Open Research Webinars

Open Collaboration in European Research Projects

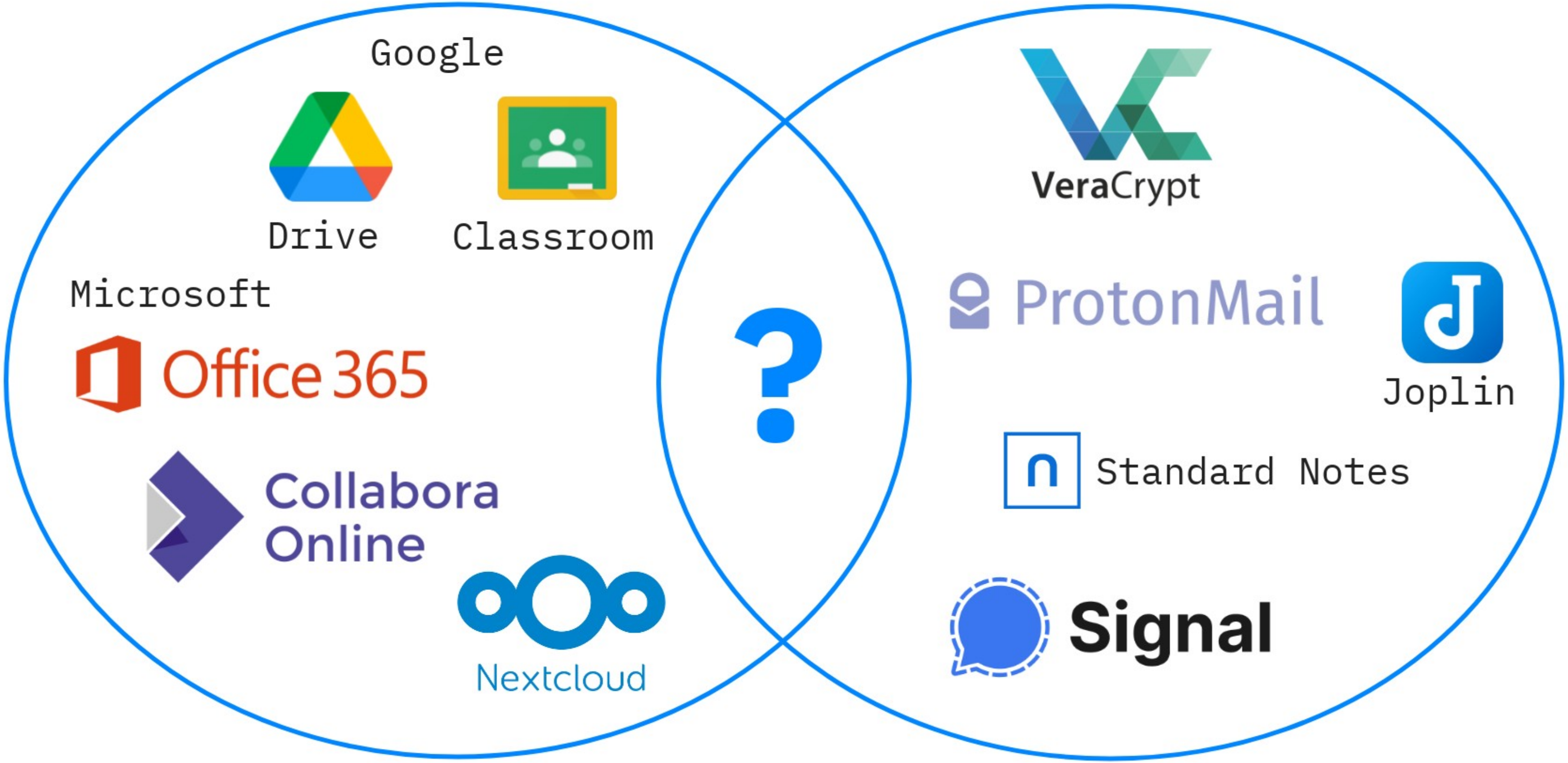
CryptPad; end-to-end encrypted collaborative office suite

David Benqué
Project Lead

Presented by: RESEARCH @ ECLIPSE FOUNDATION & OW2

Collaboration

Privacy



Google

Drive

Classroom

Microsoft

Office 365

Collabora Online

Nextcloud

?

