PRIVACYSAFE

KWLUG home town talk
November 2024

Demo
with 3NWeb services on kwlug.org

Signal

Reflections: The ecosystem is moving

moxie0 on 10 May 2016

At Open Whisper Systems, we've been developing open source "consumer-facing" software for the

Stuck in time

In some circles, this has not been a popular opinion. When someone recently asked me about federating an unrelated communication platform into the Signal network, I told them that I thought we'd be unlikely to ever federate with clients and servers we don't control. Their retort was "that's dumb, how far would the internet have gotten without interoperable protocols defined by 3rd parties?"

matrix

On Privacy versus Freedom

2020-01-02 — Thoughts — Matthew Hodgson

A few years ago, back when Matrix was originally implementing end-to-end encryption, we asked Moxie (the project lead for Signal) whether he'd ever consider connecting Signal (then TextSecure) to Matrix. After all, one of Matrix's goals is to be an interoperability layer between other communication silos, and one of the reasons for us using Signal's Double Ratchet Algorithm for Matrix's encryption was to increase our chances of one day connecting with other apps using the same algorithm (Signal, WhatsApp, Google Allo, Skype, etc). Moxie politely declined, and then a few months later wrote "The ecosystem is moving" to elaborate his thoughts on why he feels he "no longer believes that it is possible to build a competitive federated messenger at all."

Signal

matrix

On Privacy versus

Reflectio

Threema compared to:

WhatsApp	Signal	Telegram

iginally
sked Moxie (the
project lead for Signal) whether he'd ever consider
e) to Matrix. After all,
teroperability layer
s, and one of the
ble Ratchet Algorithm for
e our chances of one
ing the same algorithm
kype, etc). Moxie
onths later wrote "The
his thoughts on why he
is possible to build a
at all."

At Open Whisper Systems, we've been developing open source "consumer-facing"

Stuck in time

In some circles, this has
opinion. When someone
federating an unrelated
into the Signal network,
we'd be unlikely to ever
servers we don't control.
dumb, how far would the
without interoperable pr
parties?"

Messengers Not Considered

Messengers based on the Matrix protocol, like Element, were not taken into account because the federation leads to considerable privacy drawbacks. For example, messages and metadata are permanently stored on **all** involved servers, which means that every server operator is able to track who communicates with whom at what point in time. In the same vein, it's evident for all server operators who the members of groups are, and the operator of a user's home server is, in theory, even able to access their contact list.

Signal

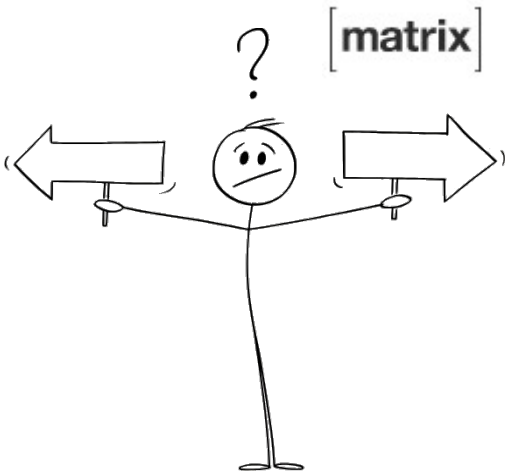
Reflections: The ecosystem is moving

moxie0 on 10 May 2016

At Open Whisper Systems, we've been developing open source "consumer-facing" software for the

Stuck in time

In some circles, this has not been a popular opinion. When someone recently asked me about federating an unrelated communication platform into the Signal network, I told them that I thought we'd be unlikely to ever federate with clients and servers we don't control. Their retort was "that's dumb, how far would the internet have gotten without interoperable protocols defined by 3rd parties?"



False Dilemma

On Privacy versus Freedom

2020-01-02 — Thoughts — Matthew Hodgson

A few years ago, back when Matrix was originally implementing end-to-end encryption, we asked Moxie (the project lead for Signal) whether he'd ever consider connecting Signal (then TextSecure) to Matrix. After all, one of Matrix's goals is to be an interoperability layer between other communication silos, and one of the reasons for us using Signal's Double Ratchet Algorithm for Matrix's encryption was to increase our chances of one day connecting with other apps using the same algorithm (Signal, WhatsApp, Google Allo, Skype, etc). Moxie politely declined, and then a few months later wrote "The ecosystem is moving" to elaborate his thoughts on why he feels he "no longer believes that it is possible to build a competitive federated messenger at all."

