The DNS as a directory for identities

ICANN DNS Symposium 2018, Montreal

Vittorio Bertola <vittorio.bertola@open-xchange.com>

Premise: We need proper online identities

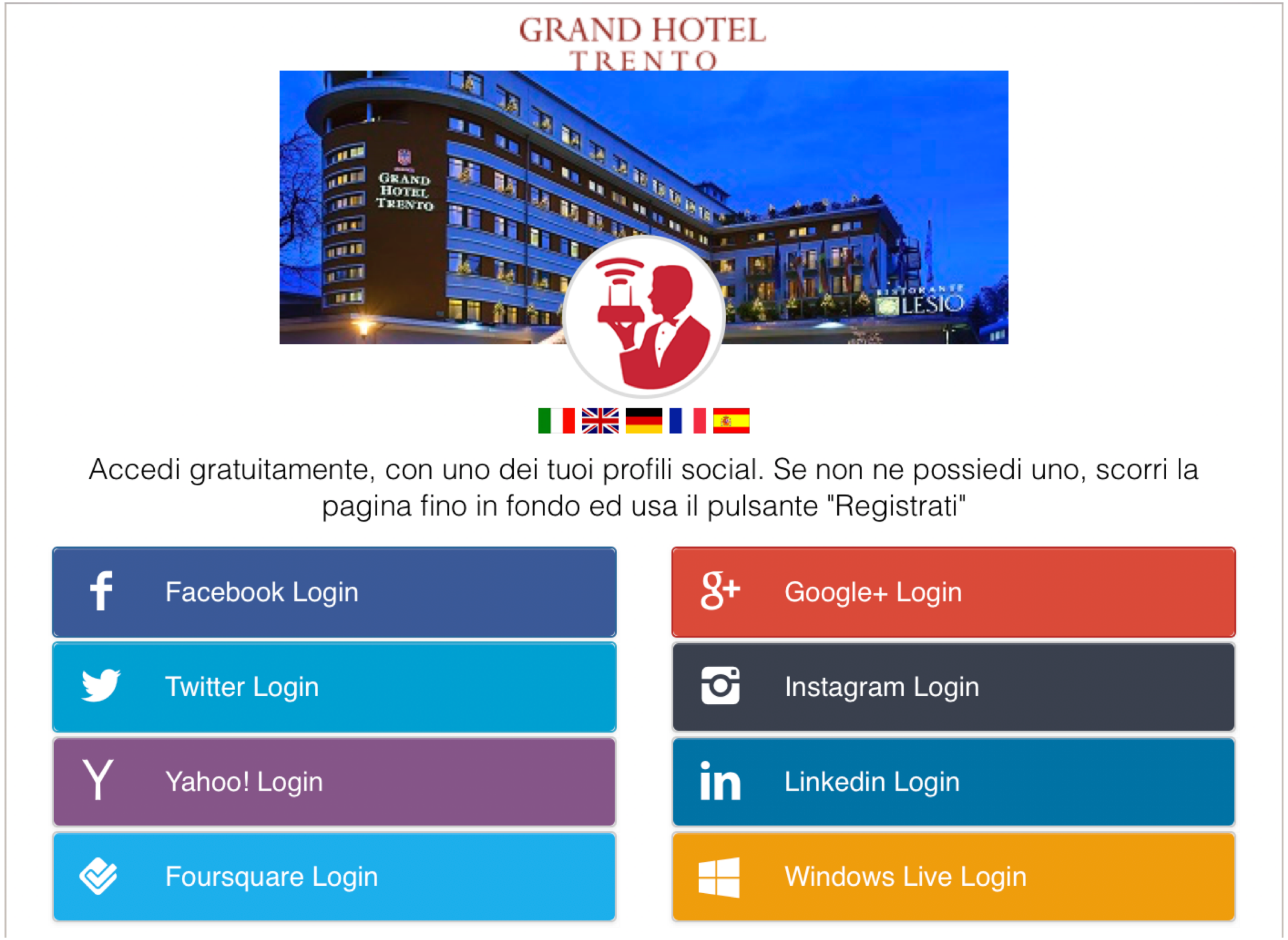
- Traditionally, we only had accounts
    - And they were not connected to each other, though they often had the same information in them
- Until some companies realized that tracking users across multiple accounts created a lot of value
    - Targeted advertising, user profiling etc.
- We already have online identities, but they are not under our control
    - We only have accounts, but others have our identity (and monetize it)

