Celebrating Ten Years of OpenID Connect

Michael B. Jones

Self-Issued Consulting

Looking Back and Looking Forward

- OpenID Connect became final in February 2014

- Today I’ll briefly share my thoughts on
  - How we created OpenID Connect
  - What we achieved together
  - Lessons learned

In the Beginning

- Artifact Binding for OpenID 2.0 started in 2010
  - Hence the openid-specs-ab@lists.openid.net mailing list name
- But developers were choosing JSON/REST over XML/SOAP
- Pivoted to instead create JSON/REST protocol over OAuth 2.0
- Result branded “OpenID Connect” at IIW in May 2011
- Five rounds of interop testing between 2011 and 2013!
  - Specifications refined after each round of interop testing
- Early developer feedback was priceless

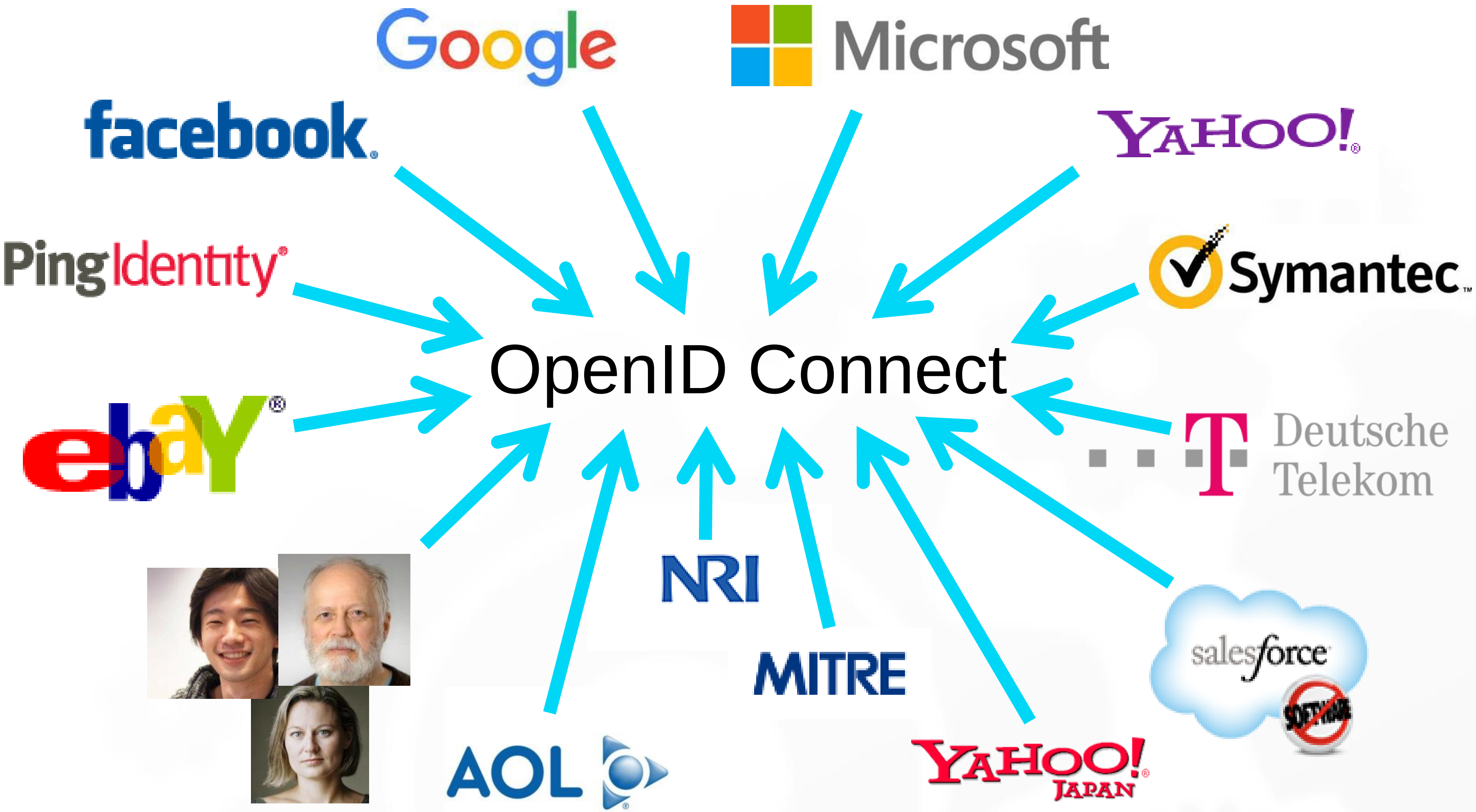
Design Philosophy

- Keep simple things simple
- Make complex things possible

The Nov Matake Test

- As we considered new features, we'd ask ourselves:
  - Would Nov want to add it to his implementation?
  - Is it simple enough that he could build it in a few hours?

