Mozilla Persona
for your domain

François Marier – @fmarier

mozilla

solving the

password problem

on the web

problem #1:

passwords are **hard to secure**

bcrypt / scrypt / pbkdf2

- bcrypt / scrypt / pbkdf2
- per-user salt

 bcrypt / scrypt / pbkdf2

 per-user salt

 site secret

 bcrypt / scrypt / pbkdf2

 per-user salt

 site secret

 password & lockout policies

 bcrypt / scrypt / pbkdf2

 per-user salt

 site secret

 password & lockout policies

 secure recovery


bcrypt / scrypt / pbkdf2
per-user salt
site secret
password & lockout policies
secure recovery
2013
password
guidelines

passwords are hard to secure

they are a **liability**

```
ALTER TABLE user
DROP COLUMN password;
```

problem #2:

passwords are **hard to remember**

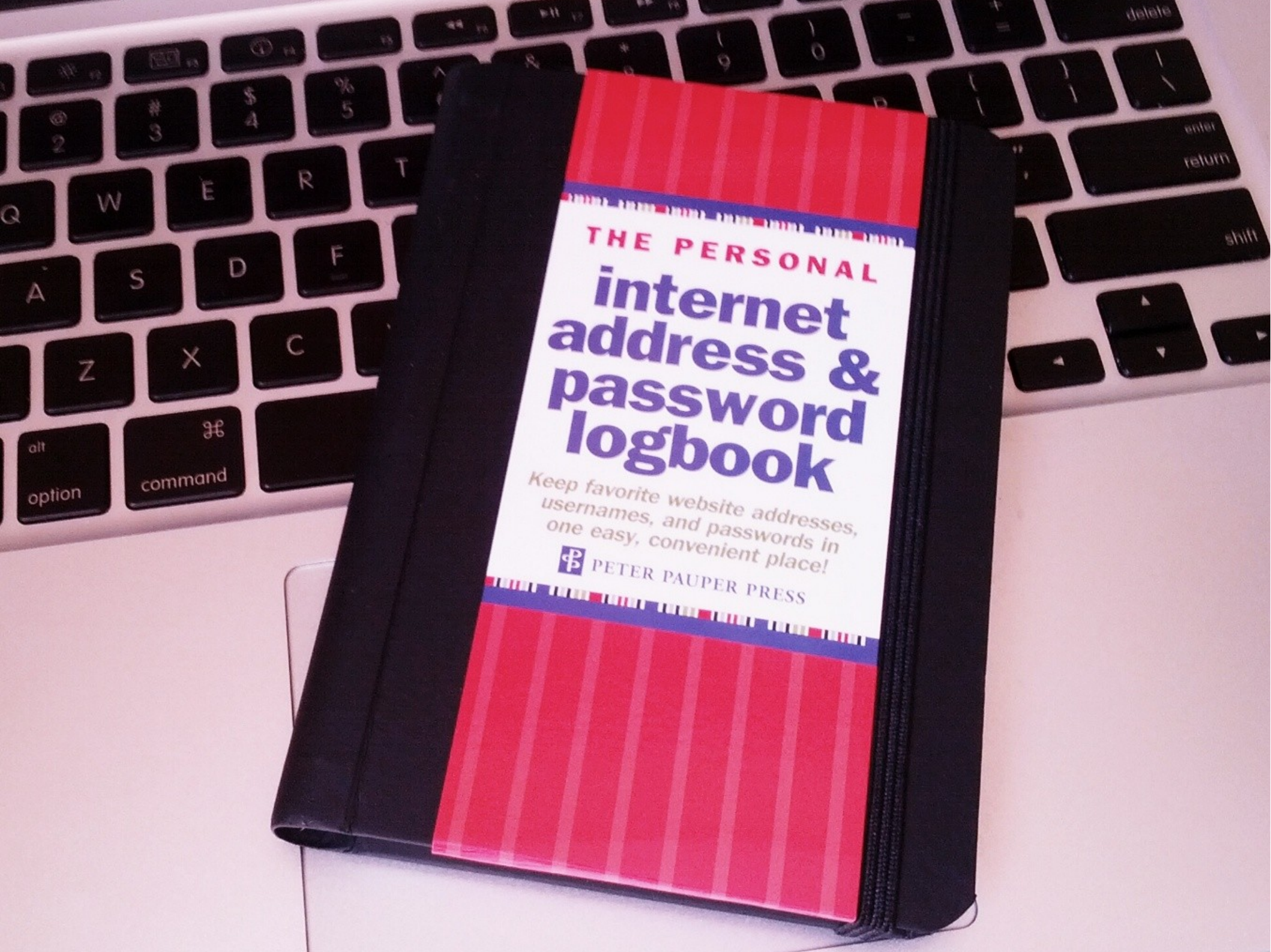
LastPass ****

Passwords and forms

- [ ] Enable Auto-fill to fill in web forms in a single click. Manage Auto-fill settings
- [x] Offer to save passwords I enter on the web. Manage saved passwords

Passwords

- [x] Remember passwords for sites
- [ ] Use a master password


THE PERSONAL
internet address & password logbook
Keep favorite website addresses, usernames, and passwords in one easy, convenient place!
PETER PAUPER PRESS

users have **two** strategies

1. pick an easy password