Online credentials for the average user

- Most people just reuse usernames and passwords across hundreds of websites and services
  - Usability issues
  - Security issues

- Single-sign-on systems in private namespaces gaining ground
  - Users like them, but:
  - Fragmentation, lack of interoperability
  - Clients have to implement each of them separately
  - Users cannot choose their provider

A wi-fi login form from the real world



Accedi gratuitamente, con uno dei tuoi profili social. Se non ne possiedi uno, scorri la pagina fino in fondo ed usa il pulsante "Registrati"

Advantages of public, federated SSO

- Why can’t your online identity work like your email address?
- You only need one account to interoperate with everyone
- You get to choose and even to change your provider
    - You can keep your identifier if it is in your own domain name
- You only need to remember and secure one set of credentials
- Any additional security mechanisms can be implemented just once by a specialized party (not by any website operator)
- You have an easy way to control the sharing of your information and to keep it updated (a legal requirement in many countries)
- You don’t need to register for new websites, just identify yourself

Ok, great idea! But what do we need?

- We already have federated identity management and authorization protocols
    - OpenID Connect / Oauth 2.0
    - Though not normally deployed in a truly federated way (at most, used for a federation with a single identity provider)

- We miss a place to keep the directory of all existing identities, and a protocol for looking identities up into it

The Web people do it on the Web

- OpenID Connect already has an optional discovery mechanism
  - It is based on WebFinger, which is based on HTTPS
  - Only accepts URIs as identifiers, with email addresses as a special case

- Requires you to deploy a web server and a WebPKI certificate on each and every domain that you want to use for identifiers
  - Even if it is a domain not used for the Web
  - Even if it is a domain not used at all, except as a reserved string
  - Even if you still need a DNS query before making an HTTPS connection

    (that is, until the Web people finally succeed in replacing DNS queries with HTTPS requests)

