Gestió de claus (Password manager) a MyDisk

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

/rdlab
Engaged with your research

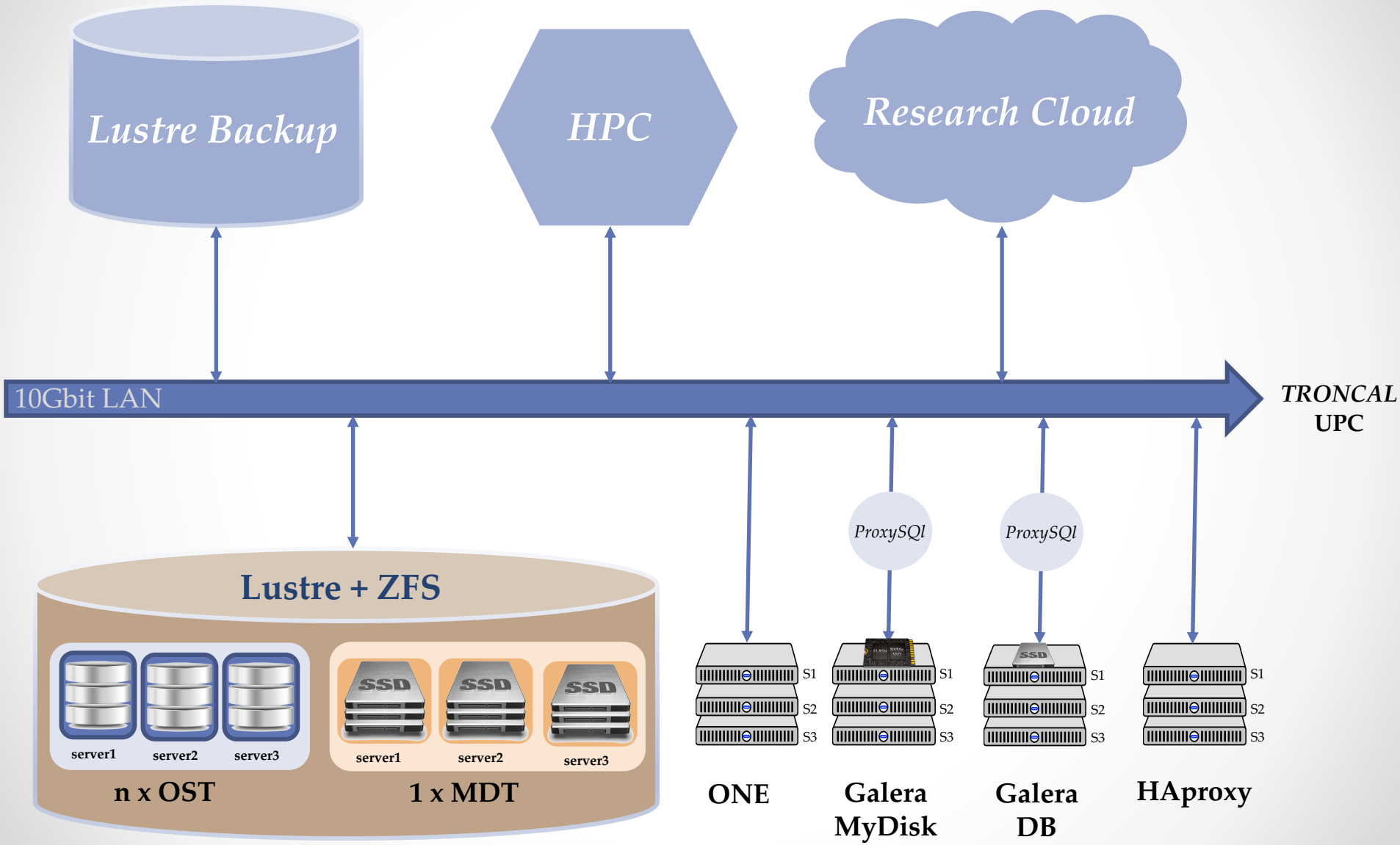
Març 2021

Gabriel Verdejo Álvarez