password
123456
12345678
1234
qwerty
12345
dragon
pussy
baseball
football
letmein
monkey
696969
abc123
mustang
michael
shadow
master
jennifer
111111
2000
jordan
superman
harley
1234567
fuckme
hunter
fuckyou
trustno1
ranger
buster
thomas
tigger
robert
soccer
fuck
batman
test
pass
killer
hockey
george
charlie
andrew
michelle
love
sunshine
jessica
asshole
6969
pepper
daniel
access
123456789
654321
joshua
maggie
starwars
silver
william
dallas
yankees
123123
ashley
666666
hello
amanda
orange
biteme
freedom
computer
sexy
thunder
nicole
ginger
heather
hammer
summer
corvette
taylor
fucker
austin
1111
merlin
matthew
121212
golfer
cheese
princess
martin
chelsea
patrick
richard
diamond
yellow
bigdog
secret
asdfgh
sparky
cowboy
source: xato.net

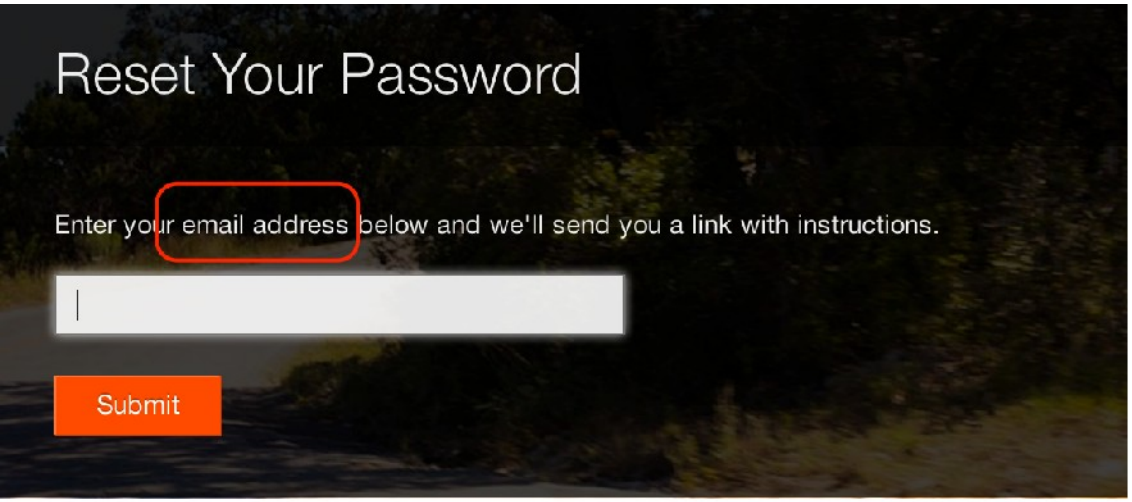
2. reuse your password

negative externality:

sites that don't care about security
impose **a cost on more important sites**

passwords are hard to remember

they need to be **reset**



Lost password

Follow these simple steps to reset your account:

1. Enter your **WordPress.com** username or email address
2. Wait for your recovery details to be sent
3. Follow instructions and be re-united with your **WordPress.com** account

Want more help? We have a full guide to resetting your password.