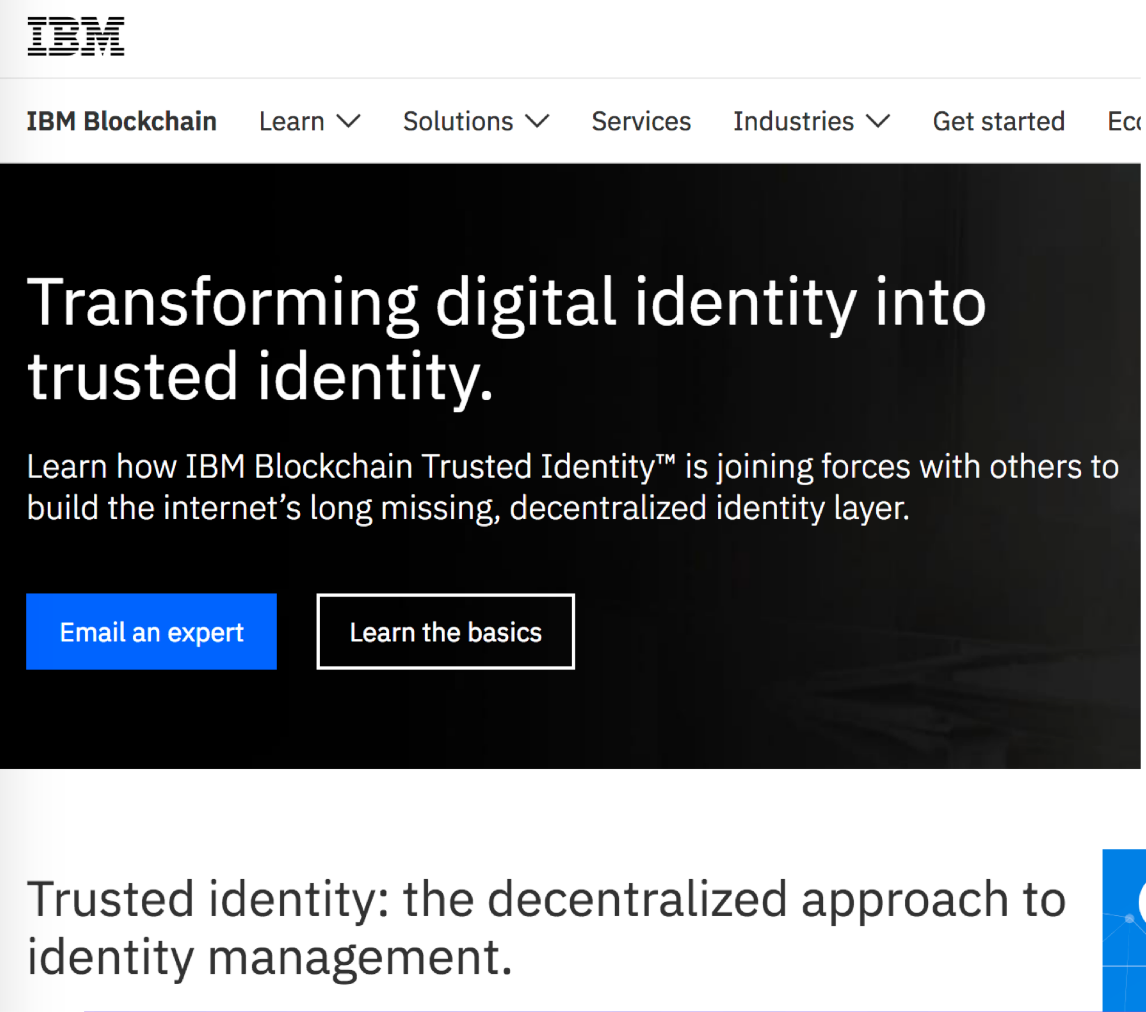
Hey, but the Web is so uncool now

- Why don’t we use a blockchain?

- Join the revolution!

- Don’t you want to be self-sovereign?