https://rdlab.cs.upc.edu
rdlab@cs.upc.edu

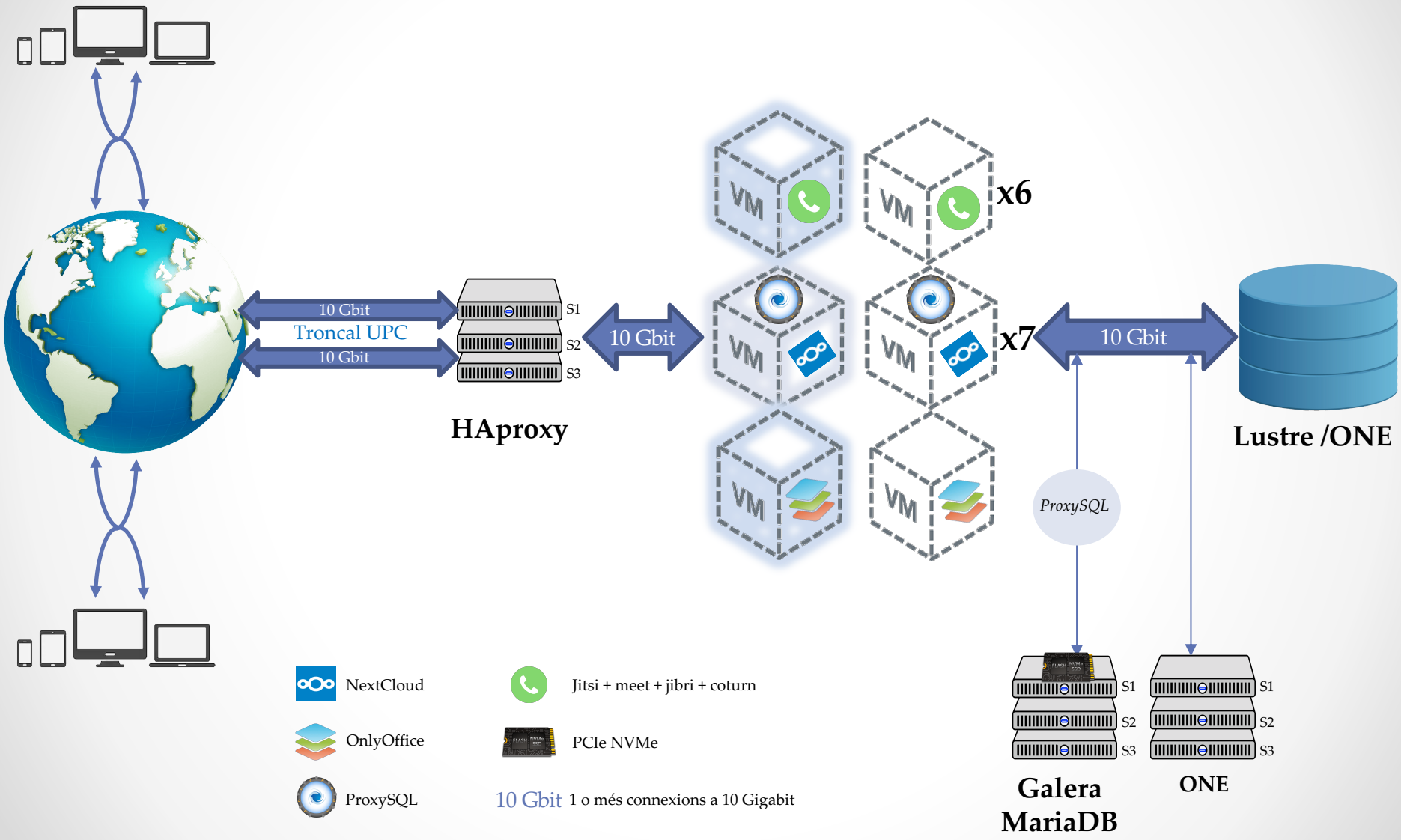
ÍNDEX DE CONTINGUTS

ARQUITECTURA /rdlab



rdlab@cs.upc.edu - https://rdlab.cs.upc.edu/

ARQUITECTURA /rdlab II (Mydisk)