Demo
with 3NWeb services on kwlug.org

- dig TXT kwlug.org +short // how little is needed to setup 3NWeb services on own domain

Demo
with 3NWeb services on kwlug.org

- dig TXT kwlug.org +short // how little is needed to setup 3NWeb services on own domain

- 3nweb // service settings, signup token

Demo
with 3NWeb services on kwlug.org

- dig TXT kwlug.org +short // how little is needed to setup 3NWeb services on own domain

- 3nweb // service settings, signup token

- Client demo:
  signup
  launcher: it is a platform for 3NWeb apps
  chat with video

How it works?

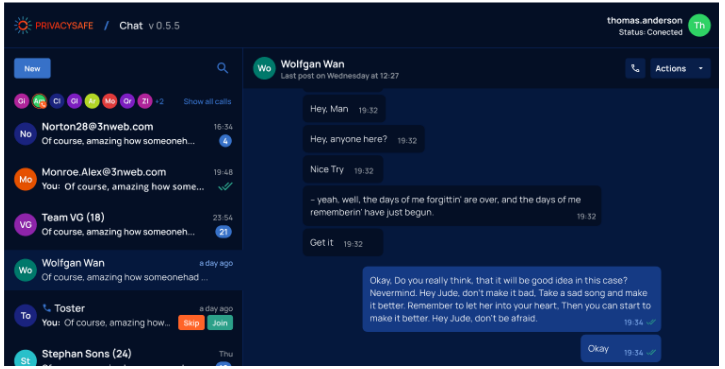
How it works?