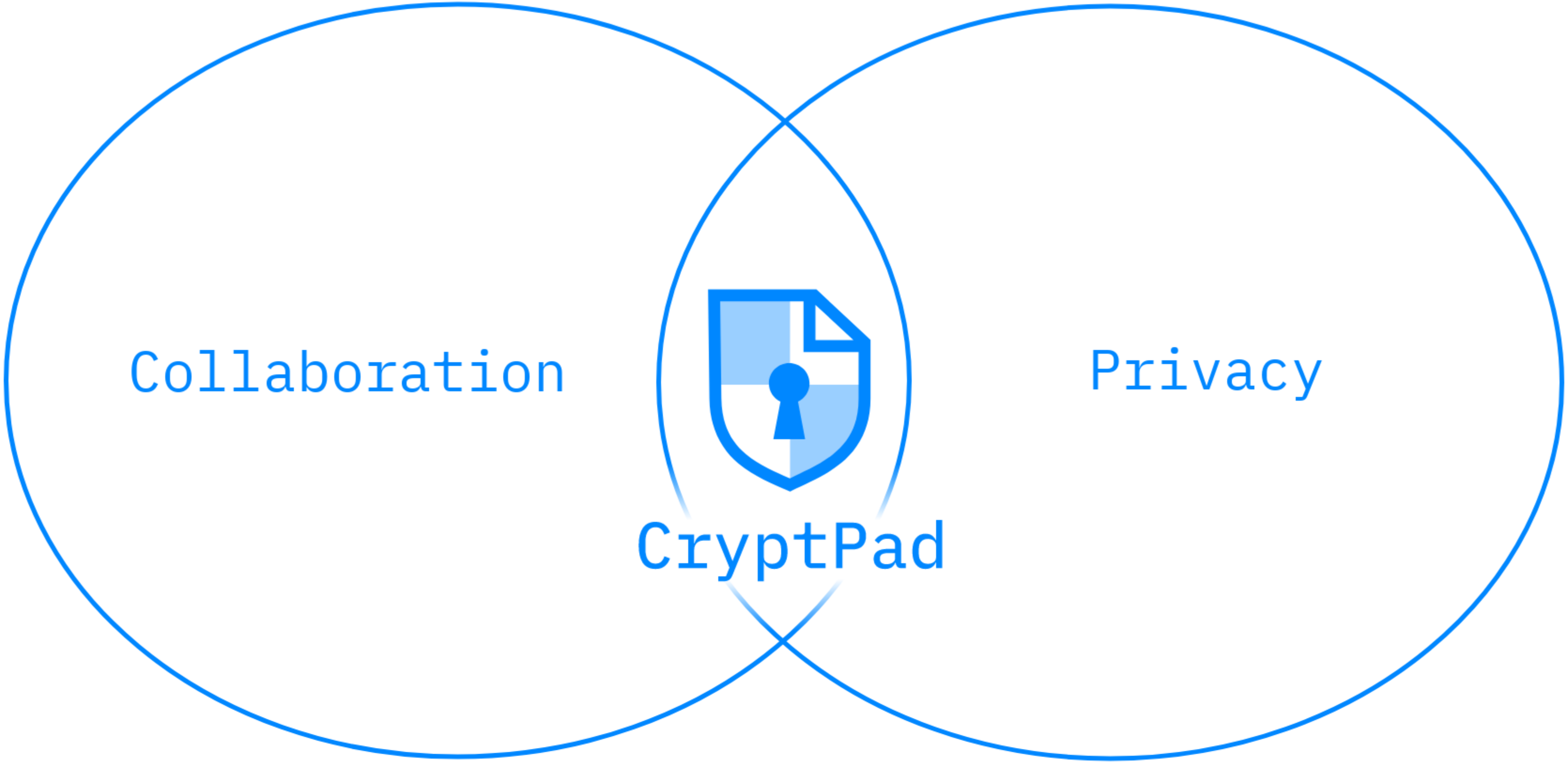
VeraCrypt

ProtonMail

Joplin

Standard Notes

Signal

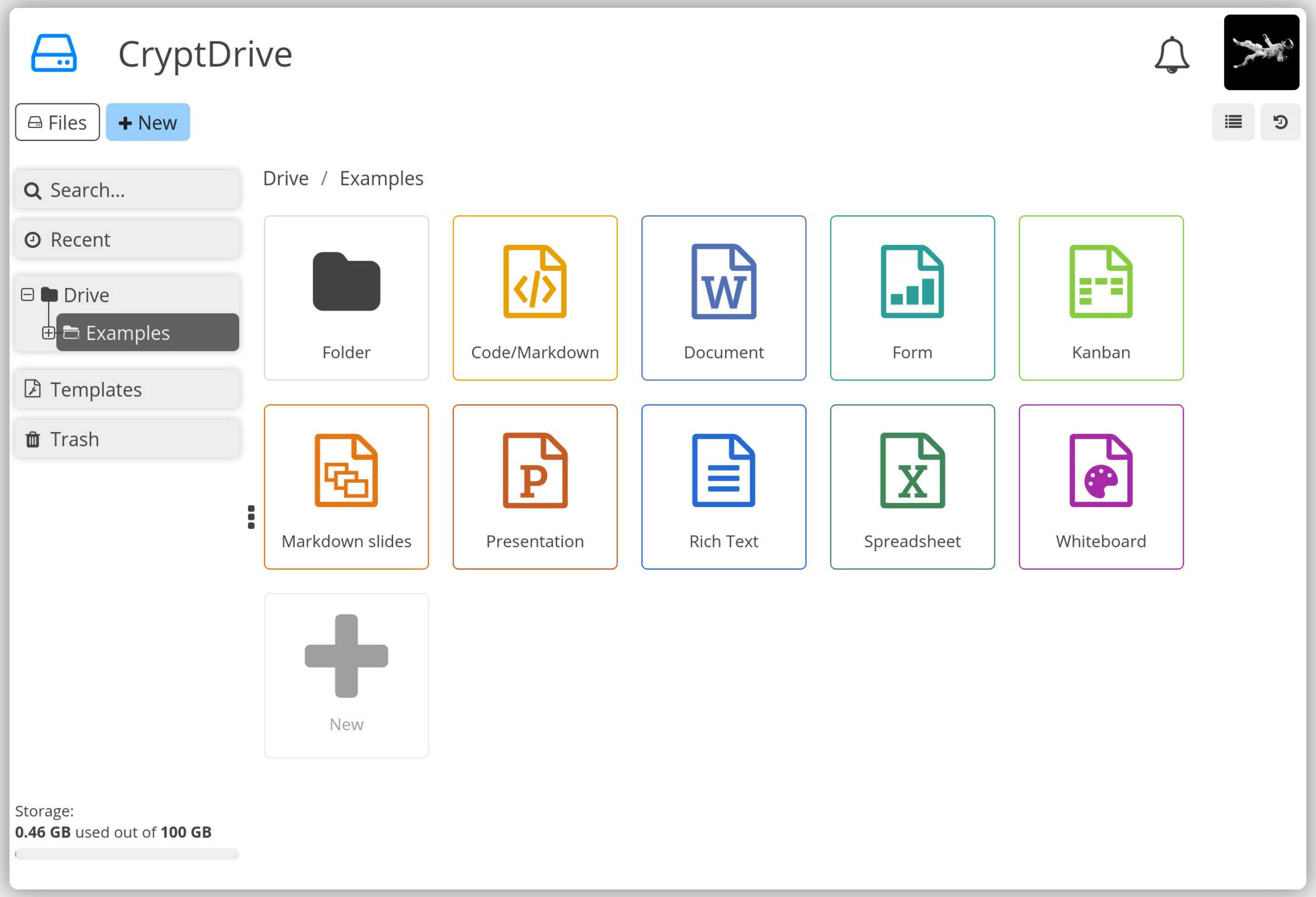


Collaboration

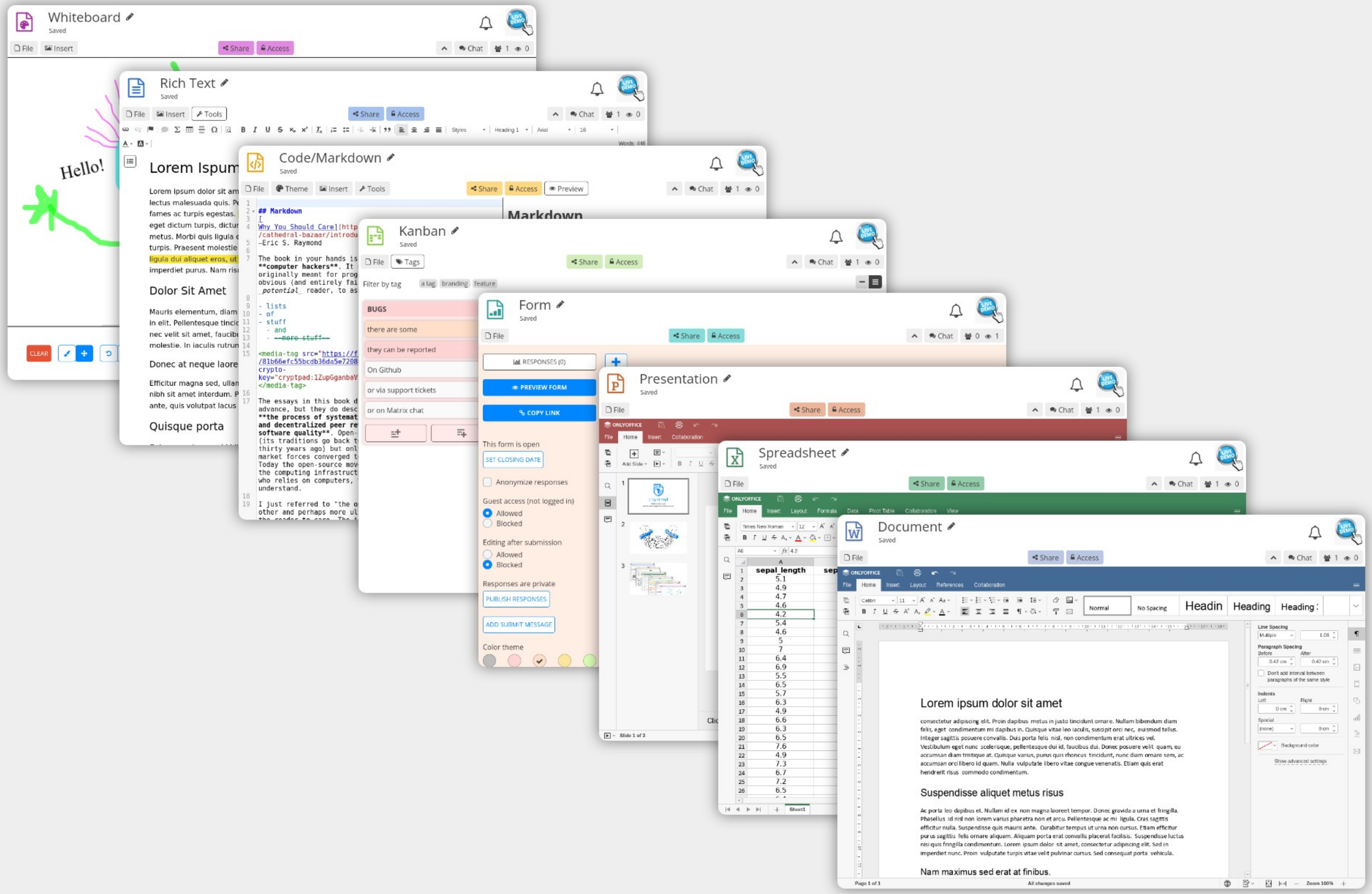
CryptPad

Privacy

Yes, you can have both



Storage:
0.46 GB used out of **100 GB**



	A
1	sepal_length
2	5.1
3	4.9
4	4.7
5	4.6
6	4.2
7	5.4
8	4.6
9	5
10	7
11	6.4
12	6.9
13	5.5
14	6.5
15	5.7
16	6.3
17	4.9
18	6.6
19	6.3
20	6.5
21	7.6
22	4.9
23	7.3
24	6.7
25	7.2
26	6.5

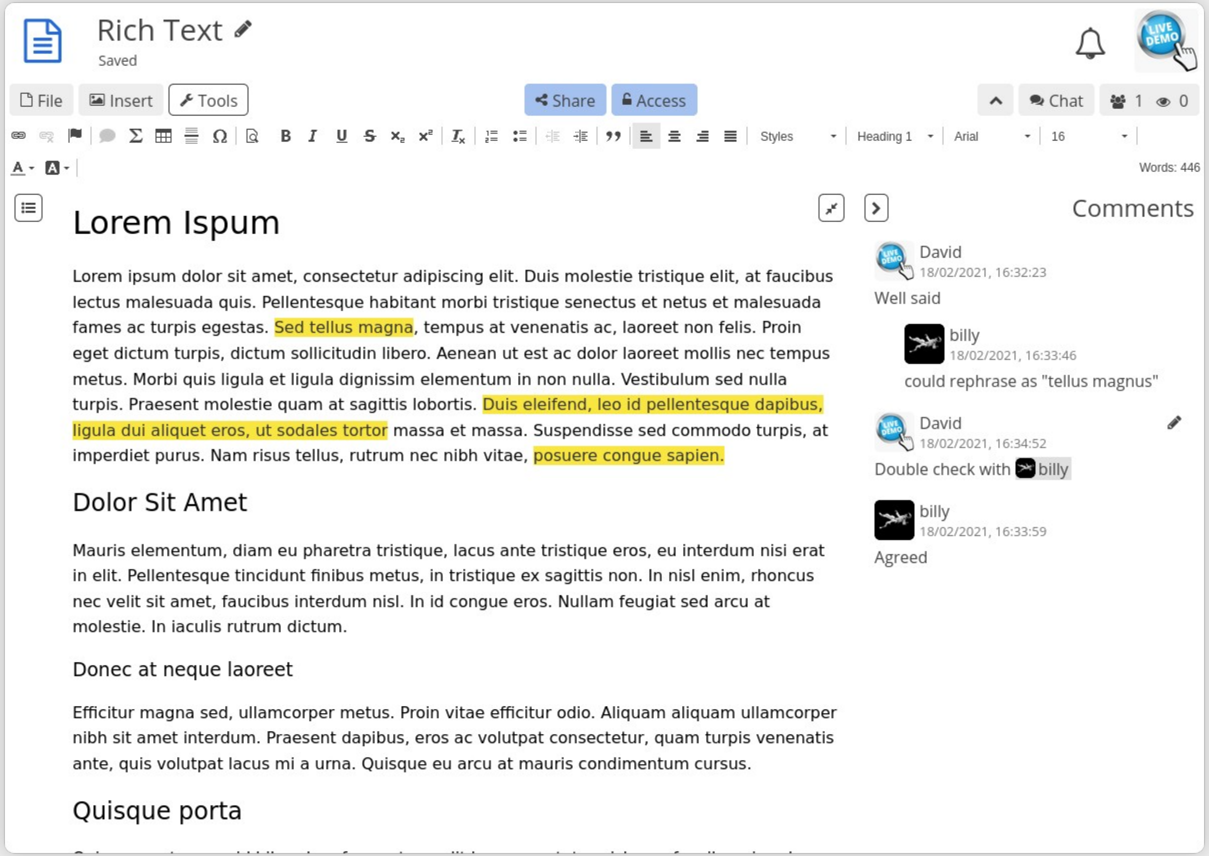
Lorem ipsum dolor sit amet

consectetur adipiscing elit. Proin dapibus metus in justo tincidunt ornare. Nullam bibendum diam felis, eget condimentum mi dapibus in. Quisque vitae leo iaculis, suscipit orci nec, euismod tellus. Integer sagittis posuere convallis. Duis porta felis nisl, non condimentum erat ultrices vel. Vestibulum eget nunc scelerisque, pellentesque dui id, faucibus dui. Donec posuere velit quam, eu accumsan diam tristique at. Quisque varius, purus quis rhoncus tincidunt, nunc diam ornare sem, ac accumsan orci libero id quam. Nulla vulputate libero vitae congue venenatis. Etiam quis erat hendrerit risus commodo condimentum.

Suspendisse aliquet metus risus

Ac porta leo dapibus et. Nullam id ex non magna laoreet tempor. Donec gravida a urna et fringilla. Phasellus id nisl non lorem varius pharetra non et arcu. Pellentesque ac mi ligula. Cras sagittis efficitur nulla. Suspendisse quis mauris ante. Curabitur tempus ut urna non cursus. Etiam efficitur purus sagittis felis ornare aliquam. Aliquam porta erat convallis placerat facilisis. Suspendisse luctus nisi quis fringilla condimentum. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed in imperdiet nunc. Proin vulputate turpis vitae velit pulvinar cursus. Sed consequat porta vehicula.

Nam maximus sed erat at finibus.



Lorem Ispum

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Duis molestie tristique elit, at faucibus lectus malesuada quis. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Sed tellus magna, tempus at venenatis ac, laoreet non felis. Proin eget dictum turpis, dictum sollicitudin libero. Aenean ut est ac dolor laoreet mollis nec tempus metus. Morbi quis ligula et ligula dignissim elementum in non nulla. Vestibulum sed nulla turpis. Praesent molestie quam at sagittis lobortis. Duis eleifend, leo id pellentesque dapibus, ligula dui aliquet eros, ut sodales tortor massa et massa. Suspendisse sed commodo turpis, at imperdiet purus. Nam risus tellus, rutrum nec nibh vitae, posuere congue sapien.

Dolor Sit Amet

Mauris elementum, diam eu pharetra tristique, lacus ante tristique eros, eu interdum nisi erat in elit. Pellentesque tincidunt finibus metus, in tristique ex sagittis non. In nisl enim, rhoncus nec velit sit amet, faucibus interdum nisl. In id congue eros. Nullam feugiat sed arcu at molestie. In iaculis rutrum dictum.

Donec at neque laoreet

Efficitur magna sed, ullamcorper metus. Proin vitae efficitur odio. Aliquam aliquam ullamcorper nibh sit amet interdum. Praesent dapibus, eros ac volutpat consectetur, quam turpis venenatis ante, quis volutpat lacus mi a urna. Quisque eu arcu at mauris condimentum cursus.