rdlab@cs.upc.edu - https://rdlab.cs.upc.edu/

GESTOR DE PASSWORDS

- ***Perquè un GP/PM?***

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

COMPUTER SCIENCE DEPARTMENT

- ***Què ha de complir un "bon" GP/PM?***

  - Gestió completa (emmagatzemar, editar, capturar, generar i sincronitzar)
  - Segur (traçable, xifrat: local/DB + comunicació) ⇆ Confiable
  - Validació ⇆ Seguretat
  - Multiplataforma (S.O / Navegador /Aplicació)
  - "Fàcil de fer servir" (segur vs simple)

rdlab@cs.upc.edu - https://rdlab.cs.upc.edu/

GESTOR DE PASSWORDS II

- ***Perquè a la UPC?***

  - Per necessitats de recerca tenim dades, infraestructures i serveis locals

  - Seguretat: Garantia i control (*user risk management*)

  - Homogeneïtzació de solucions per la comunitat UPC

  - Sobirania digital i valor afegit

- ***Perquè a MyDisk?***

  - Estratègia digital de suport TIC a la recerca /rdlab (Plataforma universal)

  - Maduresa de les solucions (v.20+) i "*momentum*"

rdlab@cs.upc.edu - https://rdlab.cs.upc.edu/

GESTOR DE PASSWORDS A MyDisk (NC)

- ***Característiques bàsiques***

  - Servei natiu del projecte NextCloud (app oficial): Programari/projecte lliure

  - Permet gestionar tot tipus de contingut digital (password, tokens, cc...)

  - Classificació en carpetes, etiquetes i favorits (personalització)

  - Compartició amb altres usuaris de la plataforma (directe + codi QR)

  - Comprovació automàtica de fortalesa del password

  - Generació segura de claus amb elecció del grau de seguretat

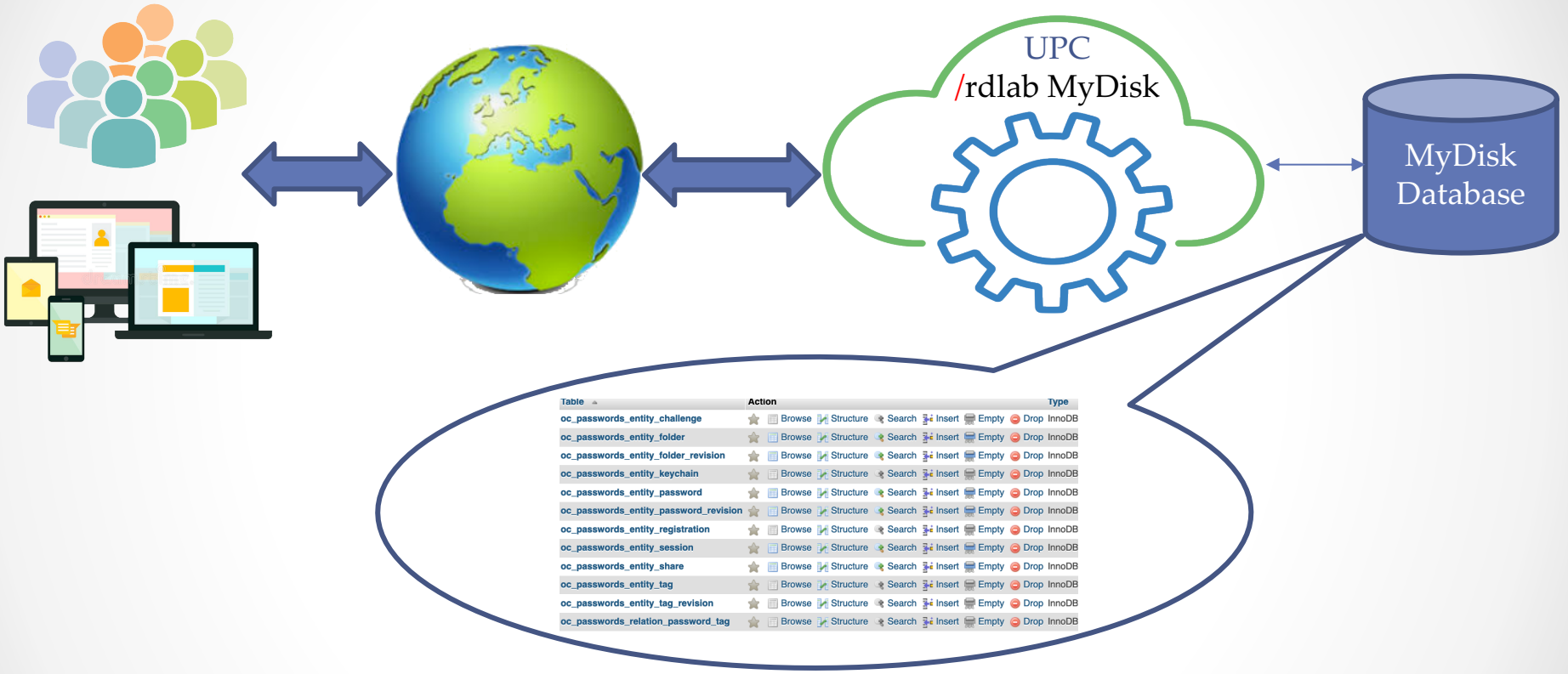
  - Sobirania digital: Importació/exportació i configuracions auto-gestionats