Forgot password

Email

wtf@lloyd.io

Submit

Username or E-mail:

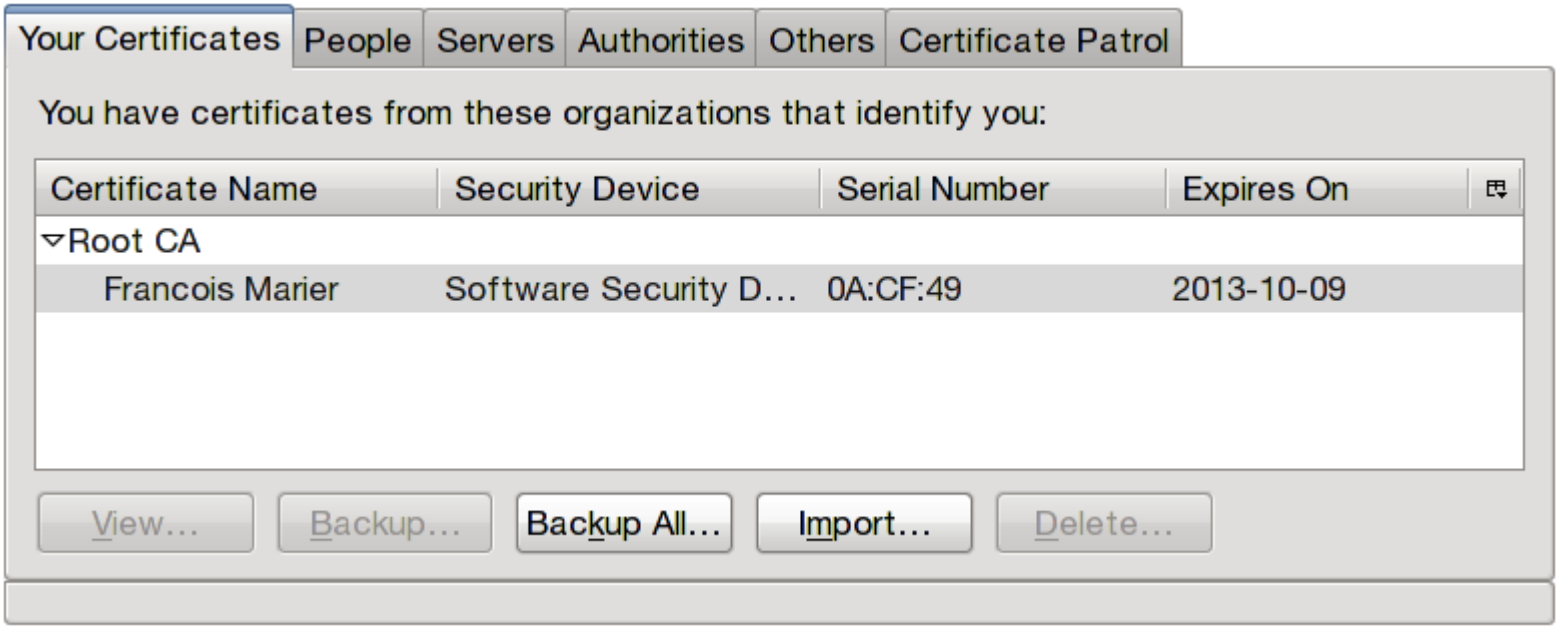
Need More Help?