- Here, buy these tokens from my ICO!



IBM

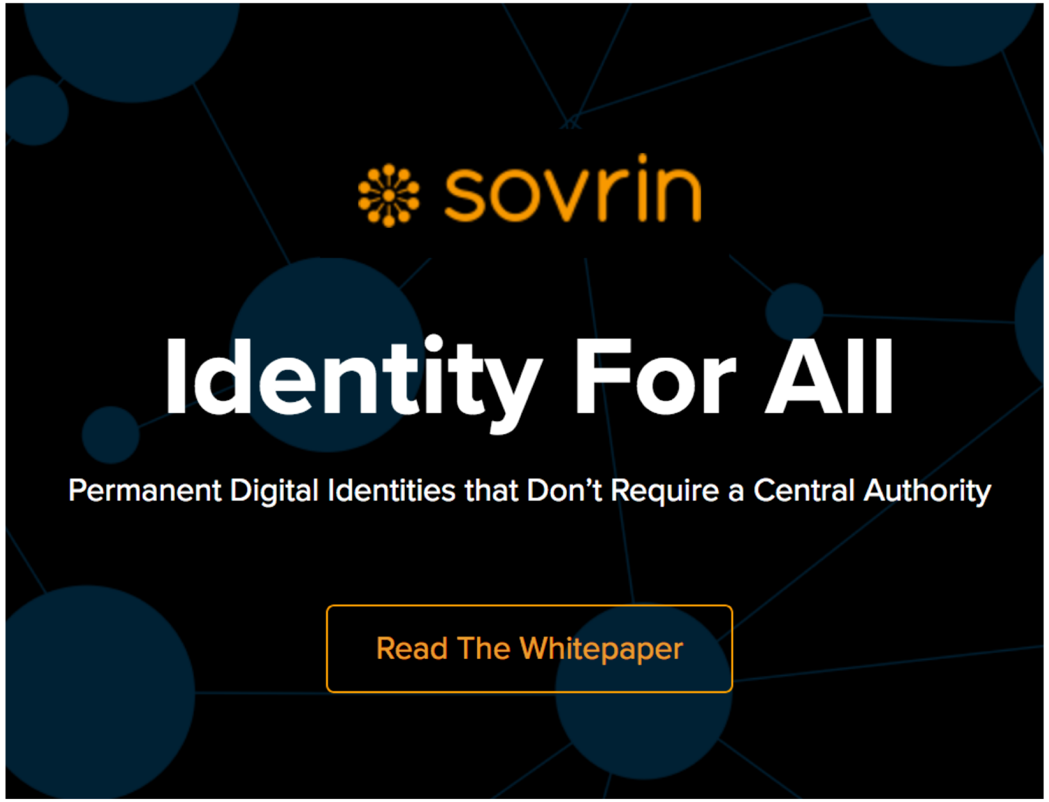
IBM Blockchain | Learn ⌄ | Solutions ⌄ | Services | Industries ⌄ | Get started | Ec