  - ***xifrat de dades a la BD per usuari***. No existeix password d'administrador!

rdlab@cs.upc.edu - https://rdlab.cs.upc.edu/

GESTOR DE PASSWORDS A MyDisk (NC) II

- ***Arquitectura de funcionament a MyDisk***



user_id	sse_type	sse_key	username	password	hash	status_code
gabriel.verdejo	SSEv1r2	u8EIR/6JrHNBCJHGKxJCFTHUHGN...	fa931dd64f7e5ea2f03192a7eefb1...	fcc09ea38917f5f076...	80029b1d4e5b52ae1...	BREACHED
ivan.couto	SSEv1r2	waCYI7QNluDiV8FZlJIOP4VFO3XE...	5d8314ee1e5ba7917890e2da19f...	0e0c05bb884b89c4...	e96116ecc3613778c8...	GOOD
gabriel.verdejo	SSEv1r2	PWpmN4lOrIP/s5zIfC4W5Rh1SpOt...	4b85249547594758403a7041e9e...	2e4e1d0f6cfdc0547...	3c5323f73eb665f00ae...	DUPLICATE
ivan.balana	SSEv1r2	3yxOK7SFJpf+9lnF4zJFpw4JDVn2...	f4807933debde2763b795b09c2a2...	30efdab282adadda84...	599589dd7174b20d1...	GOOD
gabriel.verdejo	SSEv1r2	nLT6tfKlfjkYvdk6HT3lbJsfITZzY2f...	92a04416251f0c494dae77cdc2770b...	93367d673188da3e60a...	3c5323f73eb665f00a...	DUPLICATE

rdlab@cs.upc.edu - https://rdlab.cs.upc.edu/

GESTOR DE PASSWORDS A MyDisk (NC) III

- ***Seguretat i xifrat [www10]***

- **Modes de xifrat, Server Side Encryption** (SSE):

  cap (none): L'usuari ja ha posat un password xifrat (no re-xifrar)

  SSEv1: Cada password es xifra amb una clau individual aleatòria generada pel servidor + clau específica única per usuari

  SSEv2: Els passwords es xifren seguint la cadena de claus/keychain que tingui configurat l'usuari al seu sistema. Per desxifrar, cal el password mestre (*master password*) del gestor de claus que faci servir l'usuari

- **Modes de xifrat, Client Side Encryption** (CSE):