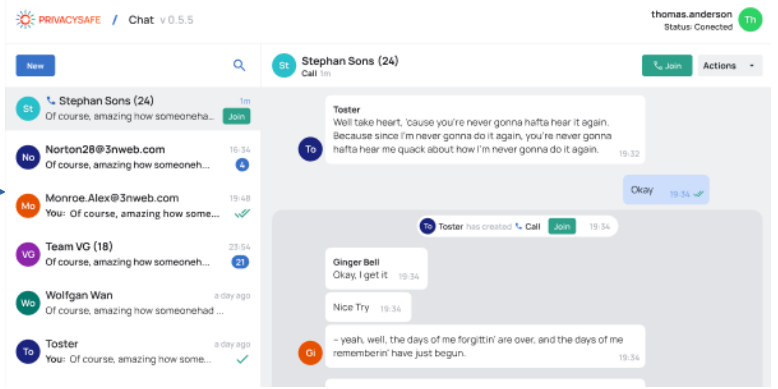
User need

How it works: convenience

User need

App for user need

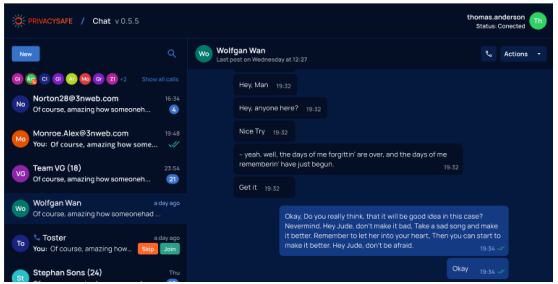


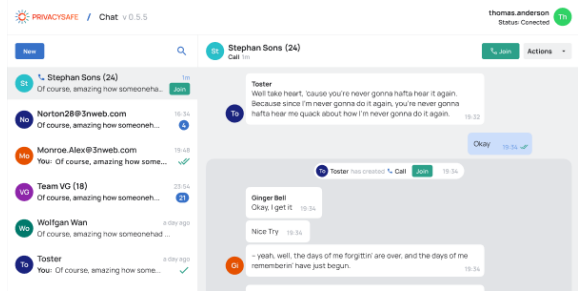


How it works: convenience with privacy, security

User need

App for user need





DNS

DNS

Client platform and servers

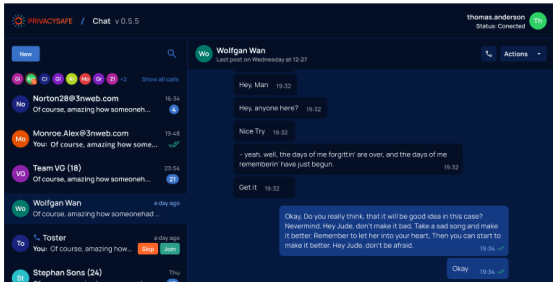
PRIVACYSAFE

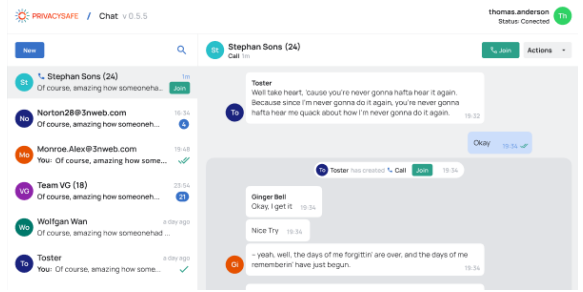
PRIVACYSAFE

How it works: convenience with privacy, security

User need

App for user need





DNS

DNS

Client platform and servers

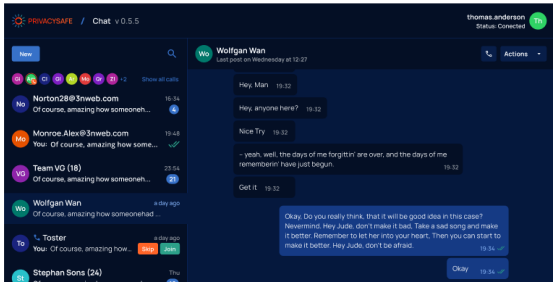
PRIVACYSAFE

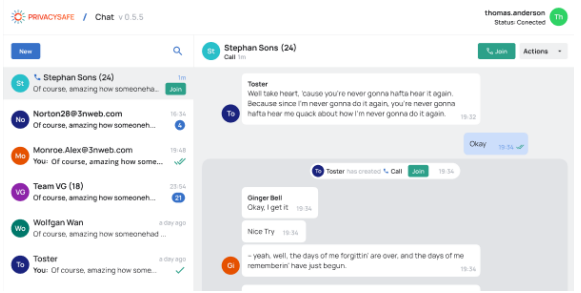
PRIVACYSAFE

How it works: convenience with privacy, security

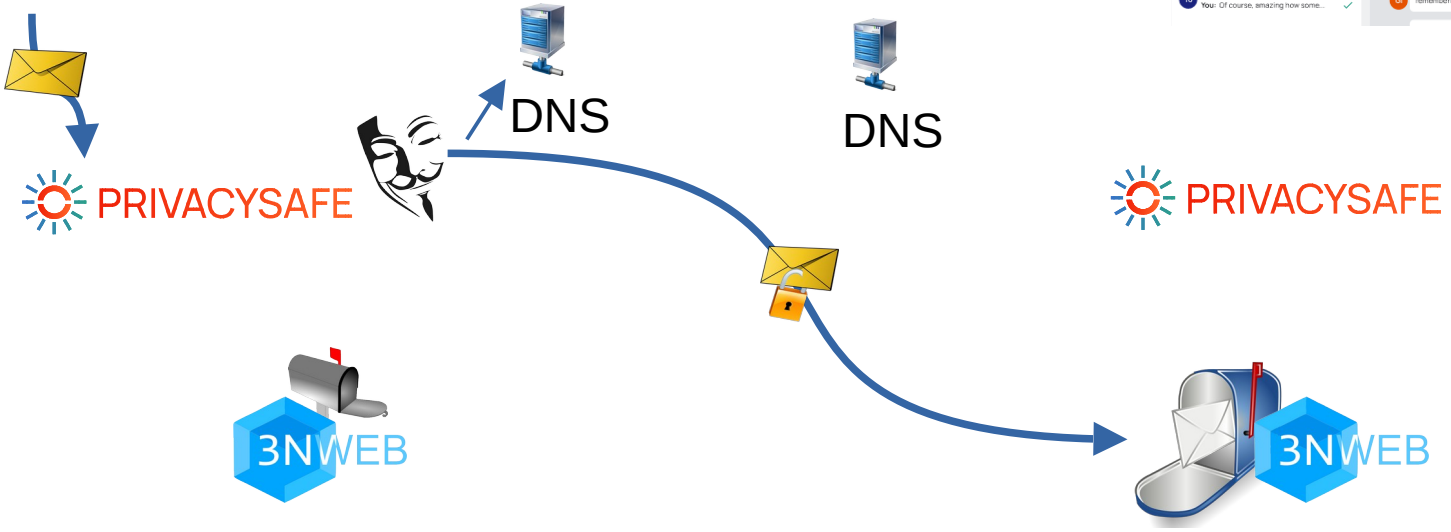
User need

App for user need