Transforming digital identity into trusted identity.

Learn how IBM Blockchain Trusted Identity™ is joining forces with others to build the internet's long missing, decentralized identity layer.

Email an expert | Learn the basics

Trusted identity: the decentralized approach to identity management.

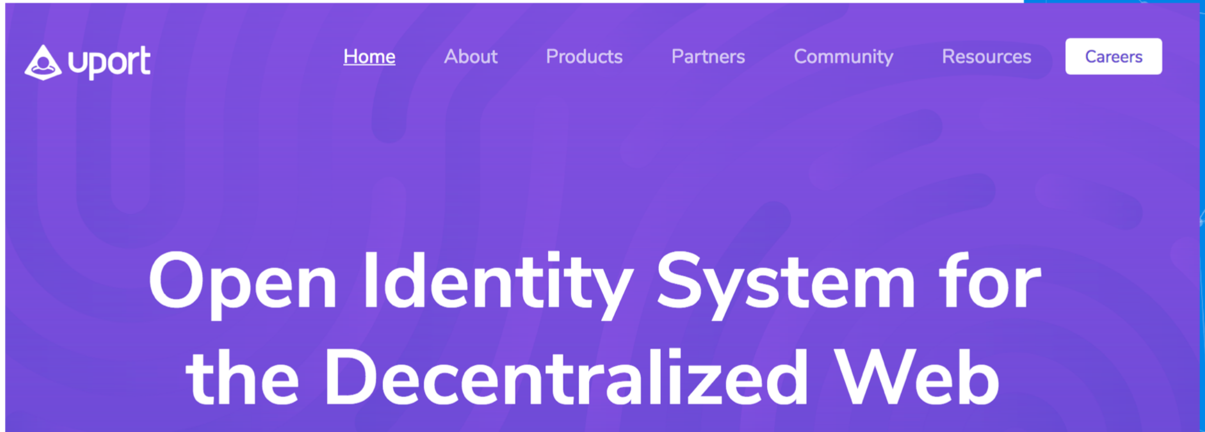


sovrin

Identity For All

Permanent Digital Identities that Don't Require a Central Authority

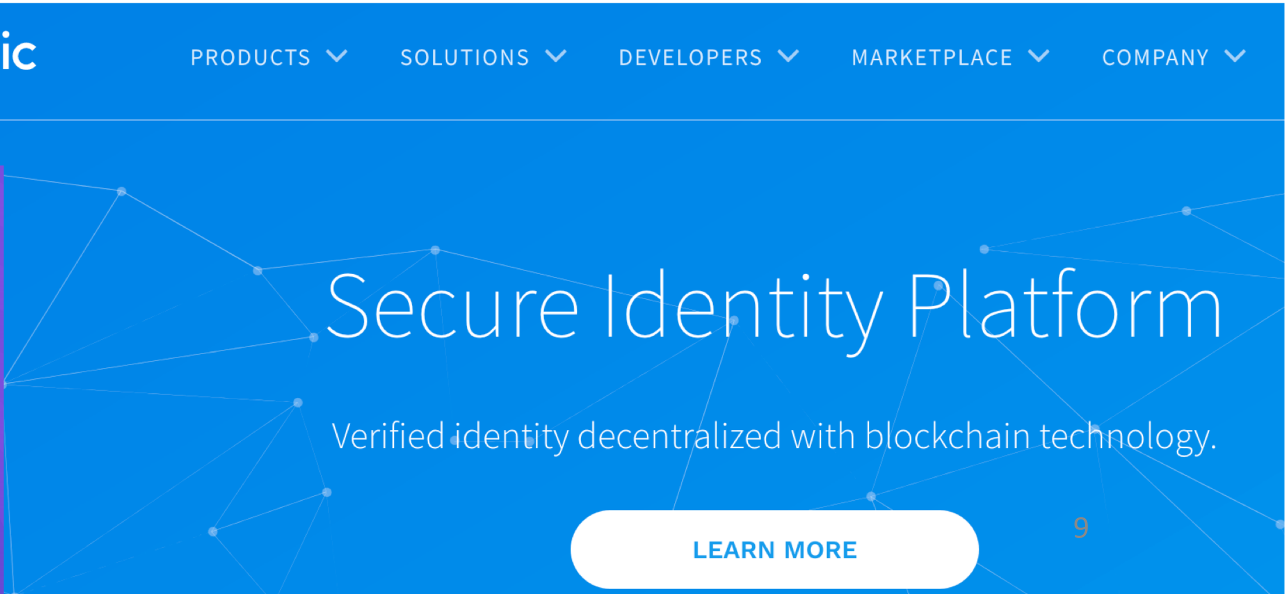
Read The Whitepaper



uport

Home | About | Products | Partners | Community | Resources | Careers

Open Identity System for the Decentralized Web



civic

PRODUCTS ⌄ | SOLUTIONS ⌄ | DEVELOPERS ⌄ | MARKETPLACE ⌄ | COMPANY ⌄

Secure Identity Platform

Verified identity decentralized with blockchain technology.

LEARN MORE

The blockchain people do it on the blockchain

- Identities, or at least pointers, or at least hashes, are written into the blockchain
  - The rest is often unclear, or proprietary, or vaporware, or all together

  A survey by a potential customer found 91 blockchain ID projects, 63 of which were having an ICO, but only 17 of them had a non-placeholder website, only 3 had downloadable software, and only 0 had working software.
  (source: European Identity Conference 2018)

- The selling point is that this is «decentralized»
  - Down with «central authorities»! No government, no ICANN can get in your way!

- Unofficial standardization ongoing at the W3C on a «DID» URI scheme

Wait a minute…

- We already have a «public distributed ledger»
- It is an open, public standard with many free implementations
- It is widely available to everyone everywhere
- It has been working reliably for 30+ years
- It is secure (with DNSSEC)
- It can scale effectively to support almost any amount of traffic
- It is decentralized and federated
- It’s the DNS!