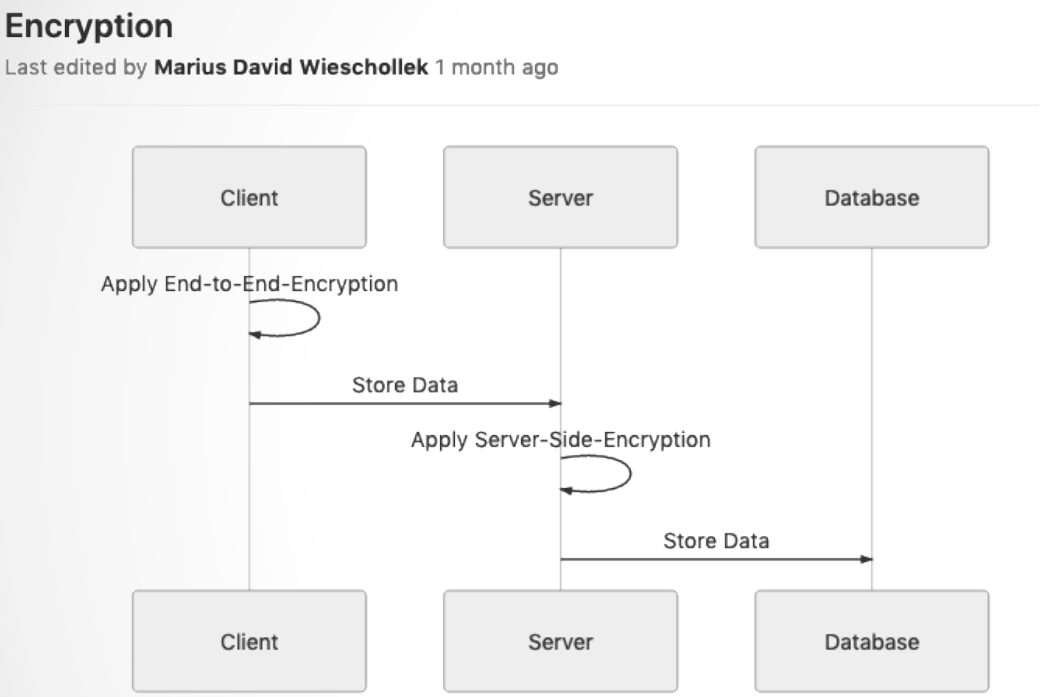
  cap (none): L'usuari no té configurat cap password mestre al seu sistema i per tant les claus s'intercanvien amb MyDisk **sempre de forma segura** fent servir https

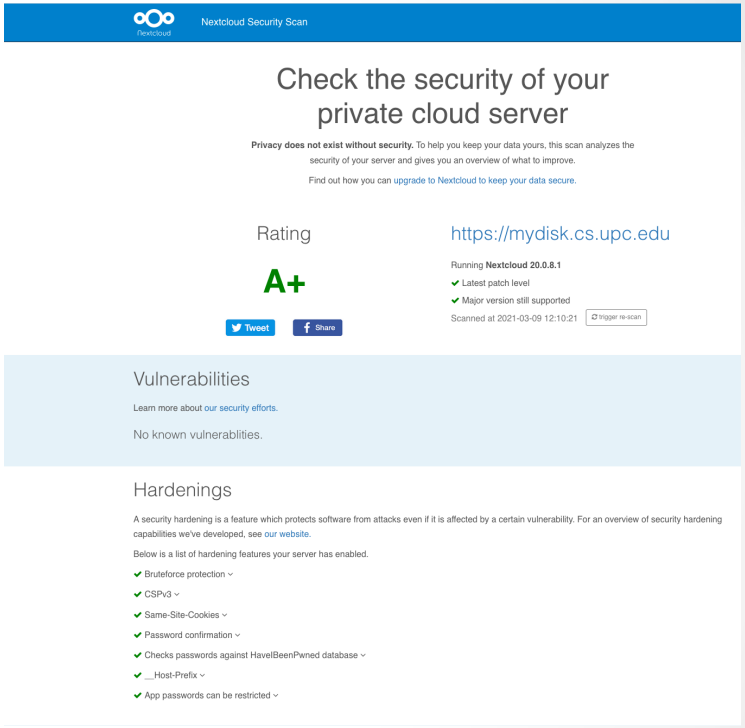
  CSEv1: L'usuari configura/té una clau mestre al seu sistema. L'intercanvi de claus amb MyDisk es fa **sempre de forma segura** amb https, i a més, les dades que circulen pel canal segur van xifrades amb aquest password de l'usuari