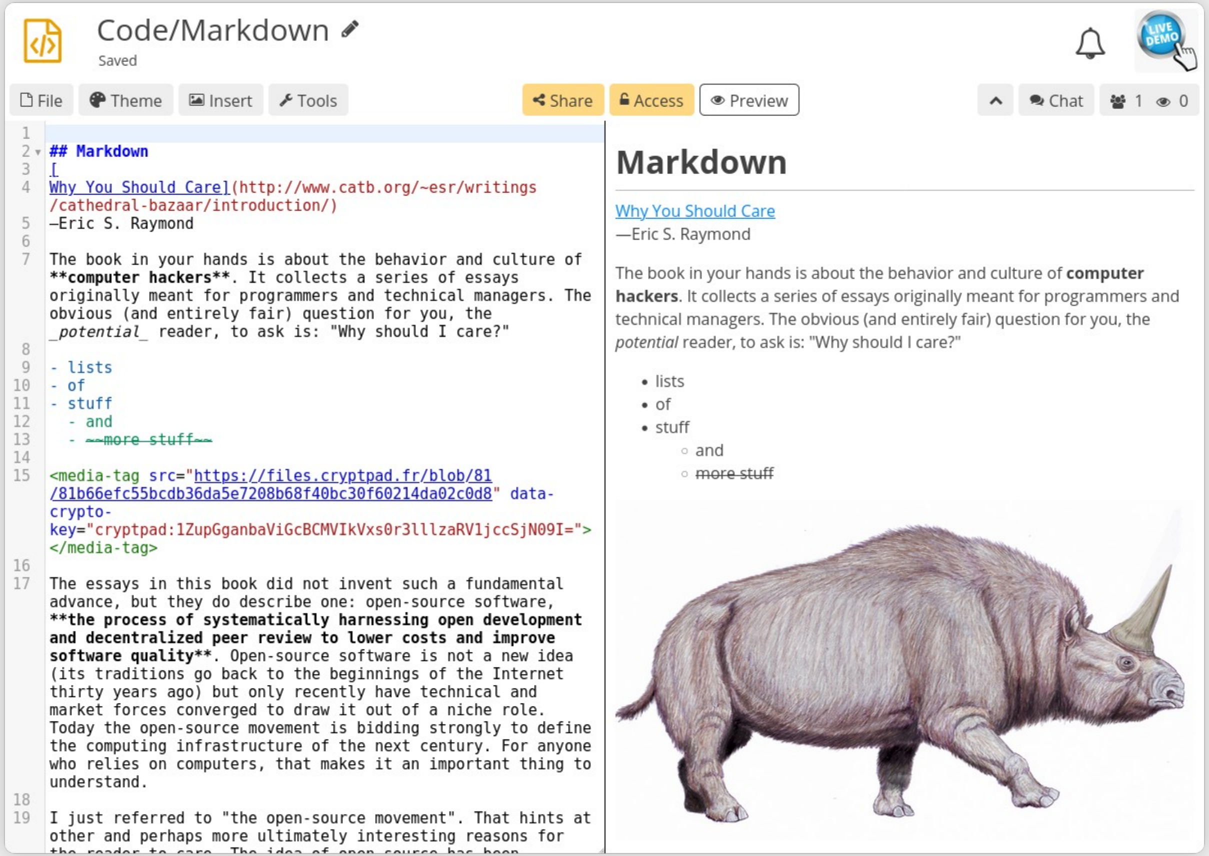
Quisque porta

David
18/02/2021, 16:32:23
Well said

billy
18/02/2021, 16:33:46
could rephrase as "tellus magnus"

David
18/02/2021, 16:34:52
Double check with billy

billy
18/02/2021, 16:33:59
Agreed



```
## Markdown
[
Why You Should Care](http://www.catb.org/~esr/writings/cathedral-bazaar/introduction/)
—Eric S. Raymond

The book in your hands is about the behavior and culture of **computer hackers**. It collects a series of essays originally meant for programmers and technical managers. The obvious (and entirely fair) question for you, the _potential_ reader, to ask is: "Why should I care?"

- lists
- of
- stuff
  - and
  - ~~more stuff~~

<media-tag src="https://files.cryptpad.fr/blob/81/81b66efc55bcdb36da5e7208b68f40bc30f60214da02c0d8" data-crypto-key="cryptpad:1ZupGganbaViGcBCMVIkVxs0r3lllzaRV1jccSjN09I="></media-tag>

The essays in this book did not invent such a fundamental advance, but they do describe one: open-source software, **the process of systematically harnessing open development and decentralized peer review to lower costs and improve software quality**. Open-source software is not a new idea (its traditions go back to the beginnings of the Internet thirty years ago) but only recently have technical and market forces converged to draw it out of a niche role. Today the open-source movement is bidding strongly to define the computing infrastructure of the next century. For anyone who relies on computers, that makes it an important thing to understand.

I just referred to "the open-source movement". That hints at other and perhaps more ultimately interesting reasons for
the reader to care. The idea of open source has been
```

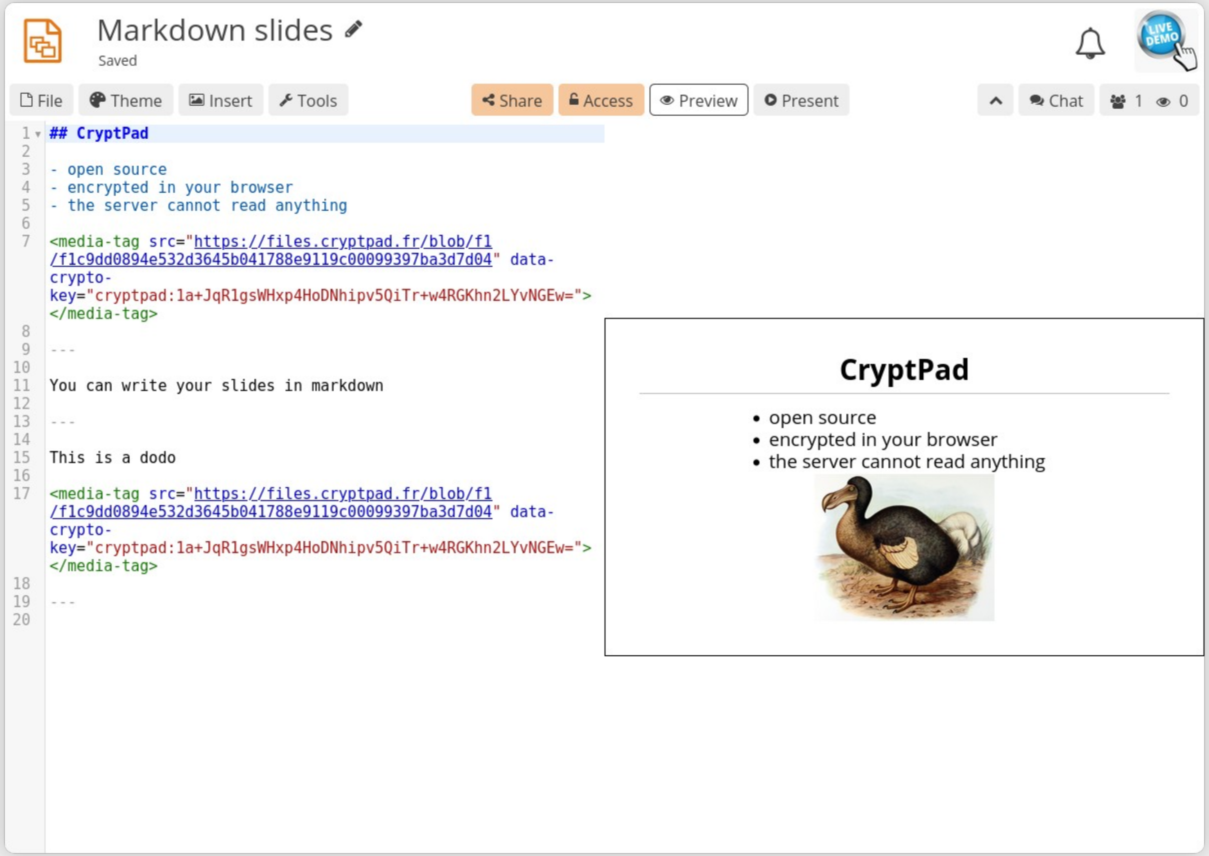
Markdown

Why You Should Care

—Eric S. Raymond

The book in your hands is about the behavior and culture of **computer hackers**. It collects a series of essays originally meant for programmers and technical managers. The obvious (and entirely fair) question for you, the *potential* reader, to ask is: "Why should I care?"

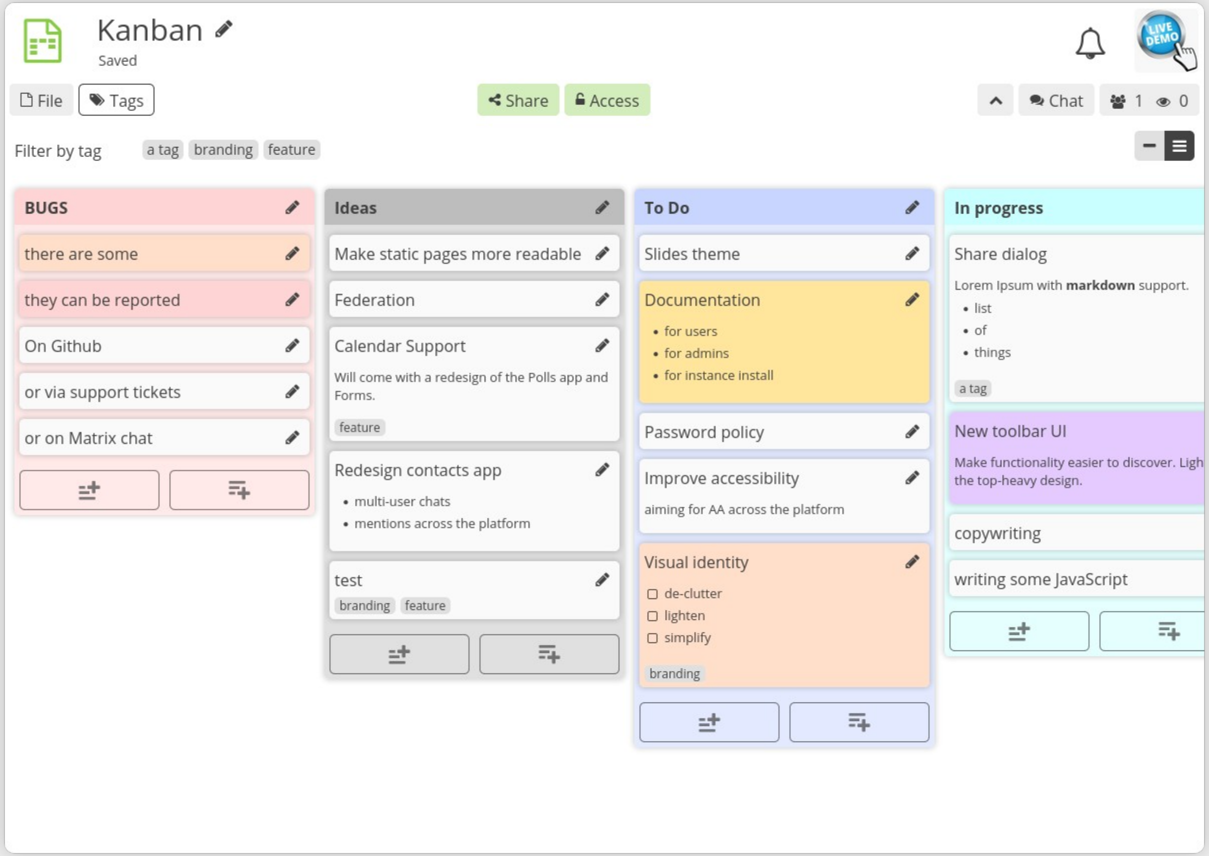
- lists
- of
- stuff
  - and
  - ~~more stuff~~



```
## CryptPad

- open source
- encrypted in your browser
- the server cannot read anything

<media-tag src="https://files.cryptpad.fr/blob/f1/f1c9dd0894e532d3645b041788e9119c00099397ba3d7d04" data-crypto-key="cryptpad:1a+JqR1gsWHxp4HoDNhipv5QiTr+w4RGKhn2LYvNGEw="></media-tag>

---

You can write your slides in markdown

---

This is a dodo

<media-tag src="https://files.cryptpad.fr/blob/f1/f1c9dd0894e532d3645b041788e9119c00099397ba3d7d04" data-crypto-key="cryptpad:1a+JqR1gsWHxp4HoDNhipv5QiTr+w4RGKhn2LYvNGEw="></media-tag>

---

