

# User Freedoms

*Client side demo of PrivacySafe*

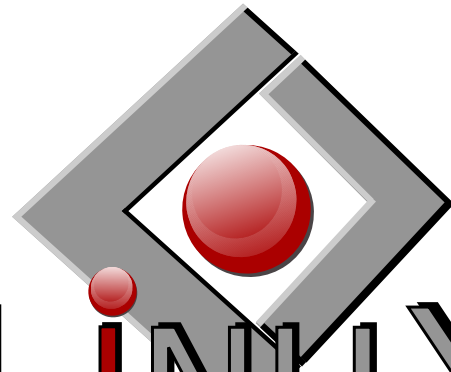
*KWLUG  
June 2022 talk*

# PDD: Presentation Driven Development

- 2019, September 9
- 2021, January 4
- Today, 2022, June 6

**KITCHENER-WATERLOO**

Present, present, present

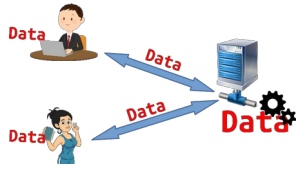


**LINUX**

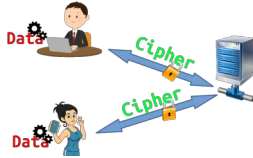
**USER GROUP**

# 3NWeb

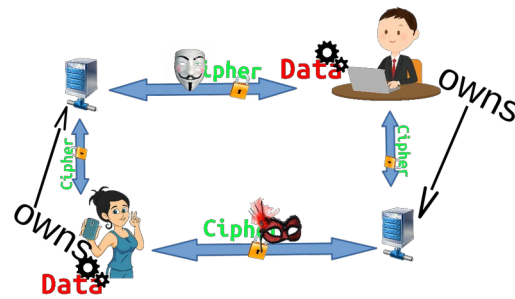
Digital Feudalism



Data Ownership



Digital Freedom



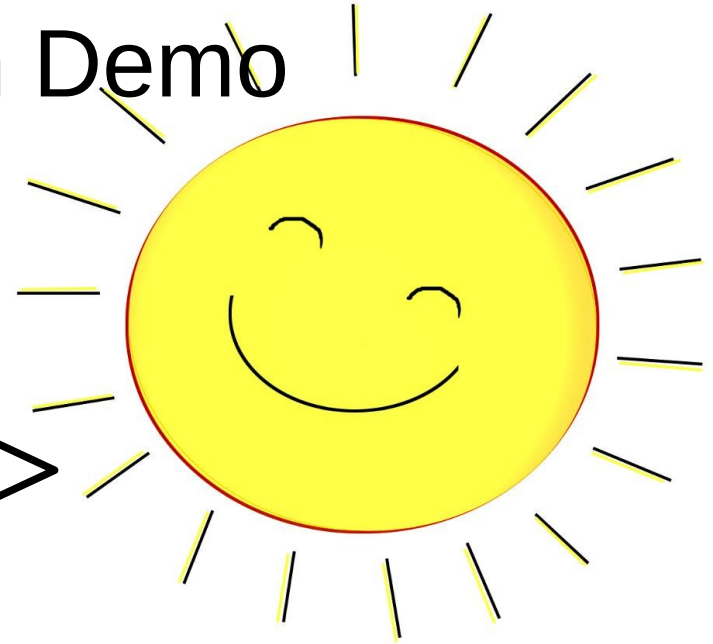
3NWeb is a set of utility services forming base for apps