rdlab@cs.upc.edu - https://rdlab.cs.upc.edu/

GESTOR DE PASSWORDS A MyDisk (NC) IV

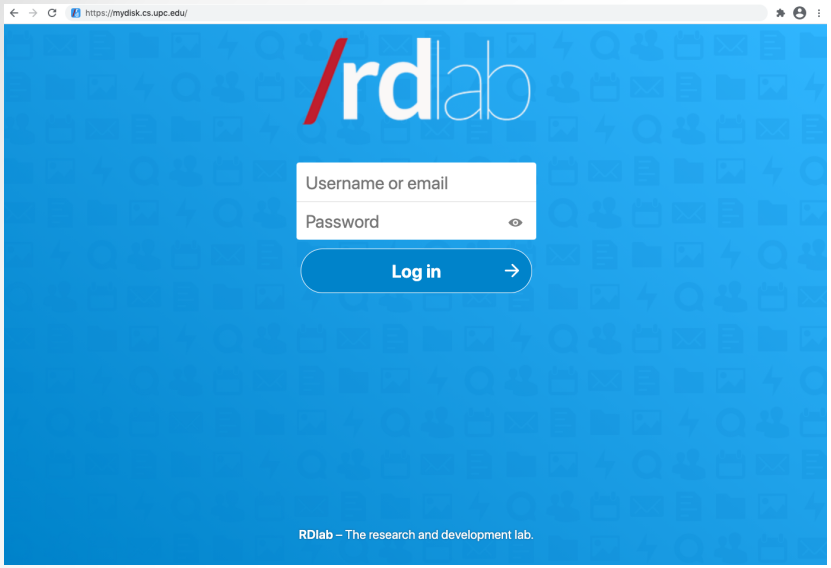
- ***Esquema visual***

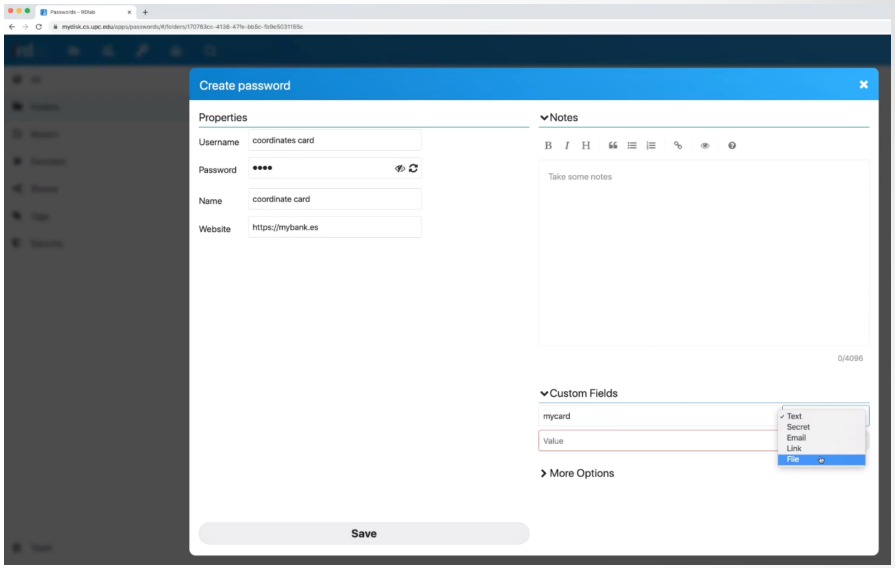


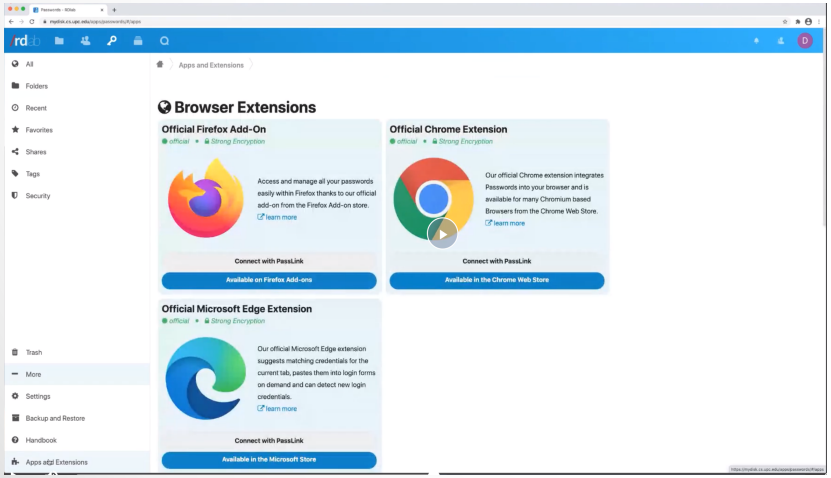


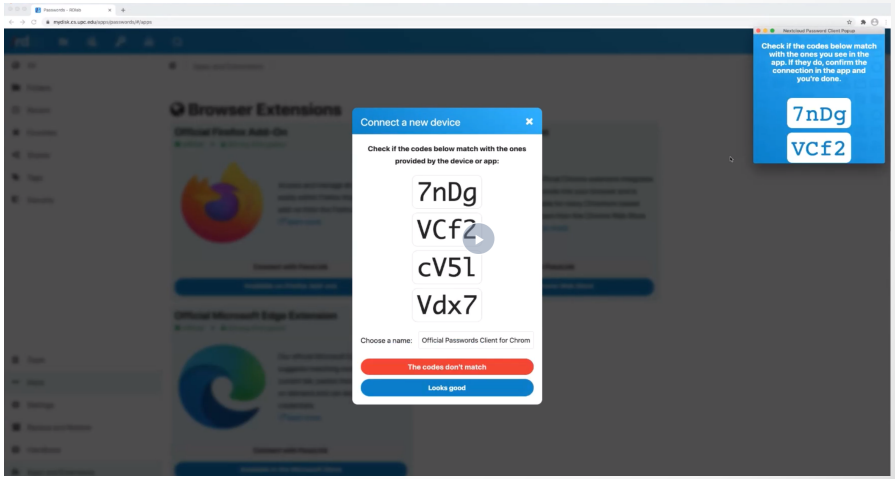
MyDisk només permet l'intercanvi de dades mitjançant SSL, i per tant, les comunicacions amb la UPC **sempre son segures**!

FUNCIONAMENT REAL (demo)