Get New Password

control email account = control **all** accounts

existing login solutions

client certificates



SAML

facebook®

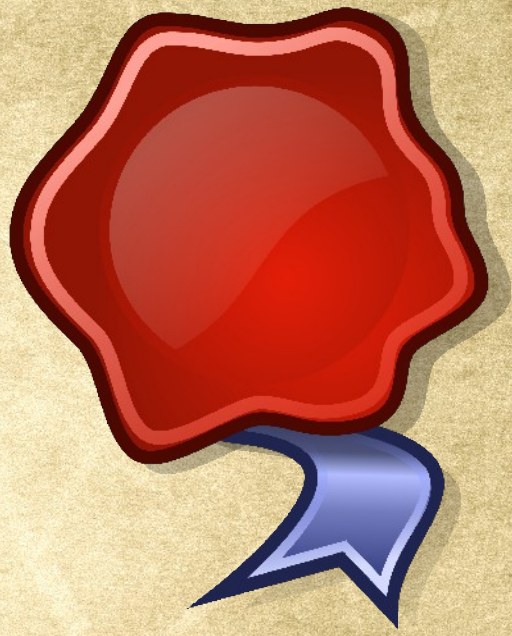

OpenID

existing login systems
are not good enough

mozilla Persona

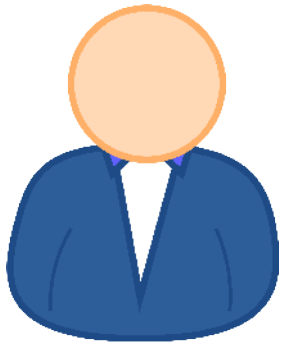
- decentralised
- simple
- cross-browser

how does it work?

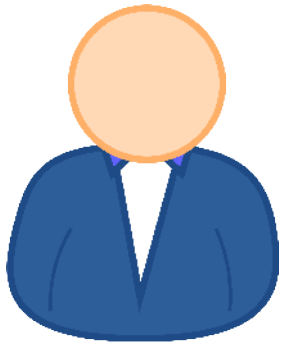


fmarier@gmail.com

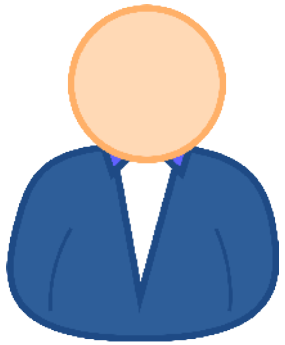
getting a proof of email ownership



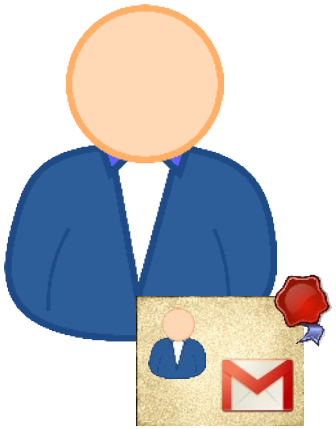
authenticate?



authenticate?



public key

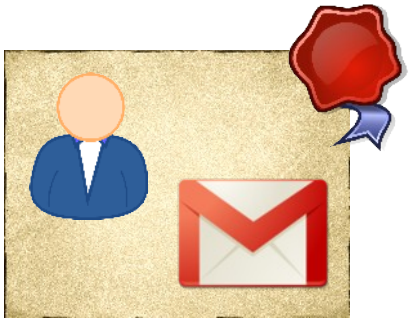


authenticate?

public key

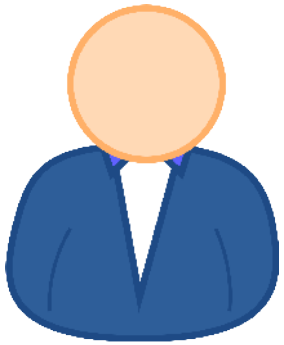
signed public key

you have a **signed statement** from your provider that you **own** your email address