```

CryptPad

- open source
- encrypted in your browser
- the server cannot read anything



Kanban

Saved

File · Tags · 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

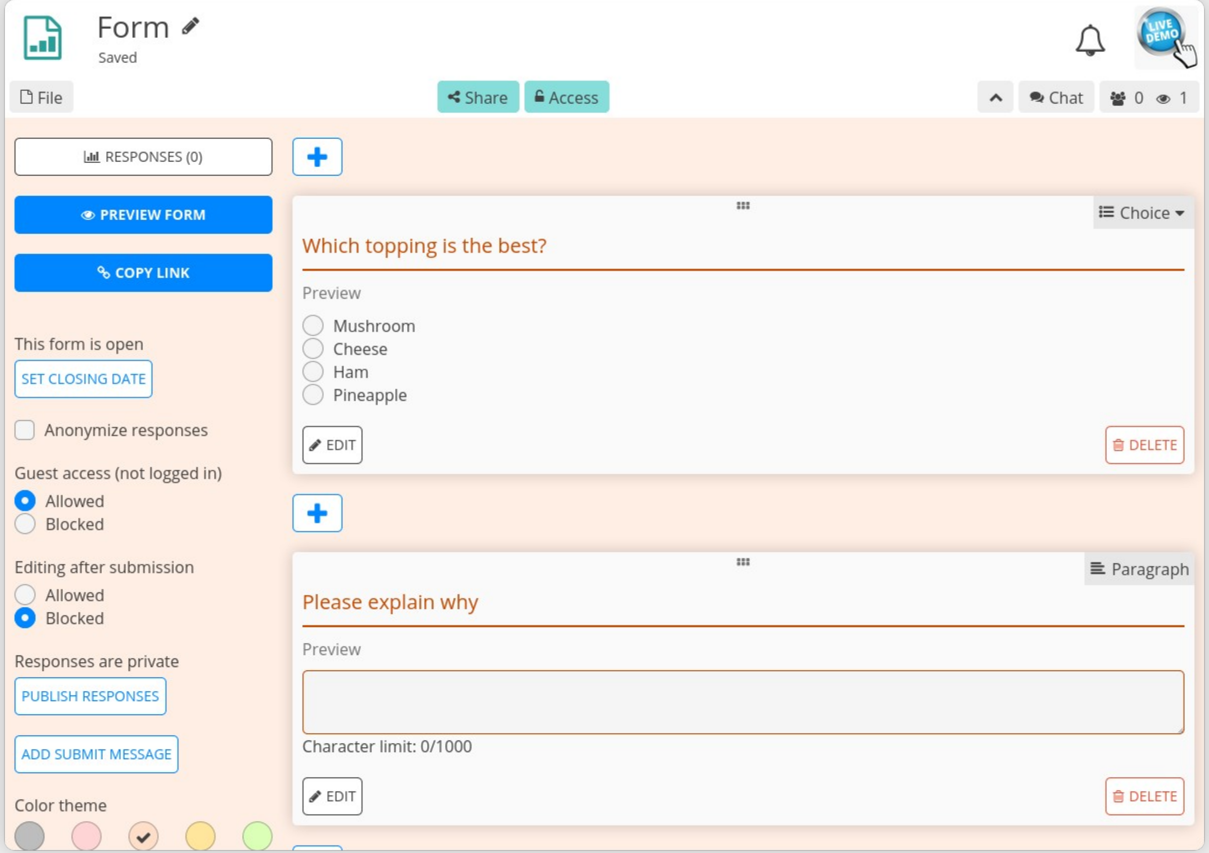
- Slides theme
- Documentation
  - for users
  - for admins
  - for instance install
- Password policy
- Improve accessibility
  aiming for AA across the platform
- Visual identity
  - □ de-clutter
  - □ lighten
  - □ simplify

  branding

In progress

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

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



Form

Saved

RESPONSES (0)

PREVIEW FORM

COPY LINK

This form is open

SET CLOSING DATE

□ Anonymize responses

Guest access (not logged in)

● Allowed
○ Blocked

Editing after submission

○ Allowed
● Blocked

Responses are private

PUBLISH RESPONSES

ADD SUBMIT MESSAGE

Color theme

Choice

Which topping is the best?

