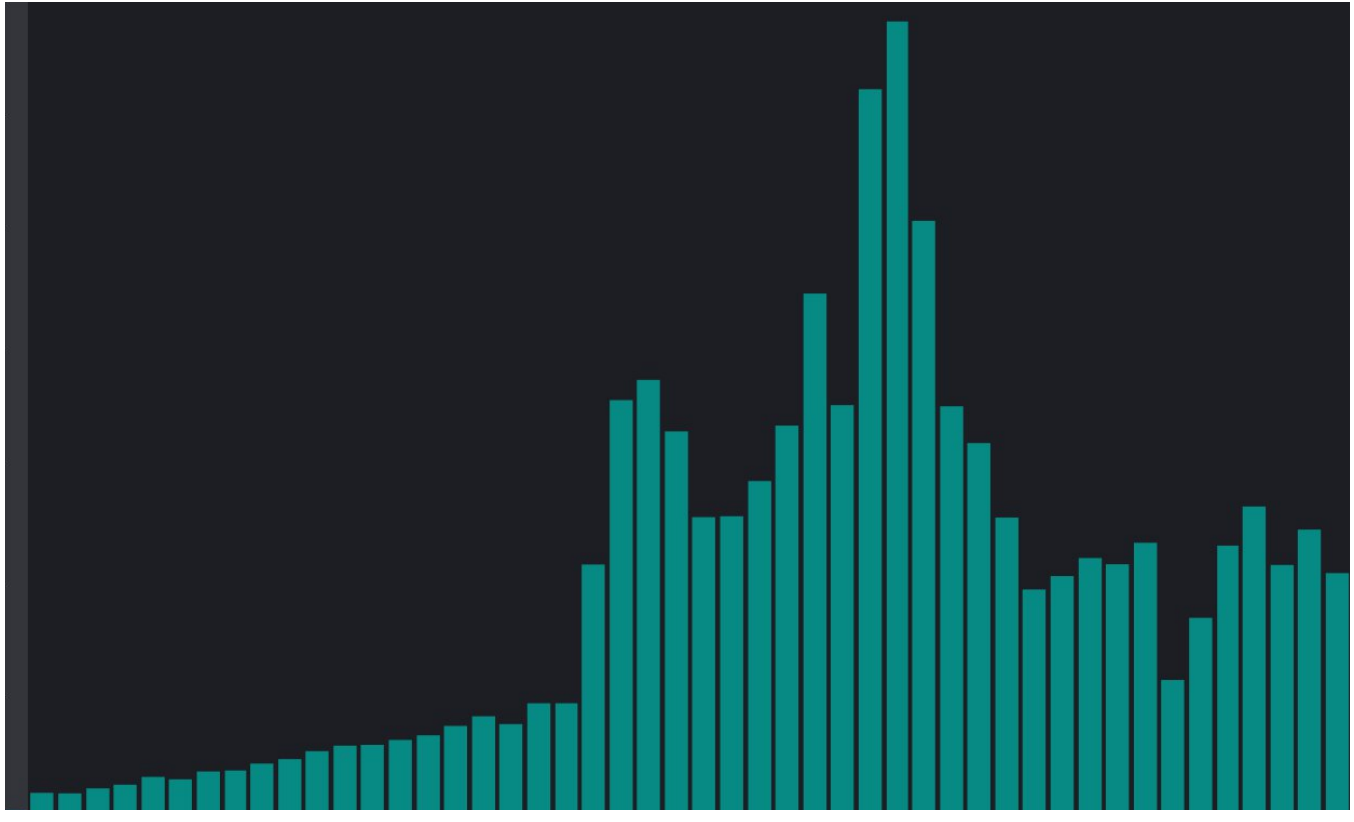
750 installations

cryptpad.fr



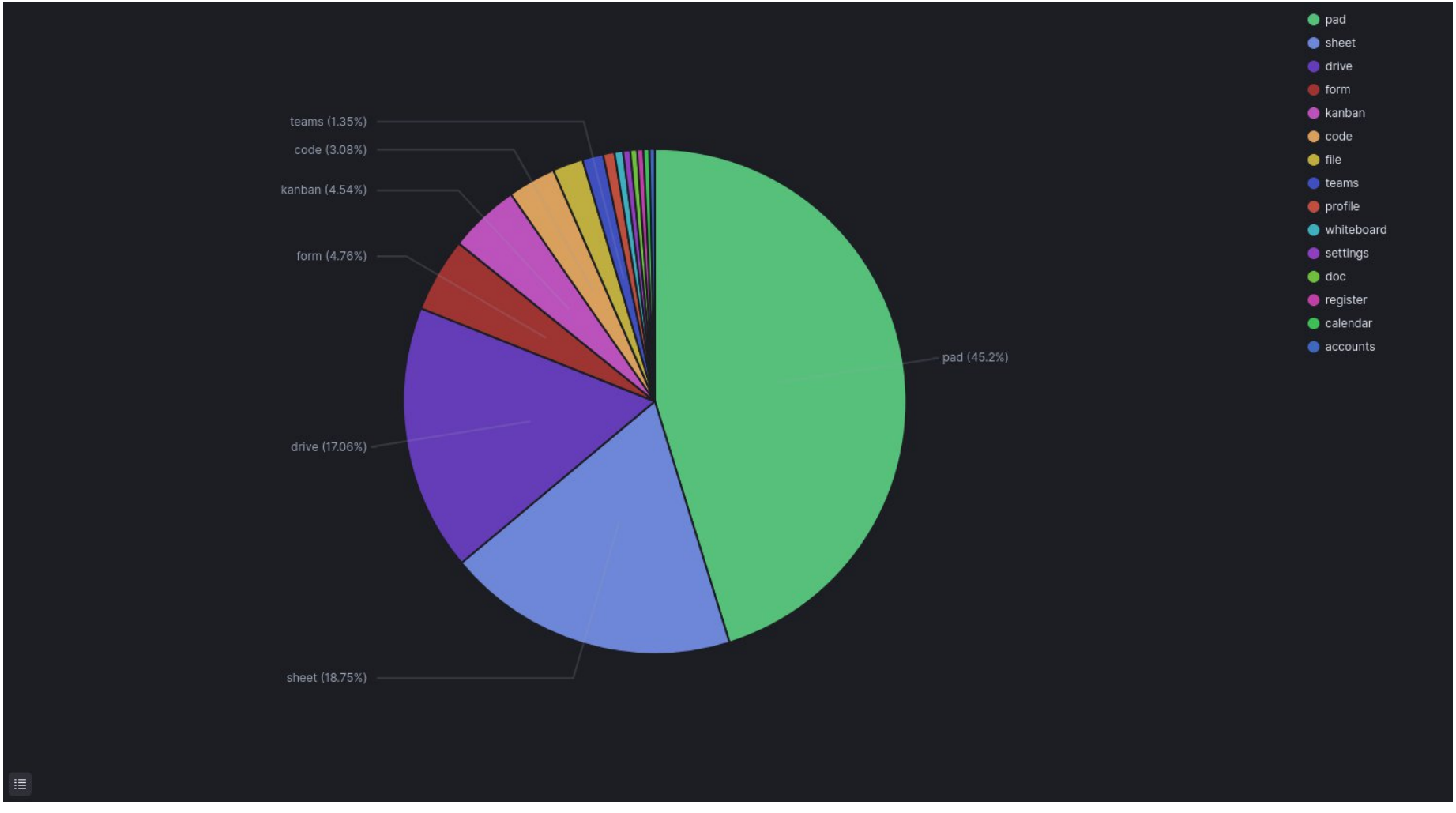
50% of our usage comes from Germany

cryptpad.fr



spike at 1,3M pads, currently 400-500k / month

cryptpad.fr: Pas types : HTML + Sheets



CryptPad : can it help reduce energy usage ?

- cryptpad.fr : 1300000 pads = 6500 * 200 pads per month = 6500 very active users -> 1 server 8 cores (70Watt) + machine et disks: 100W

-> 1 server for 6500 utilisateurs

- Google Apps (2) Mail+Collab for 18000 users: 1-5KWh/user, 60 serveurs -> considering 33% collaboration vs email

-> 1 server for 1100 users

6x less energy

- Source :
  - (1) https://www.researchgate.net/figure/CPU-Power-consumption-relationship-with-number-of-active-cores_fig2_254017286
  - (2) https://static.googleusercontent.com/media/www.google.com/fr//green/pdf/google-apps.pdf

Financing

- Subscriptions 10% https://cryptpad.fr
- Donations 5% https://opencollective.com/cryptpad/
- Entreprise offers -> coming
- Research projects 85%
  - NLNet
  - NGI DAPSI

FUNDED BY NGI

This project has received funding from the European Union's H2020 research and innovation programme under Grant Agreement no 871498

CryptPad: roadmap

- 2FA / SSO Integration
- Documentation Cryptography / Security
- Open with CryptPad (French research project)
- OnlyOffice Improvements (incl. sécurity)
- Longer term : key backup & recovery, scalability of storage

How to help !

- Use it, share it, make it known !
- Translate or help document (https://weblate.cryptpad.fr)
- Deployment / Installation / Maintain packages
- Security audits (and fixes)
- Code in JS -> Contribute / We hire https://cryptpad.fr/jobs/ jobs@xwki.com
- Present or talk about CryptPad (we can provide slides)

Hiring : See https://cryptpad.fr/jobs

- Instance Admin (almost hired)
- Interns (2 this summer)
- Javascript developers
- OnlyOffice developers
- Full Stack (JS, nodeJS, scalability)
- WebAssembly developers

Are you encrypting your data ?