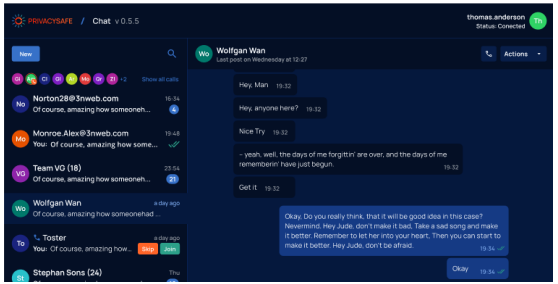
Client platform and servers

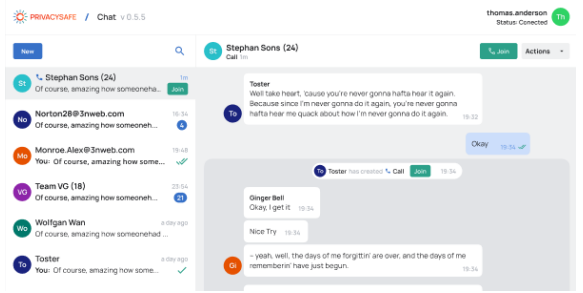


How it works: convenience with privacy, security

User need

App for user need





Client platform and servers

PRIVACYSAFE

DNS

DNS

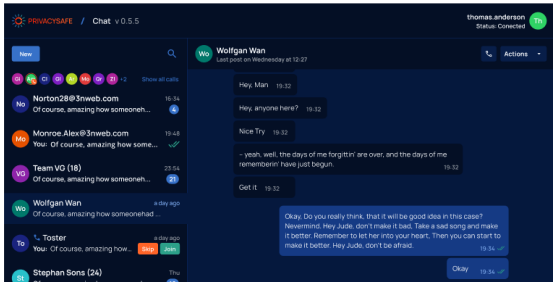
PRIVACYSAFE

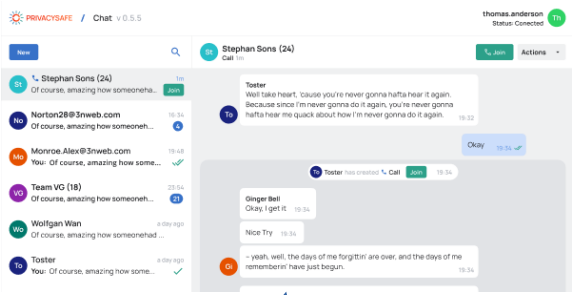
How it works: convenience with privacy, security

User need

App for user need

Client platform and servers





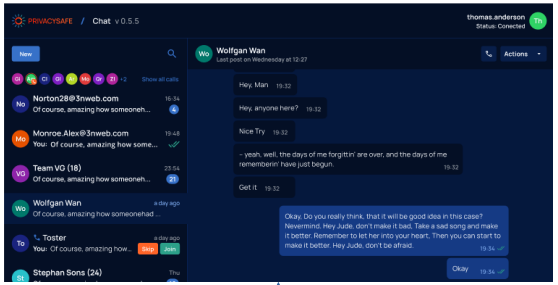
DNS

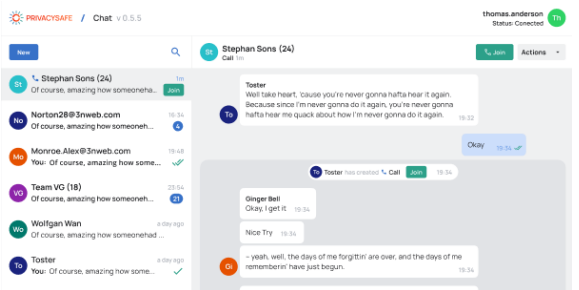
DNS

How it works: convenience with privacy, security

User need

App for user need





Client platform and servers

DNS

DNS

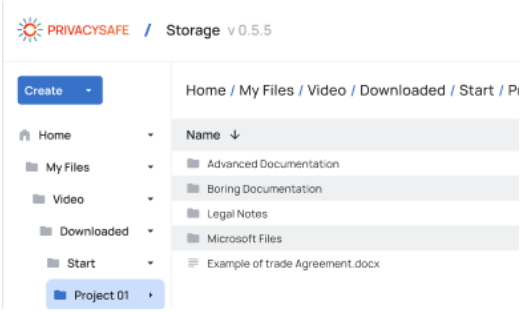
How it works: convenience with privacy, security