Preview

○ Mushroom
○ Cheese
○ Ham
○ Pineapple

EDIT

DELETE

Paragraph

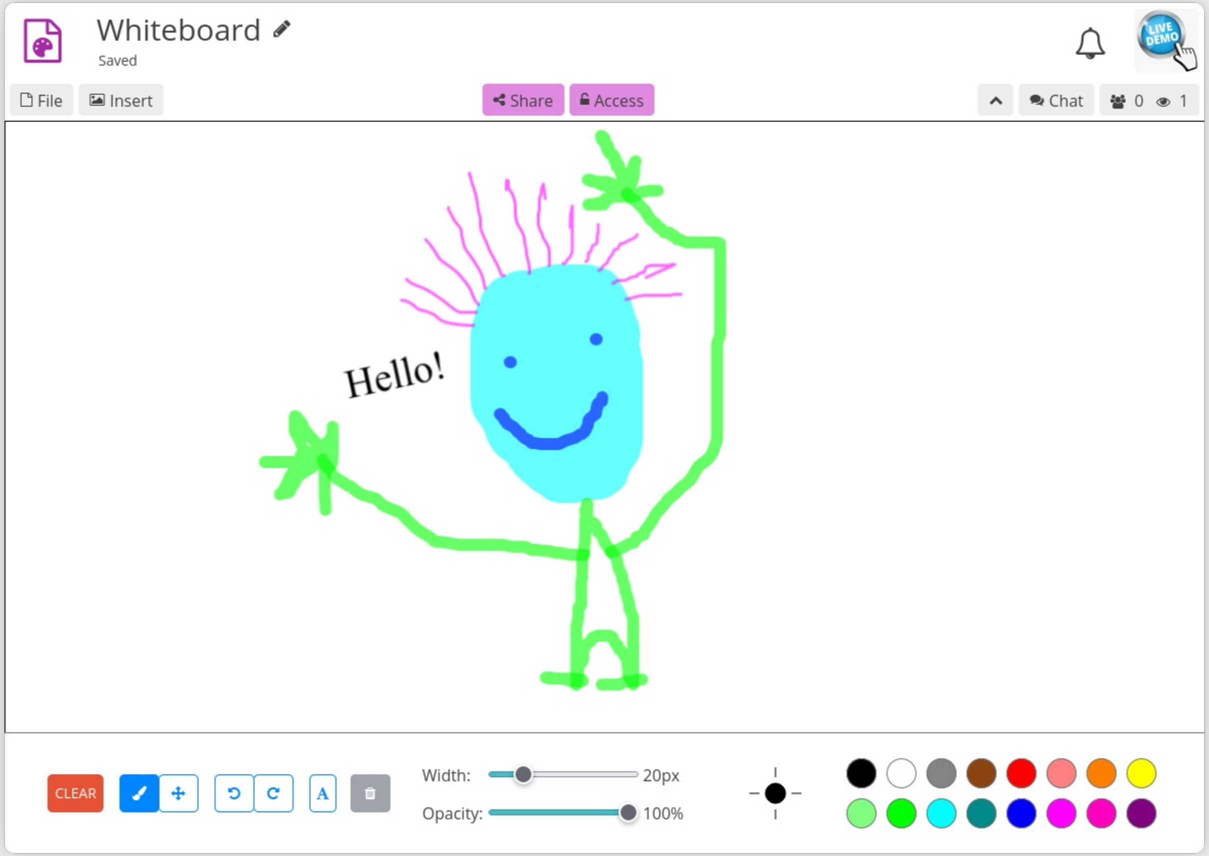
Please explain why

Preview

Character limit: 0/1000

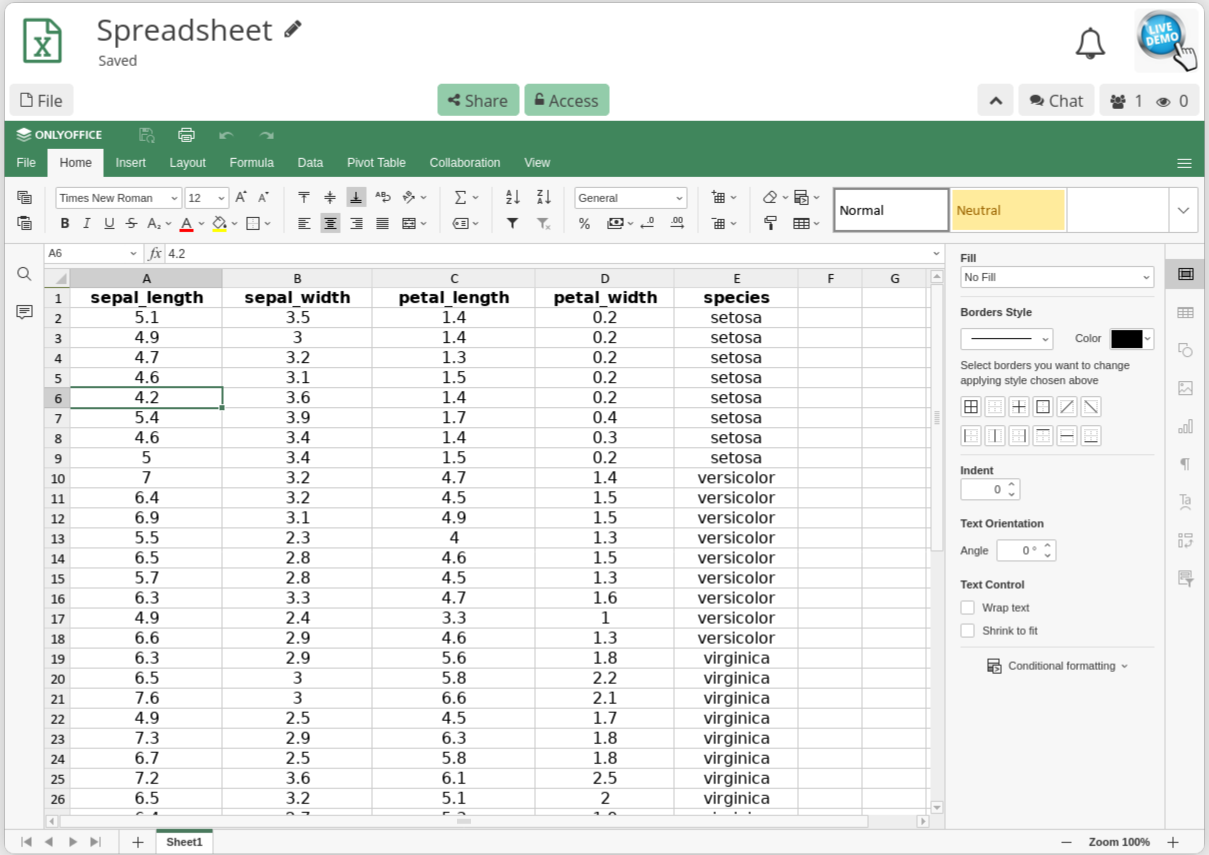
EDIT

DELETE



Width: 20px

Opacity: 100%



Font: Times New Roman, 12

Number format: General

A6 *fx* 4.2

	A	B	C	D	E	F	G
1	sepal_length	sepal_width	petal_length	petal_width	species		
2	5.1	3.5	1.4	0.2	setosa		
3	4.9	3	1.4	0.2	setosa		
4	4.7	3.2	1.3	0.2	setosa		
5	4.6	3.1	1.5	0.2	setosa		
6	4.2	3.6	1.4	0.2	setosa		
7	5.4	3.9	1.7	0.4	setosa		
8	4.6	3.4	1.4	0.3	setosa		
9	5	3.4	1.5	0.2	setosa		
10	7	3.2	4.7	1.4	versicolor		
11	6.4	3.2	4.5	1.5	versicolor		
12	6.9	3.1	4.9	1.5	versicolor		
13	5.5	2.3	4	1.3	versicolor		
14	6.5	2.8	4.6	1.5	versicolor		
15	5.7	2.8	4.5	1.3	versicolor		
16	6.3	3.3	4.7	1.6	versicolor		
17	4.9	2.4	3.3	1	versicolor		
18	6.6	2.9	4.6	1.3	versicolor		
19	6.3	2.9	5.6	1.8	virginica		
20	6.5	3	5.8	2.2	virginica		
21	7.6	3	6.6	2.1	virginica		
22	4.9	2.5	4.5	1.7	virginica		
23	7.3	2.9	6.3	1.8	virginica		
24	6.7	2.5	5.8	1.8	virginica		
25	7.2	3.6	6.1	2.5	virginica		
26	6.5	3.2	5.1	2	virginica		

Fill: No Fill

Borders Style

Color

Select borders you want to change applying style chosen above

Indent: 0

Text Orientation

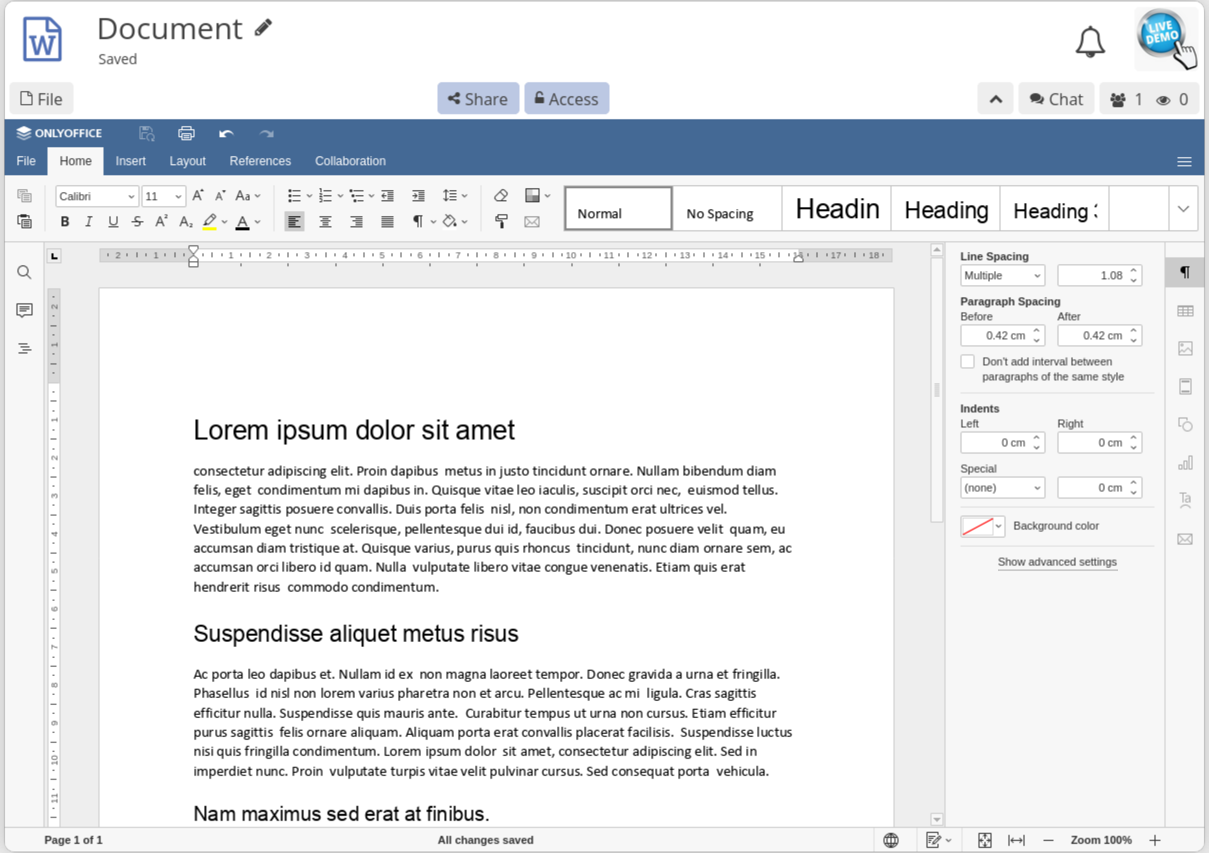
Angle: 0 °

Text Control

□ Wrap text

□ Shrink to fit

Conditional formatting



Lorem ipsum dolor sit amet

consectetur adipiscing elit. Proin dapibus metus in justo tincidunt ornare. Nullam bibendum diam felis, eget condimentum mi dapibus in. Quisque vitae leo iaculis, suscipit orci nec, euismod tellus. Integer sagittis posuere convallis. Duis porta felis nisl, non condimentum erat ultrices vel. Vestibulum eget nunc scelerisque, pellentesque dui id, faucibus dui. Donec posuere velit quam, eu accumsan diam tristique at. Quisque varius, purus quis rhoncus tincidunt, nunc diam ornare sem, ac accumsan orci libero id quam. Nulla vulputate libero vitae congue venenatis. Etiam quis erat hendrerit risus commodo condimentum.

Suspendisse aliquet metus risus

Ac porta leo dapibus et. Nullam id ex non magna laoreet tempor. Donec gravida a urna et fringilla. Phasellus id nisl non lorem varius pharetra non et arcu. Pellentesque ac mi ligula. Cras sagittis efficitur nulla. Suspendisse quis mauris ante. Curabitur tempus ut urna non cursus. Etiam efficitur purus sagittis felis ornare aliquam. Aliquam porta erat convallis placerat facilisis. Suspendisse luctus nisi quis fringilla condimentum. Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed in imperdiet nunc. Proin vulputate turpis vitae velit pulvinar cursus. Sed consequat porta vehicula.

Nam maximus sed erat at finibus.

Line Spacing
Multiple 1.08

Paragraph Spacing
Before 0.42 cm After 0.42 cm

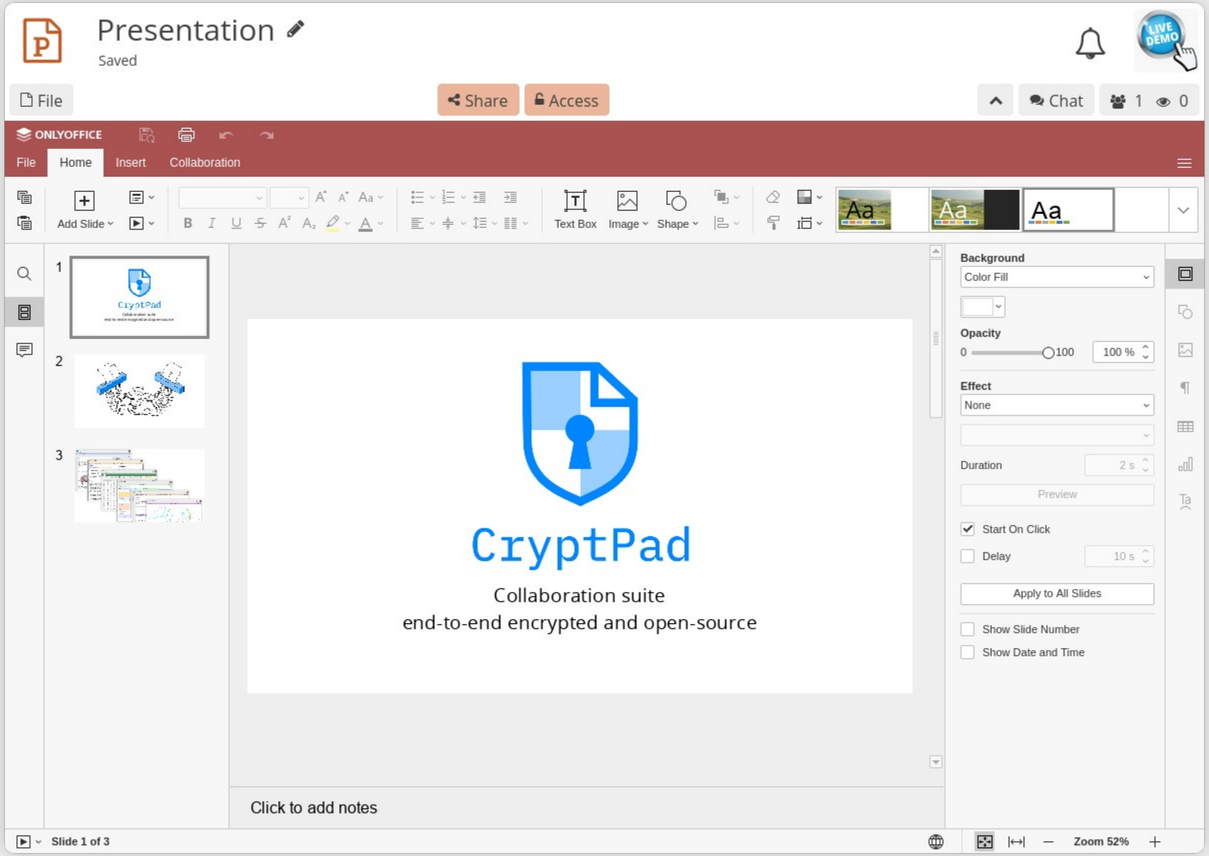
□ Don't add interval between paragraphs of the same style