# 3NComputer: user's own Live Space

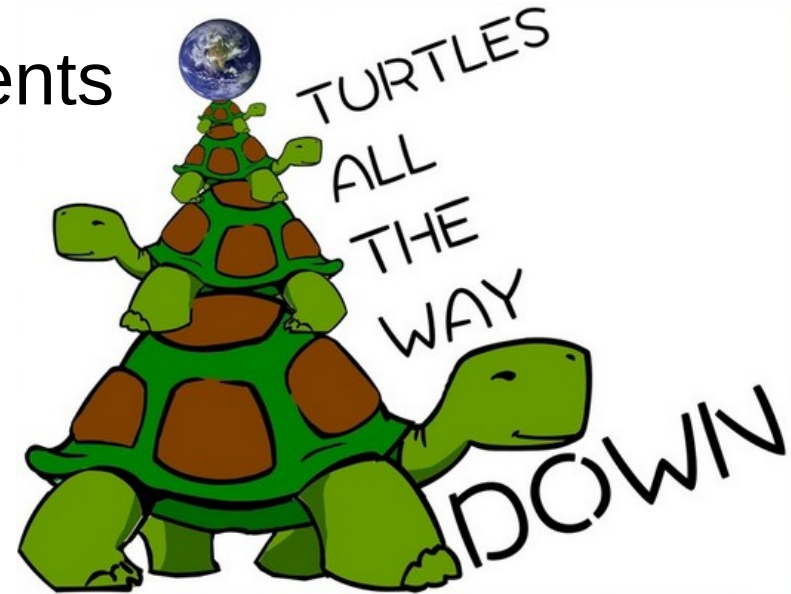


# Production Demo



# Besides encryption: segments in segments

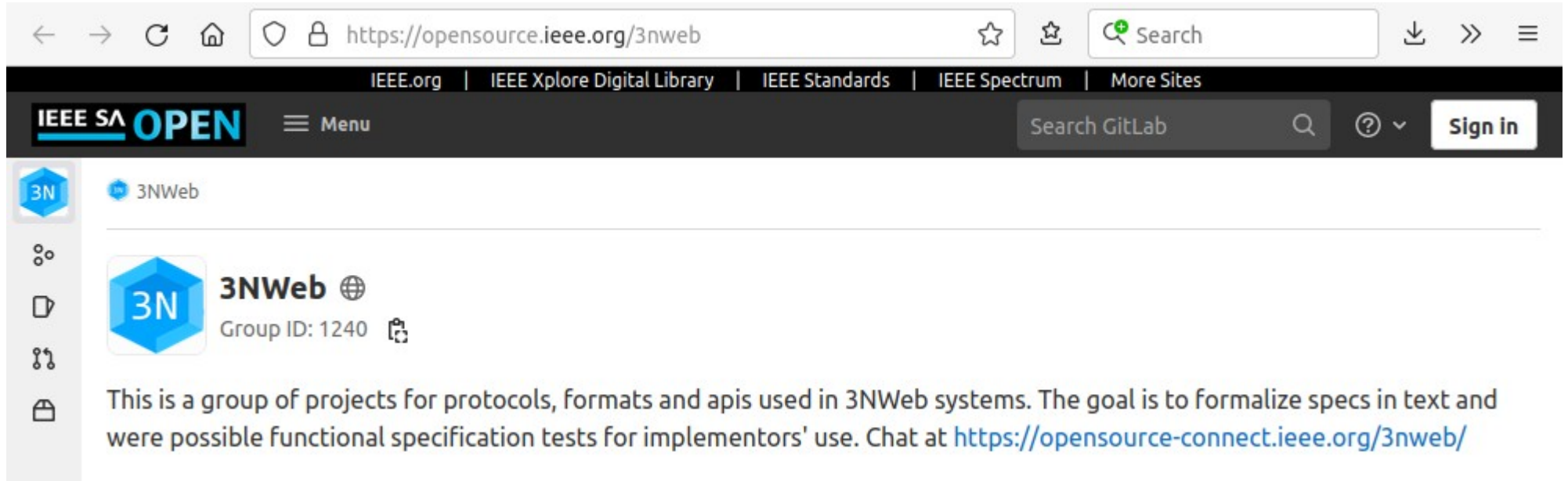
- NACL segments in encrypted object
- Segmentation to have out of order placement of cipher in file on physical disk
- Append write of encrypted segments with differently ordered content (hiding file write pattern)



# APIs, formats & protocols

Standards	Type	Needed by	Details
Public Key Login (PKL)	protocol	MailerId, ASMail, 3NStorage	Credentials based access without 3 <sup>rd</sup> parties (e.g. identity providers).
MailerId	protocol	ASMail, 3NStorage	Non-tracking identity, based on Mozilla's BrowserId approach, minus hacked browser part.
ASMail	protocol	OS' messaging functionality	3N-observing Web-style federated messaging protocol
3NStorage	protocol	OS' data persistence	3N-observing Web-style federated bulk storage protocol
XSP file format	format	ASMail, 3NStorage	AEAD (Authenticated-Encryption with Associated Data) format to pack NaCl ciphers (XSalsa+Poly)
File content packing	format	OS' file system functionality	While XSP packs encrypted segments it is beneficial to also have an additional file content segments' packing for efficiency in always encrypting, atomic versioning, and reduction of metadata in synchronization via servers.
OS to Apps IPC	api	Apps	Base approach to IPC between 3NWeb Apps and OS layers
File system objects	api	Apps	File system objects (capabilities) given to Apps
ASMail messaging	api	Apps	ASMail messaging object (capability) given to Apps
Apps and services IPC	api	Apps, OS	Meshing functionality as an application of UNIX philosophy
App manifest	format	OS	App manifest asks for capabilities, else OS doesn't give them

# 3NWeb @ IEEE



IEEE has allergy to GPL's, hence:

- specifications' test suites will here in MIT-flavour
- implementations' code elsewhere, which we distribute under GPL's



"The Rust Evangelism Strike Force"

Howard Pyle, 1897, oil on canvas

coming next:    Production