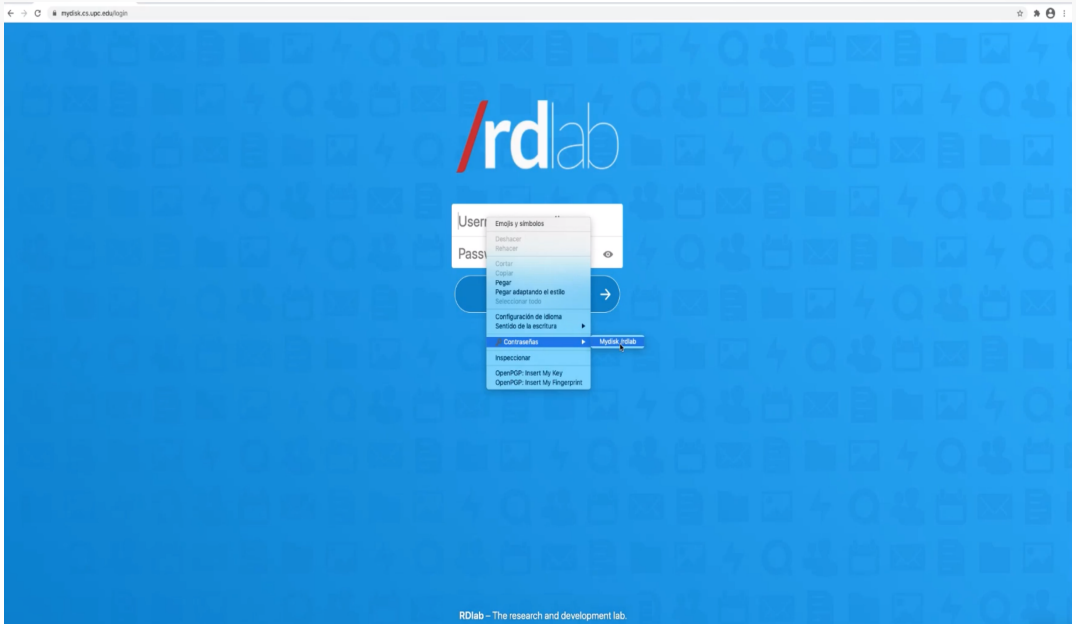


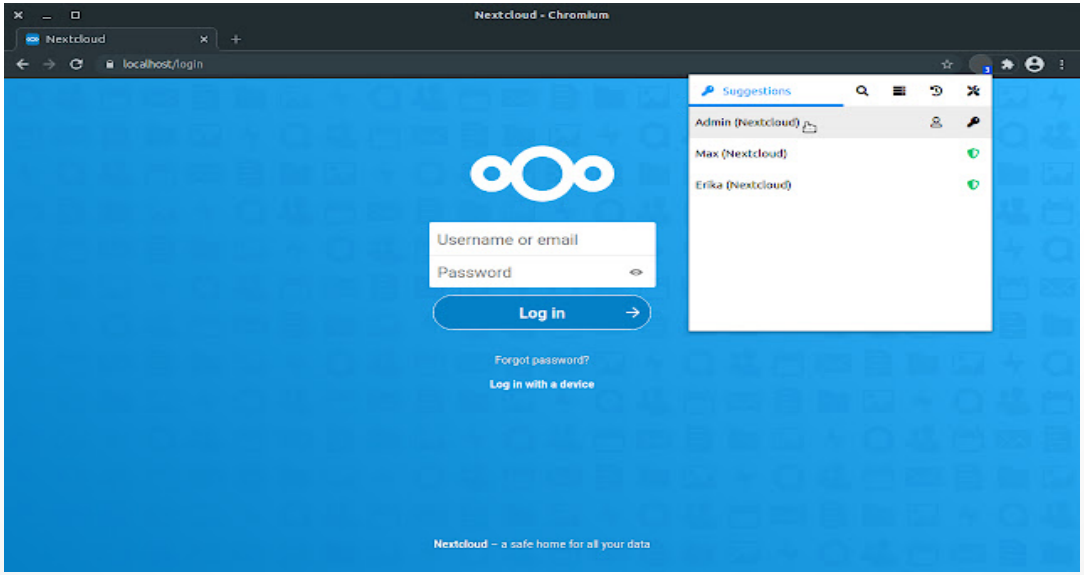






FUNCIONAMENT REAL (demo) II





FUNCIONAMENT REAL (demo) III

- ***Vídeo il.lustratiu del servei:***

https://mydisk.cs.upc.edu/s/fEHCaaf3iLXnBPs

rdlab@cs.upc.edu - https://rdlab.cs.upc.edu/

PROVA PILOT A LA UPC

- **Fase I**: Instal.lació i ús intern a /rdlab. Febrer 2021 (2-3 setmanes)

- **Fase II**: Prova pilot amb PAS i PDI de la UPC. Març 2021 (2-3 setmanes)

  - Corba d'aprenentatge d'usuari. Com de fàcil-difícil-intuïtiu és fer-lo servir?
  - Integració amb el dia a dia. Facilita i aporta coses, o resta?
  - Impressions i comparacions amb altres serveis de gestió de passwords
  - Grau de fiabilitat i confiança que dona el servei (seguretat percebuda i real)
  - Resiliència del servei. Proves sense connexió a MyDisk...
  - Avaluació dels extres (exportació dades, compartició amb tercers...)
  - Mancances que trobeu a les opcions/serveis
  - Documentació que penseu que caldria (howto/faq, vídeos d'ús, tutorials...)