Indents
Left 0 cm Right 0 cm

Special
(none) 0 cm

Background color

Show advanced settings



Presentation

Saved

CryptPad

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

Click to add notes

Background: Color Fill

Opacity: 100 %

Effect: None

Duration: 2 s

☑ Start On Click

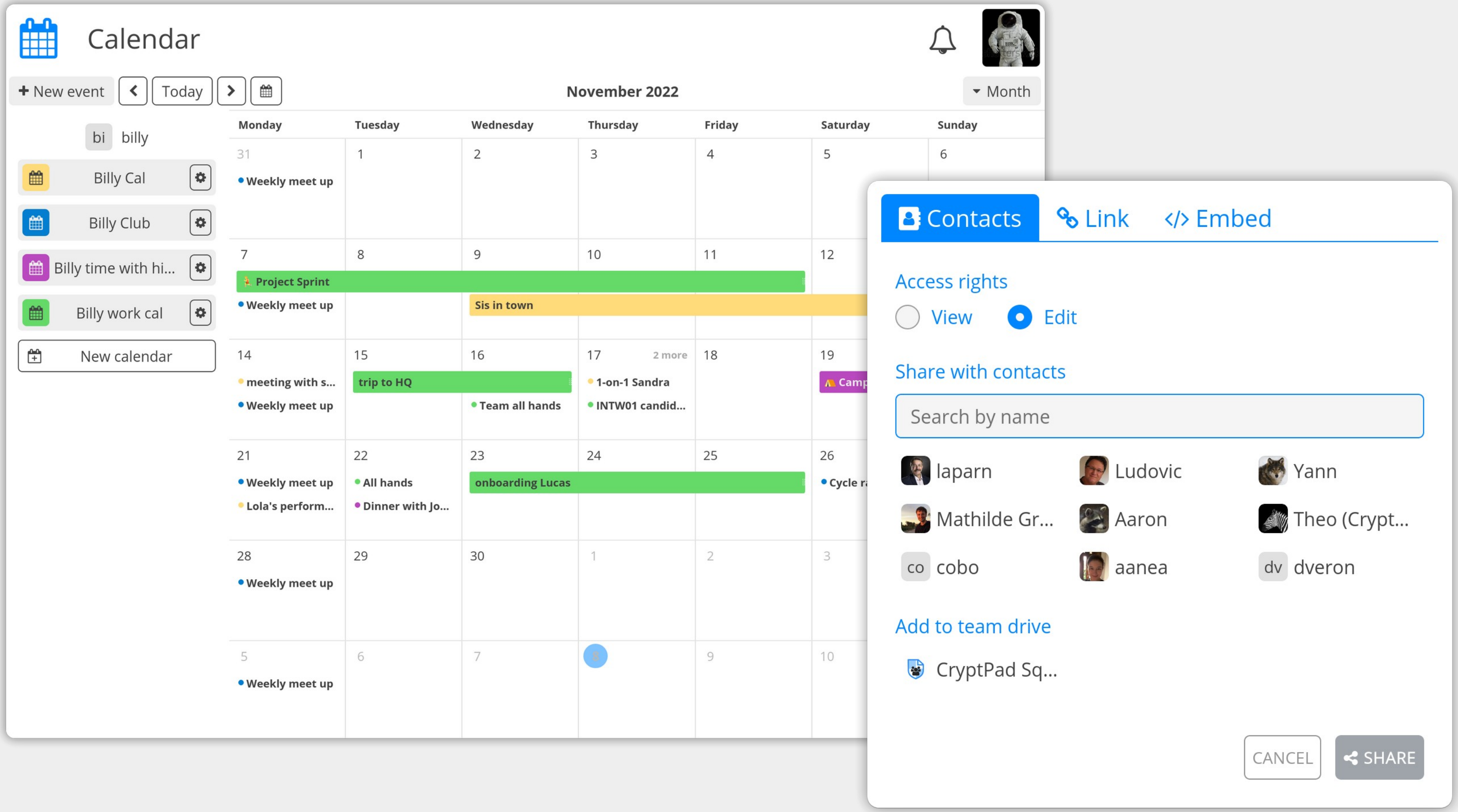
□ Delay 10 s

□ Show Slide Number

□ Show Date and Time

Slide 1 of 3

Zoom 52%



November 2022

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
31 ● Weekly meet up	1	2	3	4	5	6
7 Project Sprint ● Weekly meet up	8	9 Sis in town	10	11	12	
14 ● meeting with s... ● Weekly meet up	15 trip to HQ	16 ● Team all hands	17 2 more ● 1-on-1 Sandra ● INTW01 candid...	18	19 Camp	
21 ● Weekly meet up ● Lola's perform...	22 ● All hands ● Dinner with Jo...	23 onboarding Lucas	24	25	26 ● Cycle r	
28 ● Weekly meet up	29	30	1	2	3	
5 ● Weekly meet up	6	7	8	9	10	

Access rights

○ View ● Edit

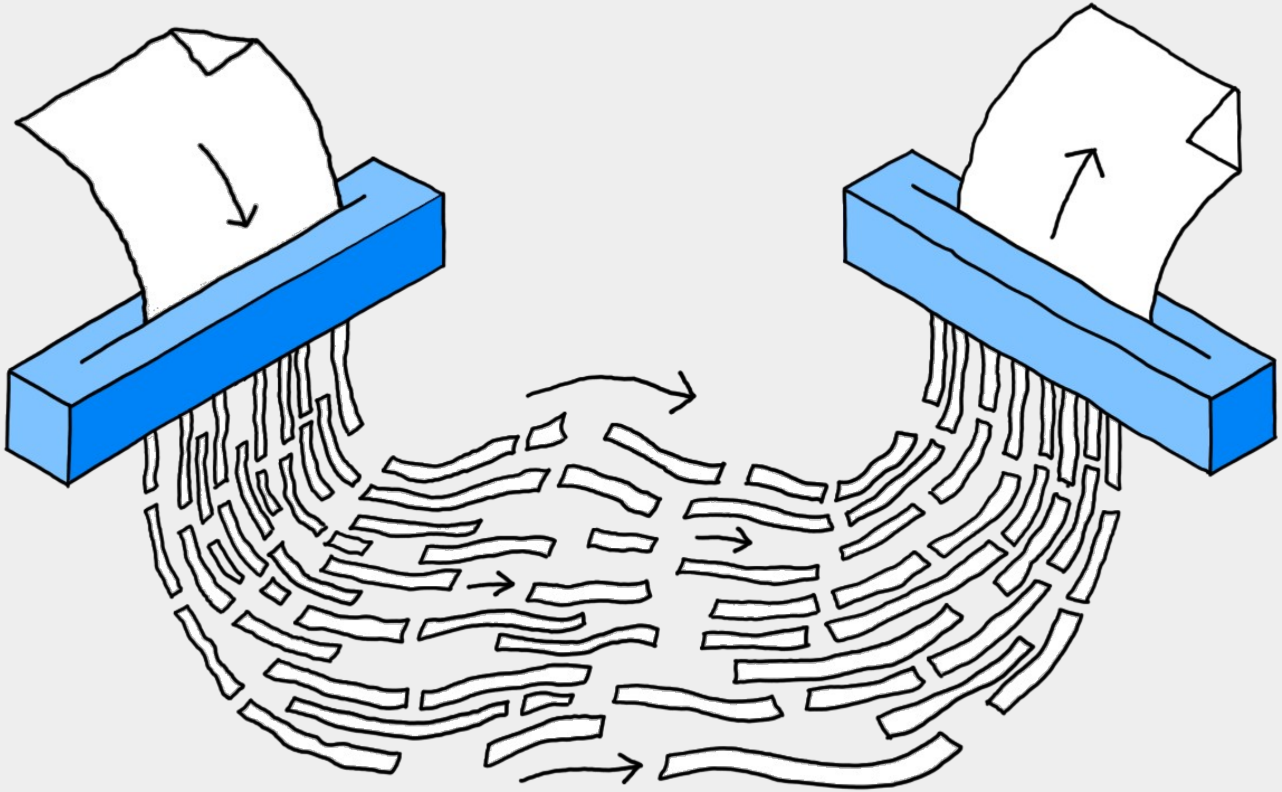
Share with contacts

Search by name

laparn
Ludovic
Yann
Mathilde Gr...
Aaron
Theo (Crypt...
co cobo
aanea
dv dveron

Add to team drive

CryptPad Sq...



