How can DomainID help this guy to remember his password (and keep ISPs relevant)

Vittorio Bertola
Research & Innovation Engineer, Open-Xchange

DNSSEC Workshop, ICANN 60, Abu Dhabi, November 1, 2017
The problem

We have too many different user accounts.

(And we can’t even use the same password for all of them)
The solution

Single sign-on (SSO)

= A single username and password couple that can be used on all existing online services

Requires an online service acting as user authentication provider (must be trusted by everyone)
Existing global SSO systems, #1

Official government-provided digital identity (e.g. eIDAS)

**Problems:**

- Usually hard to get and use
- Lack of privacy
- Overkill for most applications (scarce support)
Existing global SSO systems, #2

OTT-provided digital identity (e.g. social networks)

Problems:
- Owned & branded by the OTT
- No privacy guarantee
- No portability and choice for the user
The real solution

Feels like “Login with Facebook”, but
- public
- open and federated
- based on standards
- full control on data privacy
- could be extended to other applications
OpenID Connect plus…

1. A better discovery process, enabling the use of any hostname as identifier
2. Support of all identity providers with a single entry point
3. Identifier portability (if you own the domain)
4. Separation of roles between authorization (“identity authority”) and user data management (“identity agent”)
5. Management of user consent for sharing data
6. Many more information fields (“claims”) about the user

7. How can DomainID help this guy to remember his password
How do I get a DomainID identifier?

You do this only once

Any valid DNS hostname (in a domain you can access) can be your DomainID identifier, e.g. “user.open-xchange.net”

1. Acquire service
2. Register domain name
3. Set up DNS records
4. Register identifier
5. Verify DNS records
6. Confirm identifier
7. Provide identifier
8. Activate and set password

How can DomainID help this guy to remember his password?
How do I use a DomainID identifier?
Just two user screens (and the second one is optional)

1. Provide identifier
2. Discover authority and agent
3. Request login
4. Enter password (or be recognized by cookie)
5. Login OK
6. Request user data
7. Send user data
8. Login completed

User

Identity authority

DNS

Identity agent

Relying party (any online service)

How can DomainID help this guy to remember his password?
User advantage #1

Pick your online brand

- No more “me@gmail.com”
- Can be in the domain name of any provider
- Or it can be in your own personal domain name
User advantage #2

Pick your provider

- You can pick and change your provider (as long as you own the domain)
- Or you can host it yourself
- Choose who to trust with your data!
User advantage #3

Easier and more secure

- You only need to remember one strong password
- You only share it with one trusted partner
- And if it’s not trusted any more, you just change password and partner
User advantage #4

Easier and more private

- You can have multiple identities
- You can automatically create new accounts
- You choose how much information to share with each website
What’s in it for the domain people?

- Provide a crucial value-added service to customers
- Manage their customers’ online identity
- Sell more personal domain names
- Promote DNS & DNSSEC

© CC-BY-ND 3.0 felixart05
Stay Open.
Strategic value: very high

- Lack of proper, user-controlled authentication and identity management is at the root of many abuse, security and usability issues.

- DNS (with DNSSEC) should continue to be the Internet’s public directory, also for people and their services.

- Identity tracking is the cornerstone for OTT-run walled gardens.

- There is no public, open, federated, privacy-friendly, user-centered identity management standard for everyone else – and this is what we want to build.