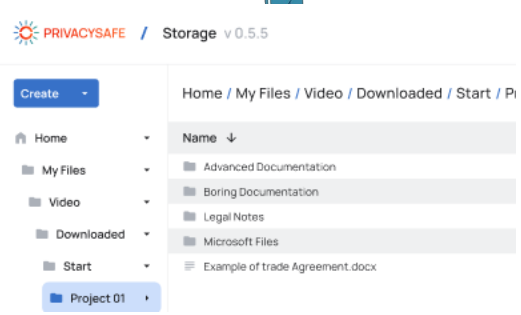
User need

How it works: convenience with privacy, security

User need

App for user need

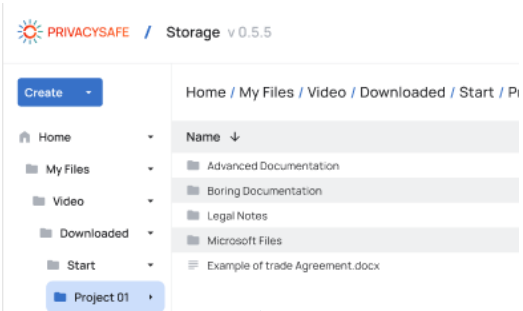


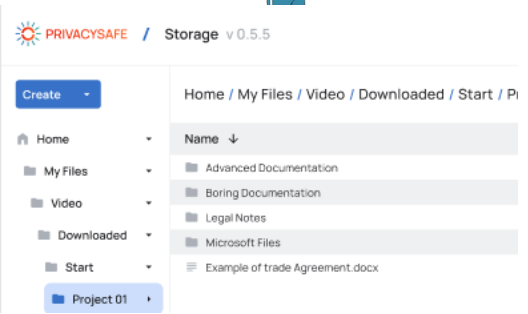


How it works: convenience with privacy, security

User need

App for user need





DNS

DNS

Client platform and servers

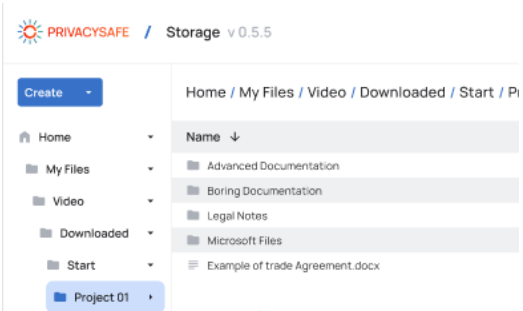
PRIVACYSAFE

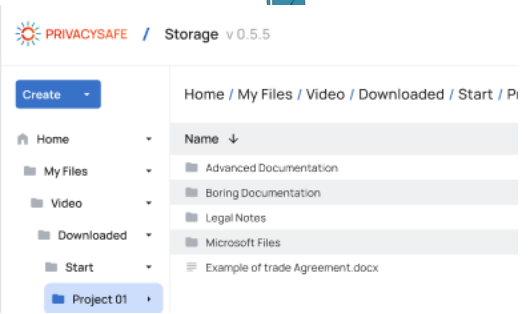
PRIVACYSAFE

How it works: convenience with privacy, security

User need

App for user need

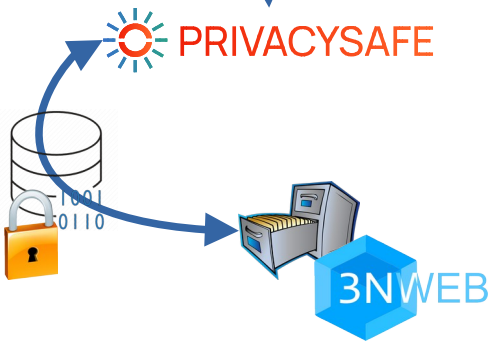




DNS

DNS

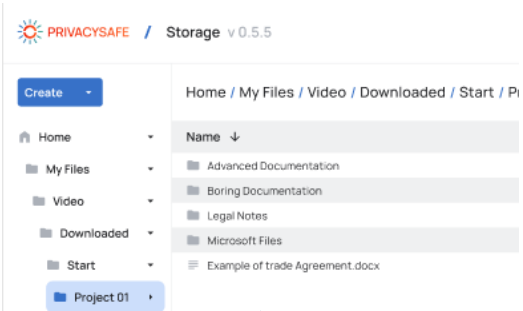
Client platform and servers

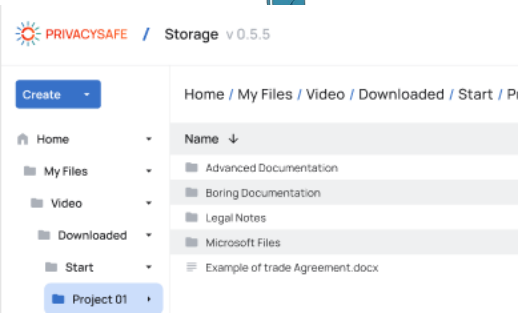


How it works: convenience with privacy, security

User need

App for user need





DNS