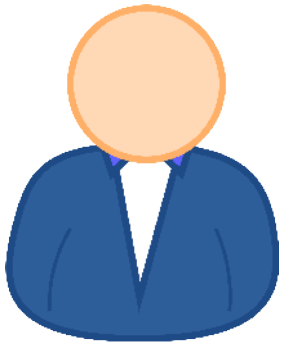



PASSPORT
United States
of America

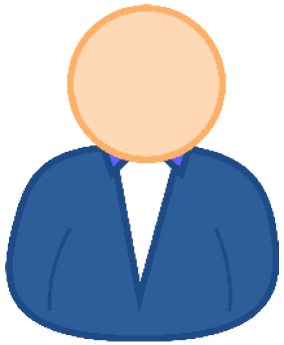
logging into a 3rd party site

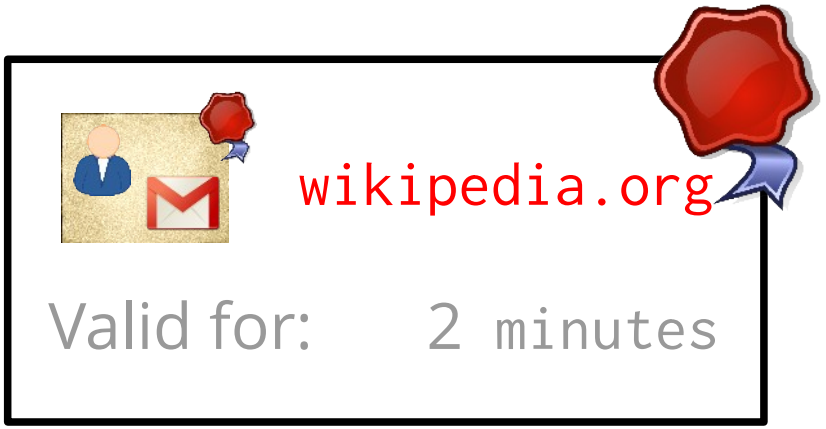


assertion



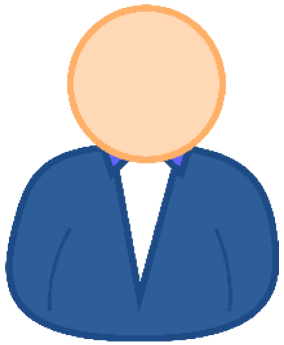
assertion





check audience

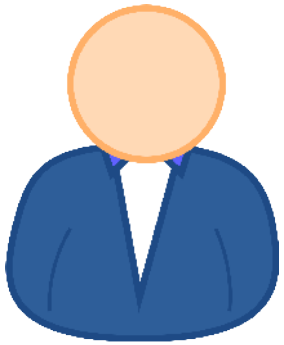
assertion

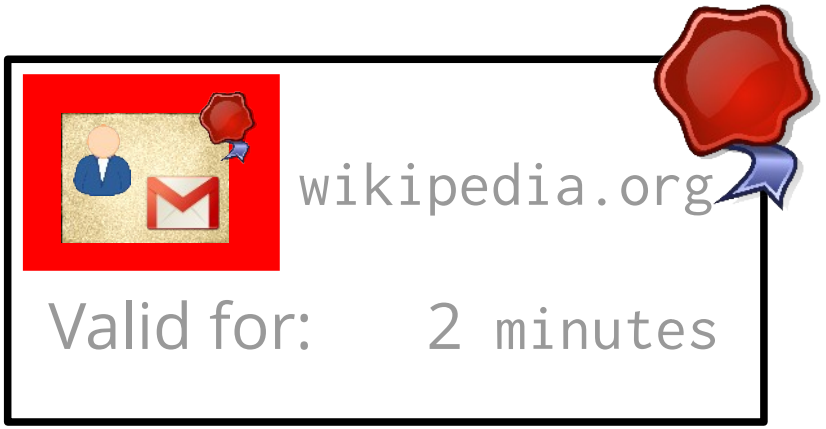


check audience ✓

check expiry