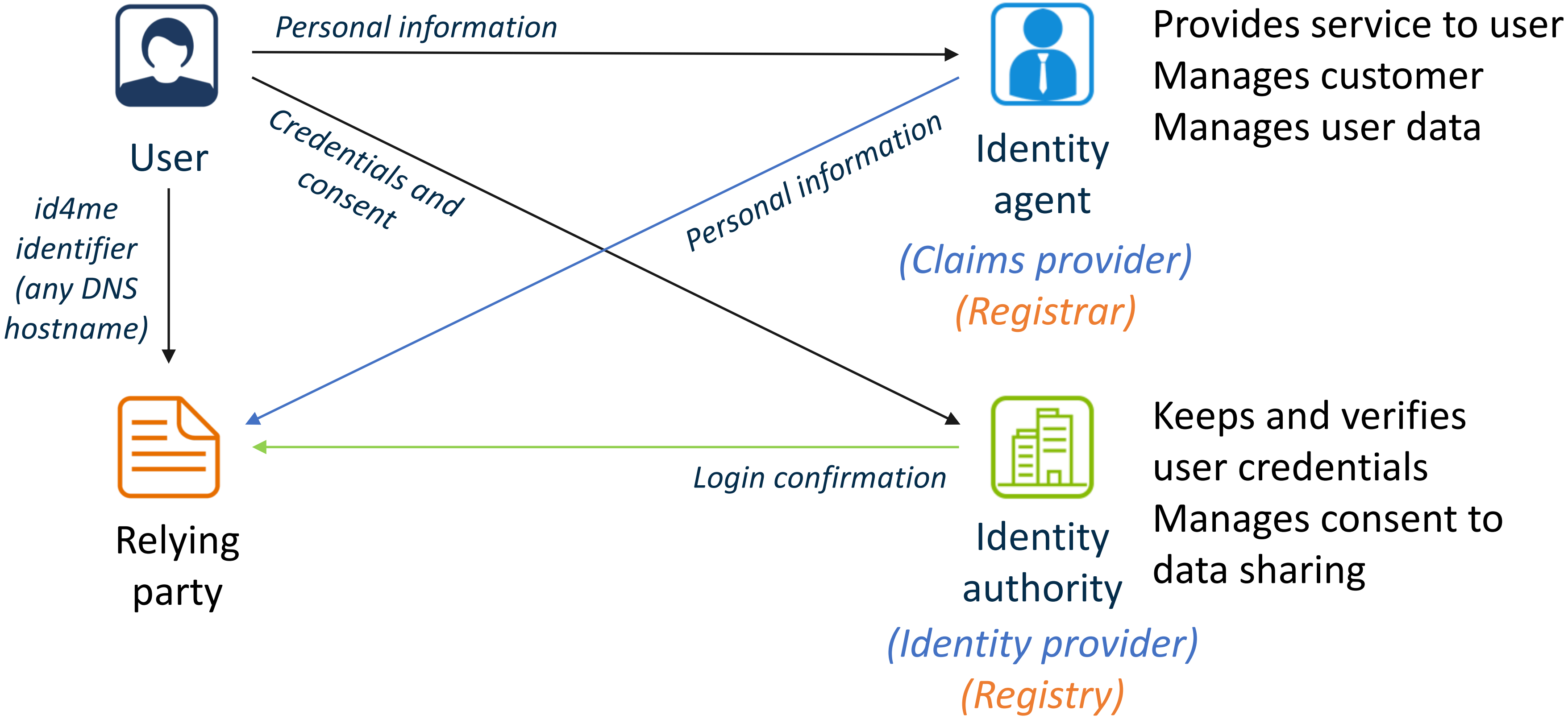
The DNS provides the namespace

- In the real world, people use «natural» names which are neither unique nor uniform nor easily parsable
- So you need a namespace to name identities uniquely on a global scale, while distributing its management… but it’s the same problem that was already solved for host names 35 years ago
- Using the DNS, you can assign human-readable identifiers to identities in a naturally federated namespace
- Users are already familiar with DNS-based strings
- You can even use email addresses if you wish
- Or you can encourage people to get their personal domain name and own a piece of the namespace

The DNS provides the discovery mechanism

- We just need a pointer to know who is responsible for an identifier
- Again, same problem already solved for email 35 years ago
- We use a TXT record, rather than a new RRtype, and we all know why
- So we are not adding straw onto the camel’s back
- Two Internet drafts independently submitted
    - Looking for the right place to make them a standard
    - Could be the IETF, could be the OpenID Foundation

The roles in ID4me



User

Personal information

Credentials and consent

id4me identifier (any DNS hostname)

Identity agent

Provides service to user
Manages customer
Manages user data

(Claims provider)

(Registrar)

Personal information

Relying party

Login confirmation

Identity authority

Keeps and verifies user credentials
Manages consent to data sharing

(Identity provider)

(Registry)

The DNS record for identity discovery

_openid.<identifier>

TXT

v=OID1;iss=<issuer>;clp=<claims_provider>

Project status

- A joint project by several companies (public name “ID4me”)
- Website, public specifications, Java API released (https://id4me.org/)
- A prototype up and running, with new features being added
- An international association in formation
- Outreach ongoing throughout the domain name industry
  - Interest by TLD registries willing to become identity authorities
  - Interest by domain name registrars willing to become identity agents
  - Interest by telcos / ISPs willing to supply identities to their users
- Looking for feedback and participation

Conclusions

- Let’s defend the role of the DNS as the true public and distributed database of the Internet
- Let’s keep the DNS relevant by adding more content types into it (rather than more protocol features)
- Comments welcome!

Thank you

vittorio.bertola@open-xchange.com

https://id4me.org/