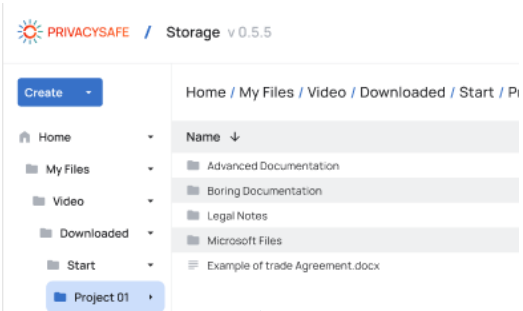
DNS

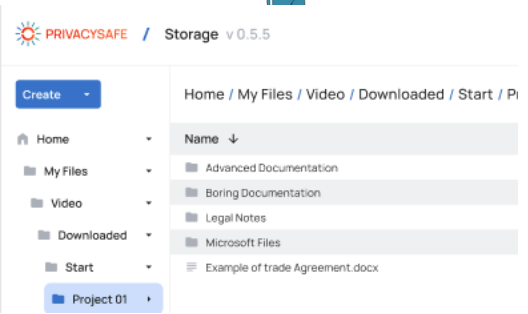
Client platform and servers

How it works: convenience with privacy, security

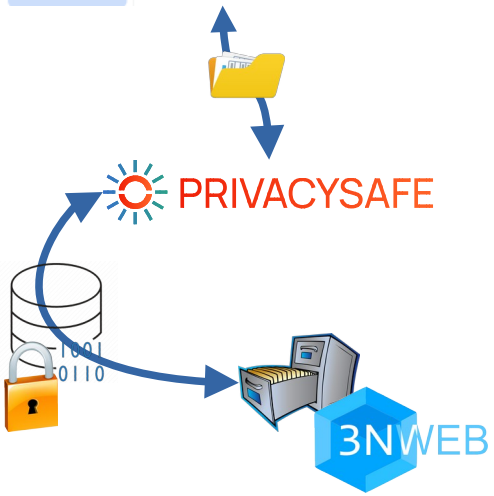
User need

App for user need





Client platform and servers



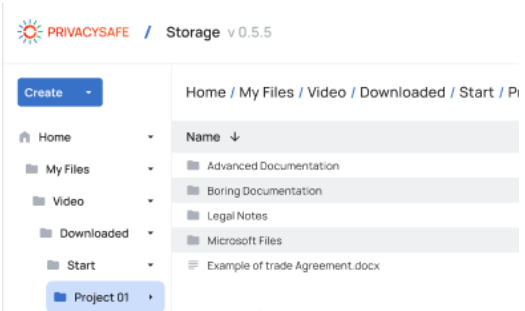
DNS

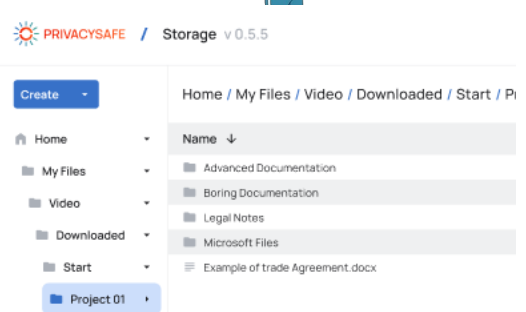
DNS

How it works: convenience with privacy, security

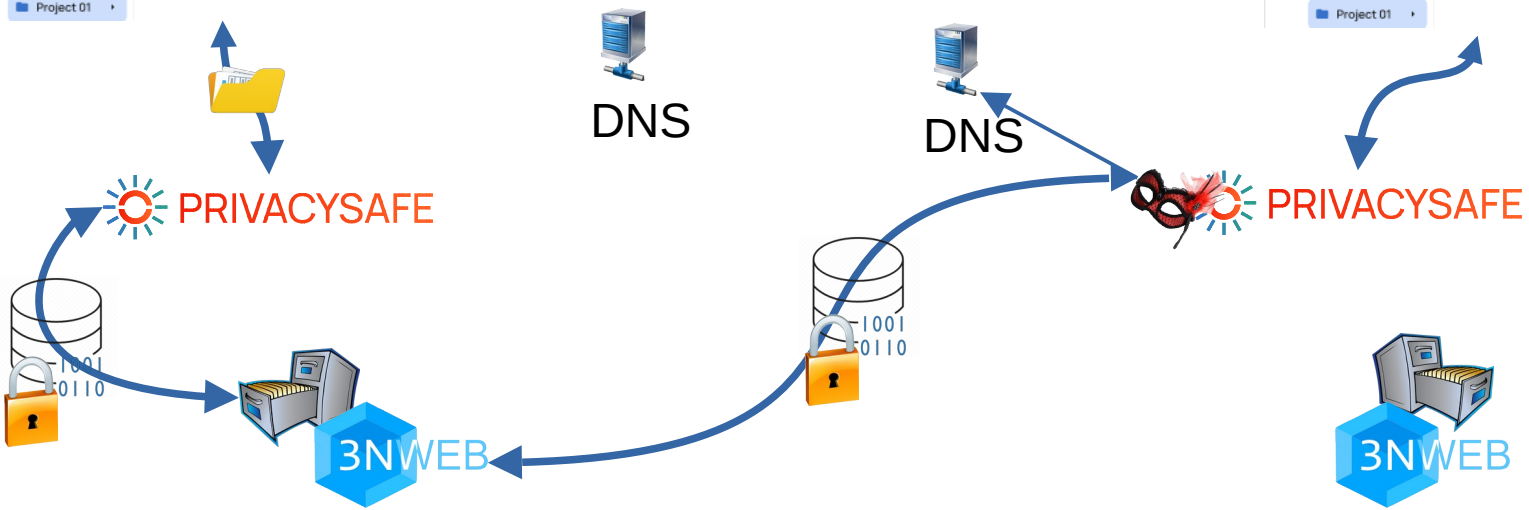
User need

App for user need





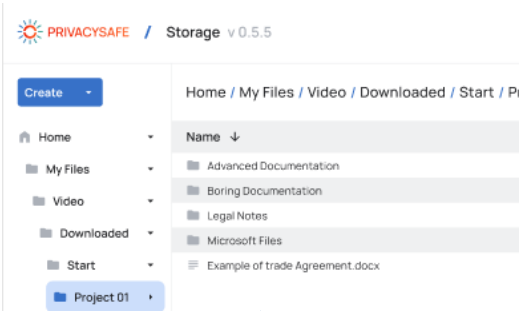
Client platform and servers

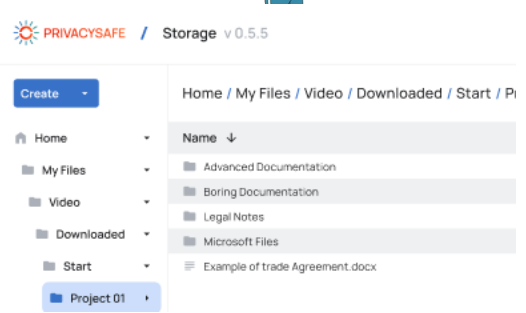


How it works: convenience with privacy, security

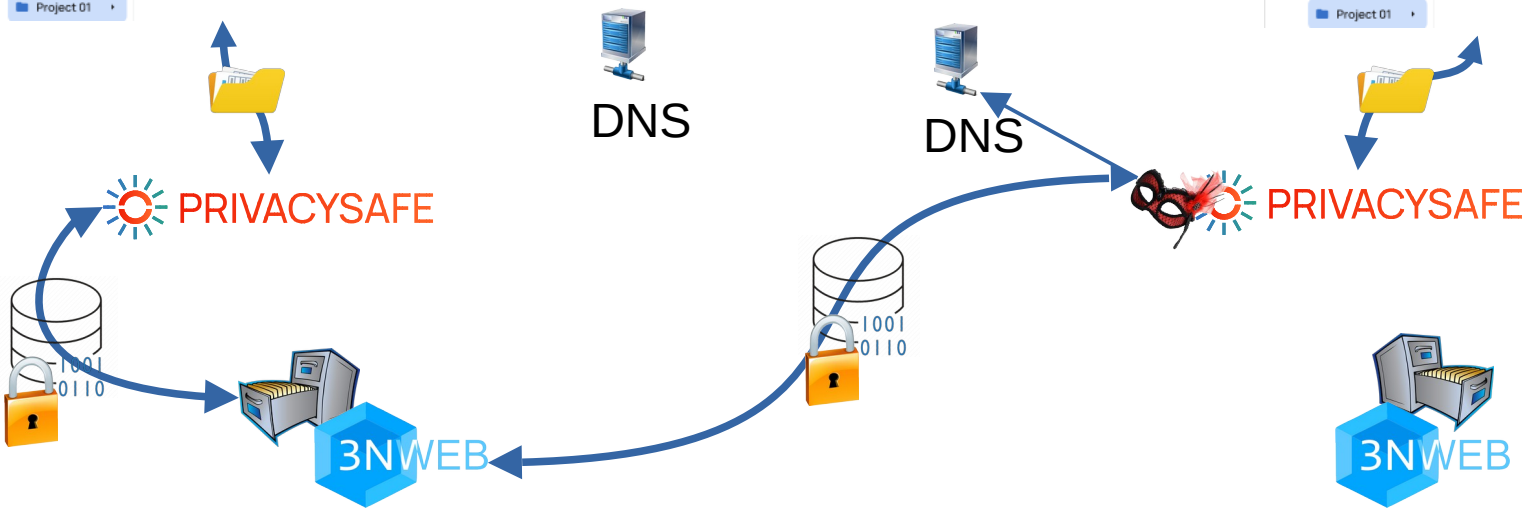
User need

App for user need





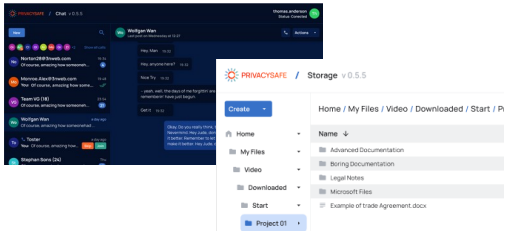
Client platform and servers