assertion



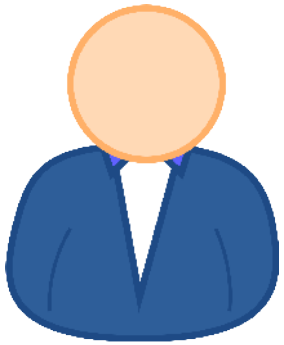


check audience ✓

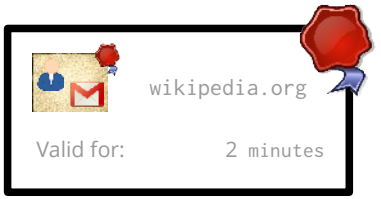
check expiry ✓

check signature

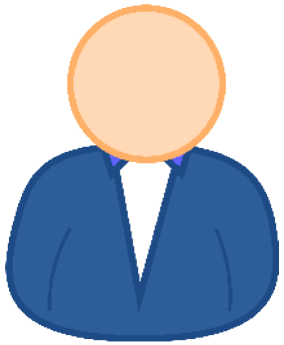
assertion

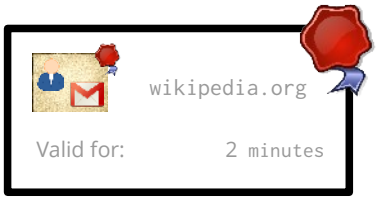


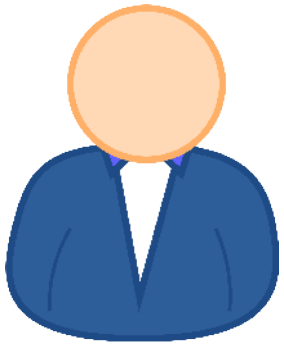
public key



assertion







assertion

session cookie

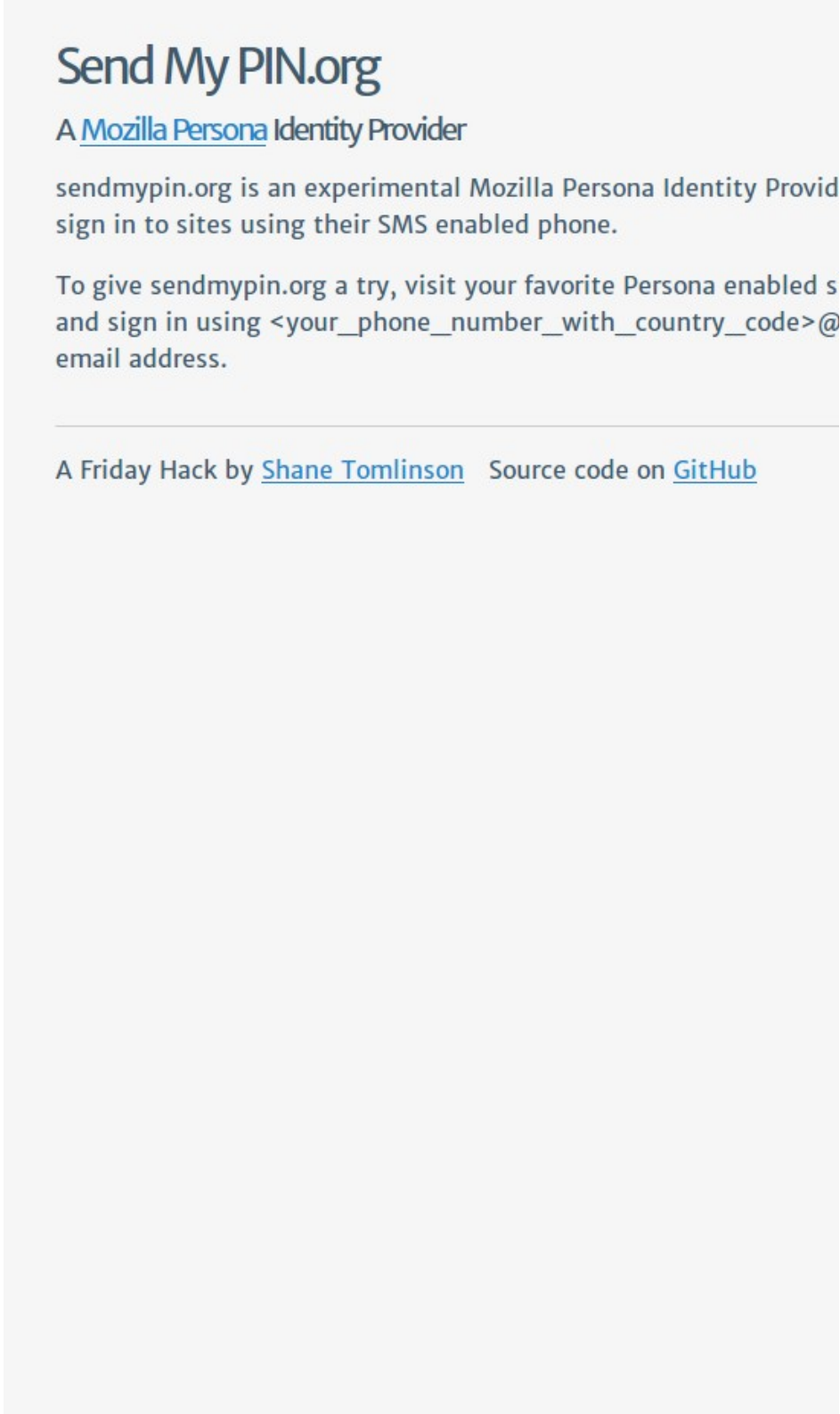
demo #1:

http://crossword.thetimes.co.uk/

fmariertest@eyedee.me

Persona is already a
decentralised system

SMS with PIN codes



SMS with PIN codes

Jabber / XMPP

SMS with PIN codes

Jabber / XMPP

Yubikeys

SMS with PIN codes

Jabber / XMPP

Yubikeys

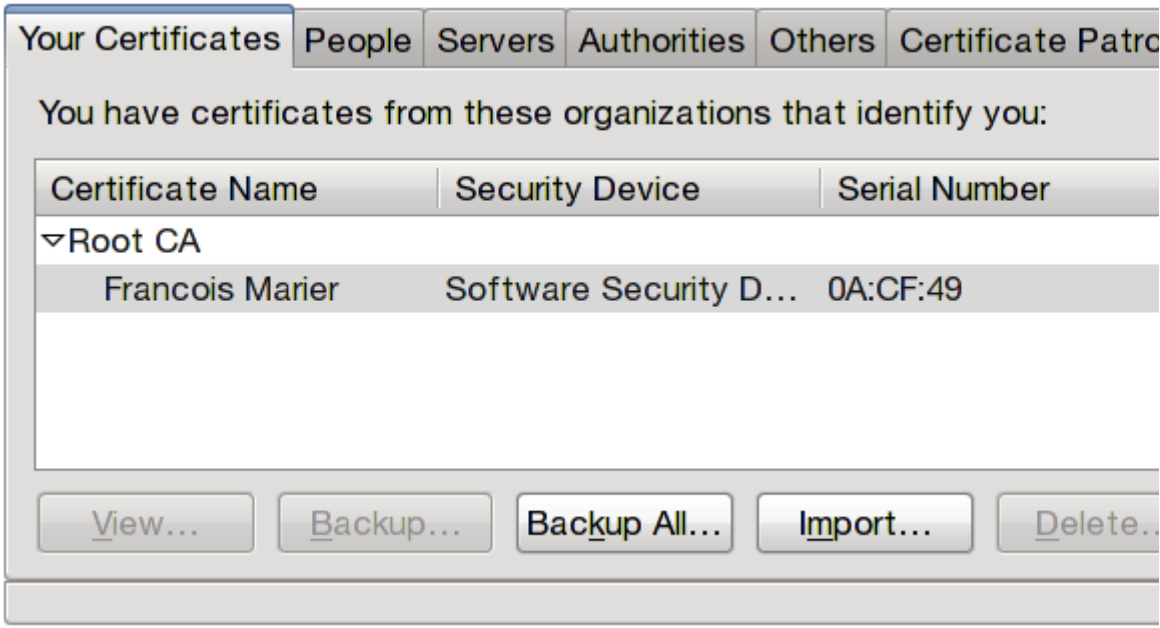
LDAP accounts

SMS with PIN codes

Jabber / XMPP

Yubikeys

LDAP accounts



Client certificates

SMS with PIN codes

Jabber / XMPP

Yubikeys

LDAP accounts

Client certificates

Password-wrapped secret key


```
{
  "public-key": {
    "algorithm":
    "RS",
    "n":"685484565272...",
    "e":"65537"
  },
  "encrypted-private-key": {
    "iv": "tmg7gztUQT...",
    "salt": "JMtGwlF5UWY",
    "ct": "8DdOjD1IA1..."
  },
  "authentication": "...",
  "provisioning": "..."
}
```

decentralisation is the answer, but it's not a **product adoption strategy**

we can't wait for **all domains**
to adopt Persona

we can't wait for **all domains**
to adopt Persona

solution: a temporary
centralised **fallback**

demo #2:

http://sloblog.io/

fmariertest@gmail.com

Persona already works
with **all email domains**

Persona supports
all modern browsers









Persona is decentralised, simple and cross-browser

how can I add Persona support to my domain?

support document

`https://eyedee.me/.well-known/browserid`

https://eyedee.me/.well-known/browserid:

```
{
  "public-key": {
    "algorithm":"RS",
    "n":"8606...",
    "e":"65537"
  },
  "authentication": "/browserid/sign_in.html",
  "provisioning": "/browserid/provision.html"
}
```

https://eyedee.me/.well-known/browserid:

```
{
  "public-key": {
    "algorithm":"RS",
    "n":"8606...",
    "e":"65537"
  },
  "authentication": "/browserid/sign_in.html",
  "provisioning": "/browserid/provision.html"
}
```

https://eyedee.me/.well-known/browserid:

```
{
  "public-key": {
    "algorithm":"RS",
    "n":"8606...",
    "e":"65537"