Research

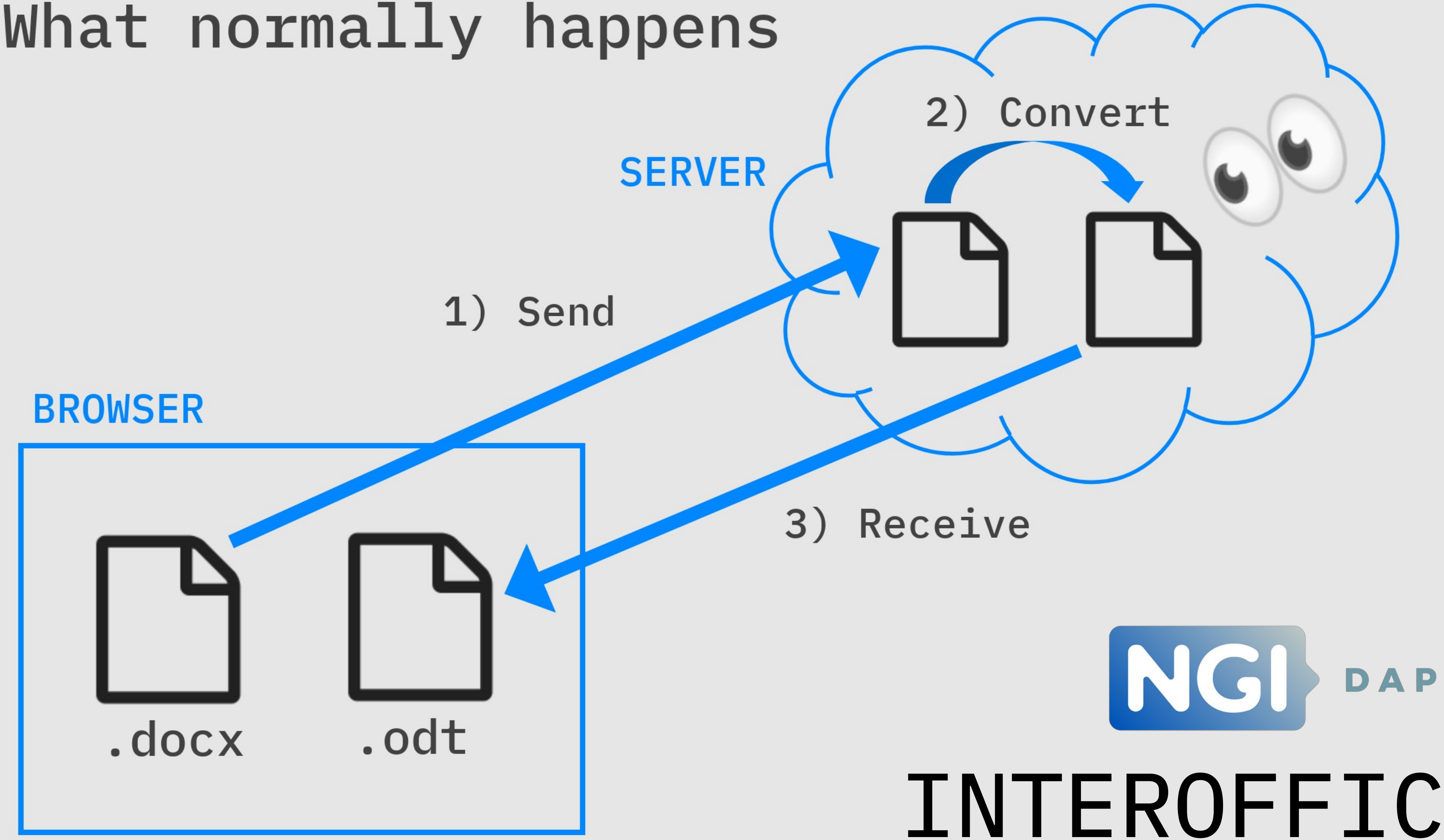
nlnet FOUNDATION

NGI ZERO ENTRUST

NGI ASSURE

NGI DAPSI

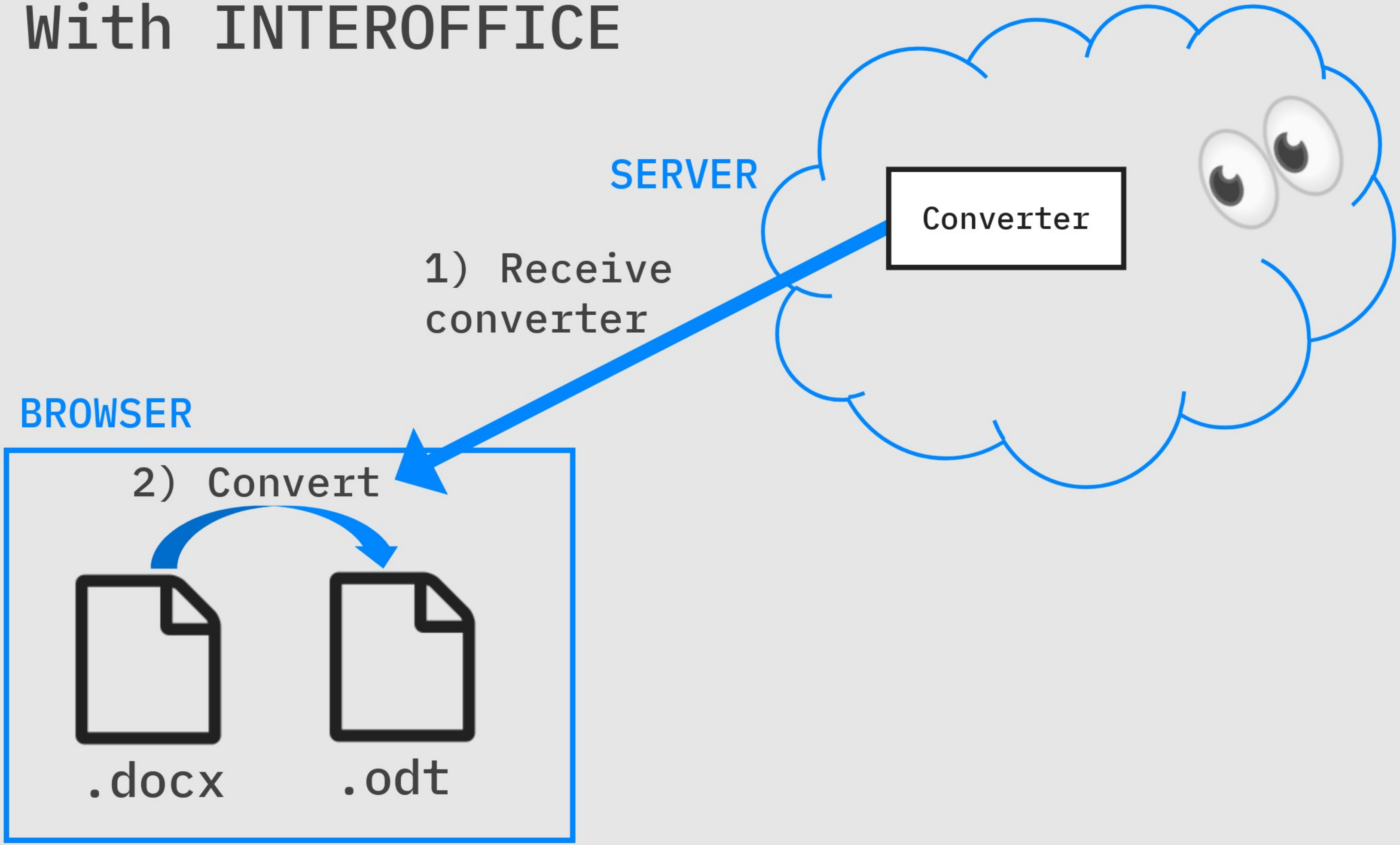
A)What normally happens



NGI DAPSI

INTEROFFICE

B) With INTEROFFICE



CryptPad Blueprints

NGI ZERO ENTRUST

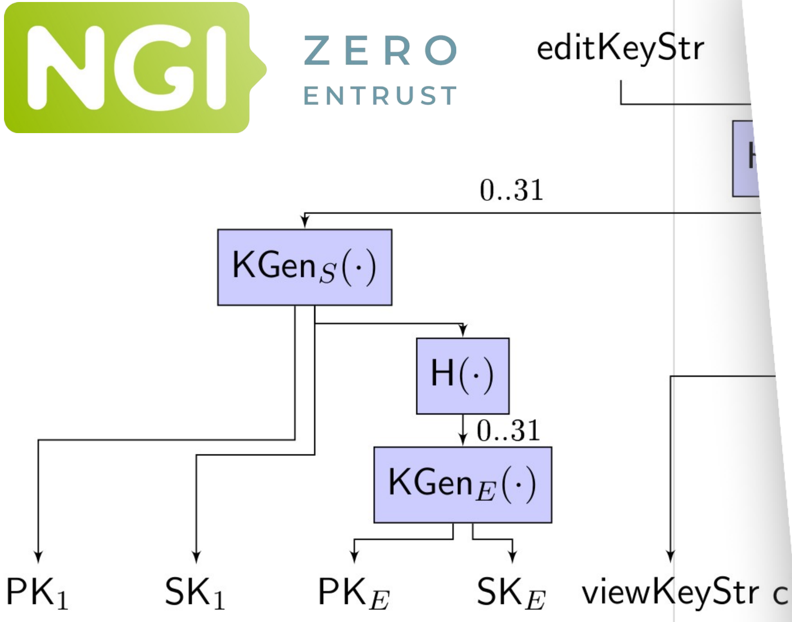
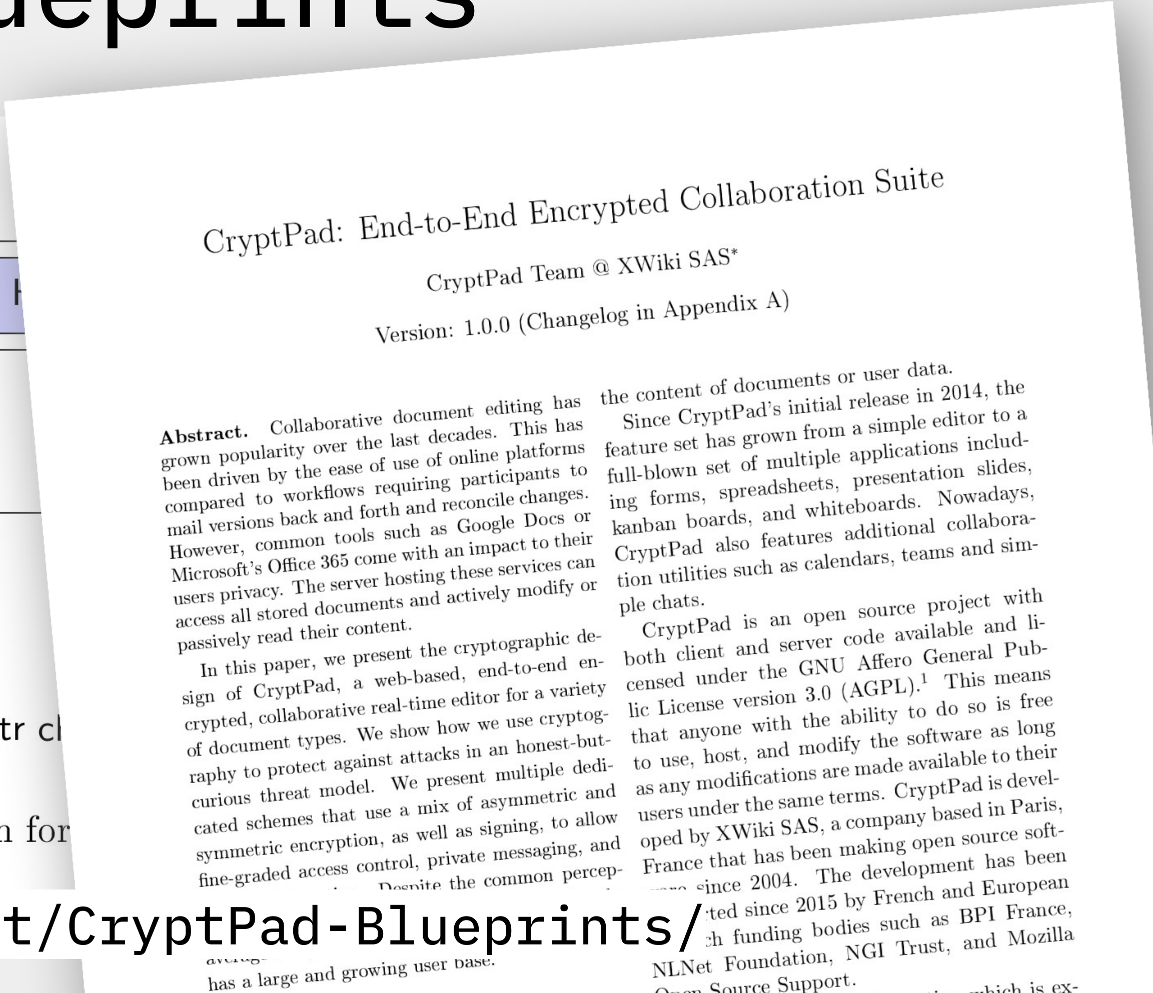


Figure 3: Key derivation for



CryptPad: End-to-End Encrypted Collaboration Suite

CryptPad Team @ XWiki SAS*

Version: 1.0.0 (Changelog in Appendix A)

Abstract. Collaborative document editing has grown popularity over the last decades. This has been driven by the ease of use of online platforms compared to workflows requiring participants to mail versions back and forth and reconcile changes. However, common tools such as Google Docs or Microsoft's Office 365 come with an impact to their users privacy. The server hosting these services can access all stored documents and actively modify or passively read their content.