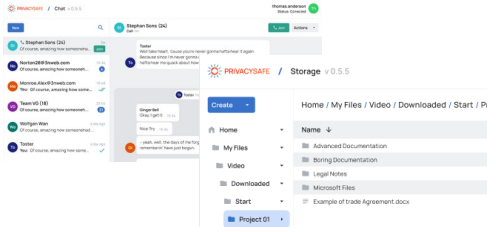


How it works: convenience with privacy, security, choice

User need

App for user need





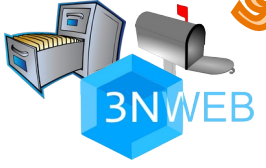
DNS

DNS

Client platform and servers

PRIVACYSAFE

Montague.it



PRIVACYSAFE

capulet.it

Convenience with privacy, security, freedom of choice

take all four with

based on

Without 3NWeb

End-to-End Encrypted Cloud Storage in the Wild: A Broken Ecosystem

Jonas Hofmann*
ETH Zurich
Switzerland
jonas.hofmann1@tu-darmstadt.de

Kien Tuong Truong
ETH Zurich
Switzerland
kientuong.truong@inf.ethz.ch

Table 2: Summary of the providers analysed, with the attacks and leakages that affect them.

● Attack works ◐ Attack works under specific conditions ○ Attack does not work – The attack is not applicable

	Unauthenticated Key Material	Unauthenticated Public Keys	Protocol Downgrade	Link-sharing Leakage	Unauthenticated Encryption	Unauthenticated Chunking	Tampering with Files and File Names	Tampering with Metadata	File Injection	Folder Injection	Leaks Plaintext Information	Leaks Metadata	Leaks Directory Structure
Sync	●	●	○	●	○	○	●	●	◐ *	●	○	●	●
pCloud	● †	–	○	–	○	●	●	●	●	●	○	●	●
Icedrive	○	–	○	–	●	●	●	●	◐ **	○	○	●	●
Seafile	○	–	●	–	●	●	●	●	◐ **	●	●	●	●
Tresorit	○	●	○	○	○	○	○	●	○	○	○	●	●

†Works in the CLI client. Most browsers implement adequate checks for public keys which prevents the attack in that setting.
*Only as a consequence of folder injection.
**The adversary can only create a new file by composing chunks of other files, hence the attack is not targeted.

Thank you.