Criteris d'avaluació

- **Fase III**: Desplegament pels nostres grups de recerca (Abril-Maig 2021)

  - Generació de documentació
  - Proves tutelades (caps de grup de recerca, influencers i early-adopters)

- **Fase IV**: (*wishlist*) Obrir-lo a altres serveis/col.lectius UPC (100 aniversari UPC?)

rdlab@cs.upc.edu - https://rdlab.cs.upc.edu/

rdlab@cs.upc.edu - https://rdlab.cs.upc.edu/

BIBLIOGRAFÍA/REFERÈNCIES

[www1] https://en.wikipedia.org/wiki/Password_manager
[www2] https://apps.nextcloud.com/apps/passwords
[www3] https://help.nextcloud.com/c/apps/passwords/133
[www4] https://git.mdns.eu/nextcloud/passwords
[www5] https://t.me/nc_passwords
[www6] https://github.com/marius-wieschollek/passwords
[www7] https://docs.nextcloud.com/server/latest/admin_manual/configuration_files/encryption_configuration.html
[www8] https://nextcloud.com/encryption/
[www9] https://nextcloud.com/endtoend/
[www10] https://git.mdns.eu/nextcloud/passwords/wikis/Users/Encryption
[www11] https://rdlab.cs.upc.edu
[www12] https://mydisk.cs.upc.edu