In this paper, we present the cryptographic design of CryptPad, a web-based, end-to-end encrypted, collaborative real-time editor for a variety of document types. We show how we use cryptography to protect against attacks in an honest-but-curious threat model. We present multiple dedicated schemes that use a mix of asymmetric and symmetric encryption, as well as signing, to allow fine-graded access control, private messaging, and

Despite the common percep-

averag-

has a large and growing user base.

the content of documents or user data.

Since CryptPad's initial release in 2014, the feature set has grown from a simple editor to a full-blown set of multiple applications including forms, spreadsheets, presentation slides, kanban boards, and whiteboards. Nowadays, CryptPad also features additional collaboration utilities such as calendars, teams and simple chats.

CryptPad is an open source project with both client and server code available and licensed under the GNU Affero General Public License version 3.0 (AGPL).[1] This means that anyone with the ability to do so is free to use, host, and modify the software as long as any modifications are made available to their users under the same terms. CryptPad is developed by XWiki SAS, a company based in Paris, France that has been making open source software since 2004. The development has been

ted since 2015 by French and European

ch funding bodies such as BPI France, NLNet Foundation, NGI Trust, and Mozilla Open Source Support.

which is ex-

https://nlnet.nl/project/CryptPad-Blueprints/

CryptPad AUTH

NGI ASSURE

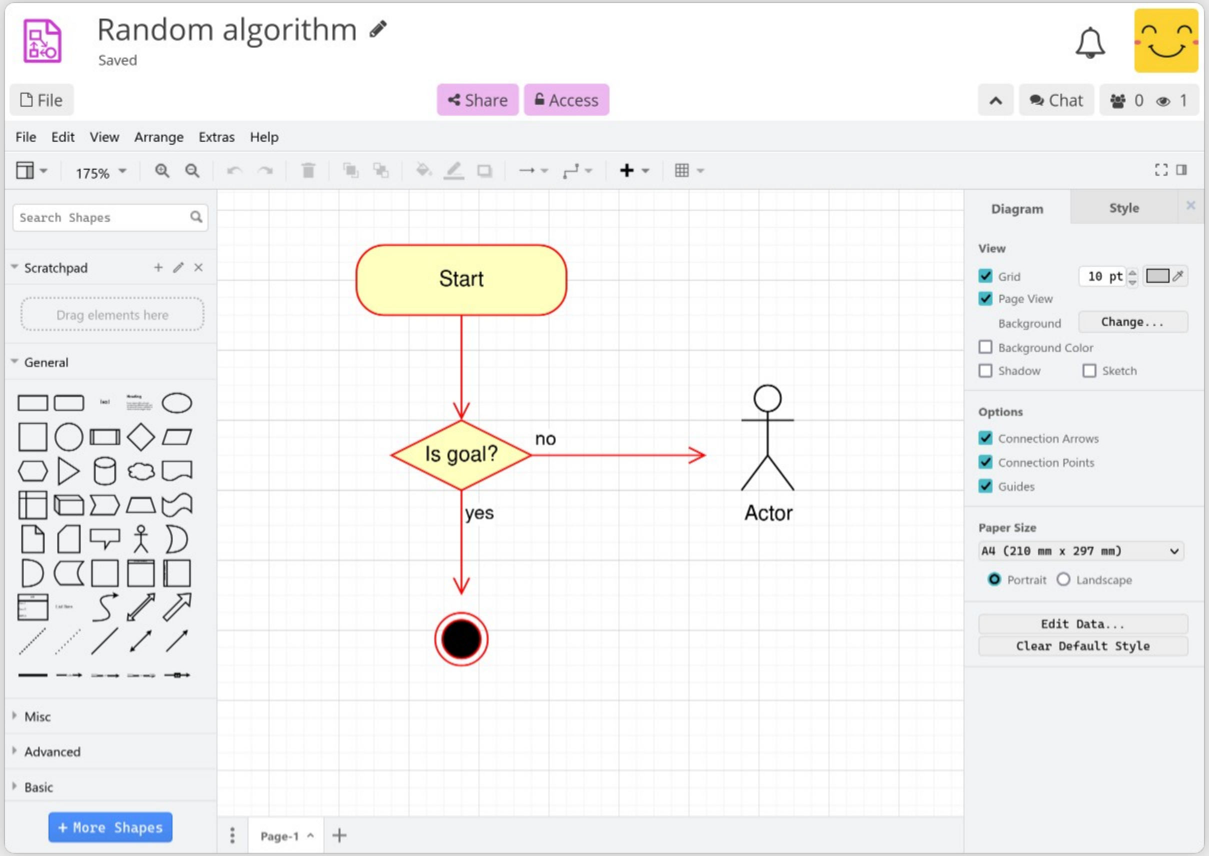
- Single Sign On
- Multi-factor authentication

https://nlnet.nl/project/CryptPad-Auth/

OpenDesk

- Diagram application
- Nextcloud integration

https://nlnet.nl/project/CryptPad-Auth/



☑ Grid 10 pt

☑ Page View

Background Change...

☐ Background Color

☐ Shadow ☐ Sketch

☑ Connection Arrows

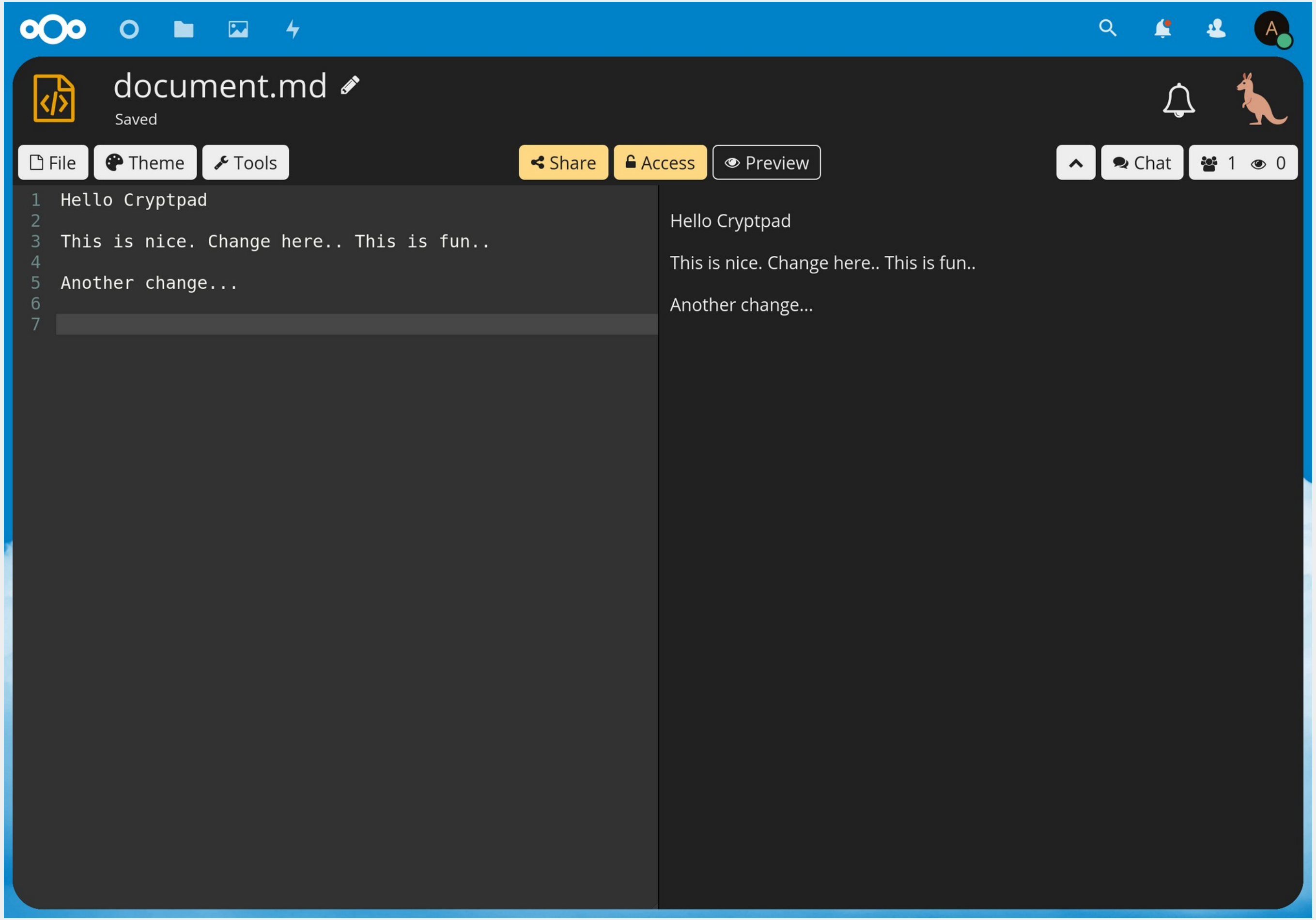
☑ Connection Points

☑ Guides

Paper Size

A4 (210 mm x 297 mm)

● Portrait ○ Landscape



```
Hello Cryptpad

This is nice. Change here.. This is fun..

Another change...

```

Hello Cryptpad

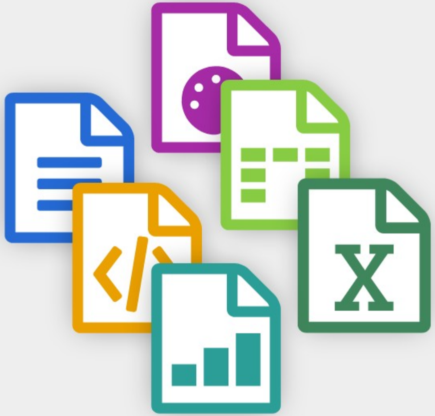
This is nice. Change here.. This is fun..

Another change...

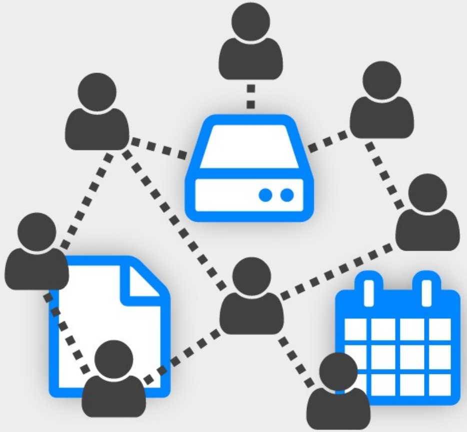
Cloud de Confiance

Sovereign Office Suite partnerships and subsidies

https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2023/04/20230406_cp_f2030-offres_cloud_de_confiance_vf.pdf



End-to-end encrypted



Full suite of apps

Real-time editing and collaboration

cryptpad.org

David Benqué
David.benque@xwiki.com
@dbenque:matrix.xwiki.com

David - Project Lead
Yann - Privacy Engineer
Wolfgang - R&D Engineer
Faye - Cryptography Engineer
Fabrice – Cryptography Engineer
Mathilde - Community & Support
Zuzanna – Developer
Diana – Junior Developer
Daria – Junior Developer

Ludovic - XWiki CEO