  },
  "authentication": "/browserid/sign_in.html",
  "provisioning": "/browserid/provision.html"
}
```

https://eyedee.me/.well-known/browserid:

```
{
  "public-key": {
    "algorithm":"RS",
    "n":"8606...",
    "e":"65537"
  },
  "authentication": "/browserid/sign_in.html",
  "provisioning": "/browserid/provision.html"
}
```

identity provider API

1. check for your `/.well-known/browserid`

identity provider API

1. check for your `/.well-known/browserid`
2. try the provisioning endpoint

identity provider API

1. check for your `/.well-known/browserid`
2. try the provisioning endpoint
3. show the authentication page

identity provider API

1. check for your `/.well-known/browserid`
2. try the provisioning endpoint
3. show the authentication page
4. call the provisioning endpoint again

as an organization, you control:

- details of the **authentication process**

as an organization, you control:

- details of the **authentication process**
- the **duration** of certificates

To learn more about Persona:

https://login.persona.org/
http://identity.mozilla.com/

https://developer.mozilla.org/docs/Persona/Quick_Setup
https://developer.mozilla.org/Persona/Implementing_a_Persona_IdP

https://github.com/mozilla/browserid-cookbook
https://developer.mozilla.org/docs/Persona/Libraries_and_plugins

https://wiki.mozilla.org/Identity#Get_Involved

Photo credits:

Door man: https://secure.flickr.com/photos/wildlife_encounters/8024166802/

Top 500 passwords: http://xato.net/passwords/more-top-worst-passwords/

Parchment: https://secure.flickr.com/photos/27613359@N03/6750396225/

Cookie on tray: https://secure.flickr.com/photos/jamisonjudd/4810986199/

Uncle Sam: https://secure.flickr.com/photos/donkeyhotey/5666065982/

US passport: https://secure.flickr.com/photos/damian613/5077609023/

Stop sign: https://secure.flickr.com/photos/artbystevejohnson/6673406227/