Broad Participation



OpenID Connect

Learning from the Past

- Architects had extensive SAML and OpenID 2.0 experience
- Borrowed ideas that already worked well
  - Metadata
  - Authentication Contexts
- Added useful things that were previously hard or missing
  - Support for native applications
  - Encrypted claims
  - Signed requests

Extensible by Design

- Successful systems have to adapt and grow
- Always specified that “additional values may be used”
  - And specified that not-understood values don’t cause errors
  - Enables adding things without breaking existing deployments

- Indeed, many successful Connect (and OAuth) extensions have been created and deployed
  - Including logout and identity assurance

Built using Modular Components

- Created components and features we needed in parallel
  - JSON Web Signature (JWS)
  - JSON Web Encryption (JWE)
  - JSON Web Key (JWK)
  - JSON Web Token (JWT)
  - WebFinger
  - ID Token

What We Achieved

- Most used identity protocol
- Thousands of interoperable implementations
  - In every conceivable language
- Certification Program making interop a reality
- ISO accepted our submission for republication

Innumerable OpenID Connect Deployments

- Android, AOL, Apple, AT&T, Auth0, Deutsche Telekom, ForgeRock, Google, GrabTaxi, GSMA Mobile Connect, IBM, KDDI, Microsoft, NEC, NRI, NTT, Okta, Oracle, Orange, Ping Identity, Red Hat, Salesforce, Softbank, Symantec, Telefónica, Verizon, Yahoo, Yahoo! Japan, all use OpenID Connect
- And many MANY more!

Lessons Learned

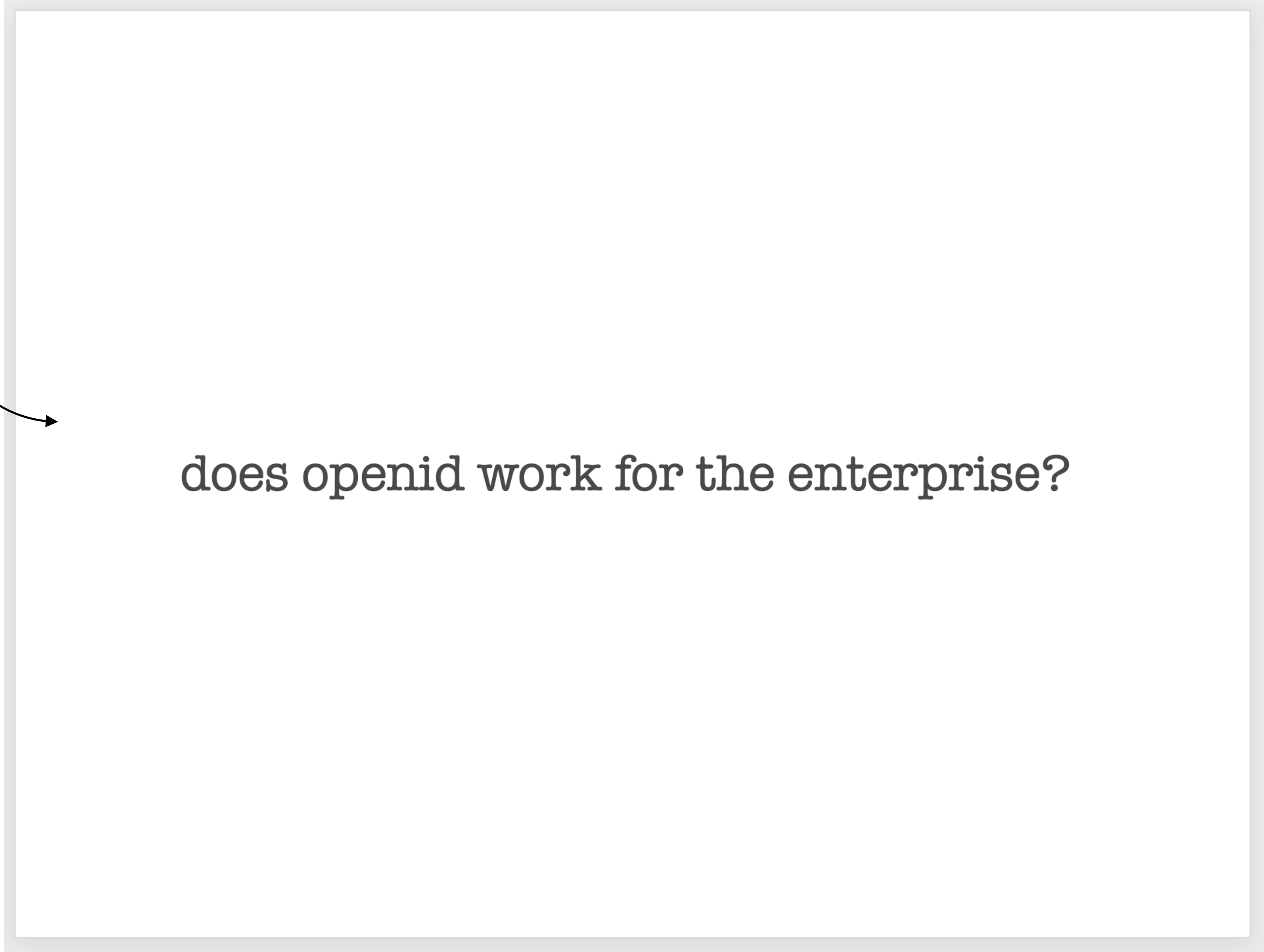
- Developers choose things that are simple
  - Developer choice critical to adoption
- Interoperability and security require rigorous testing
  - OpenID Certification program was essential to Connect's success
- Extensibility is critical to long-term success
- Deployments have to be easy to use (or they won't be used)
  - Most RPs limited IdP choice as a simplification
    - Even though Connect was designed to give users complete choice
- Not everything works out the way you planned
- Developer and deployer feedback is gold!

OpenID and the Enterprise

Chuck Mortimore

Disney (Salesforce at the time)

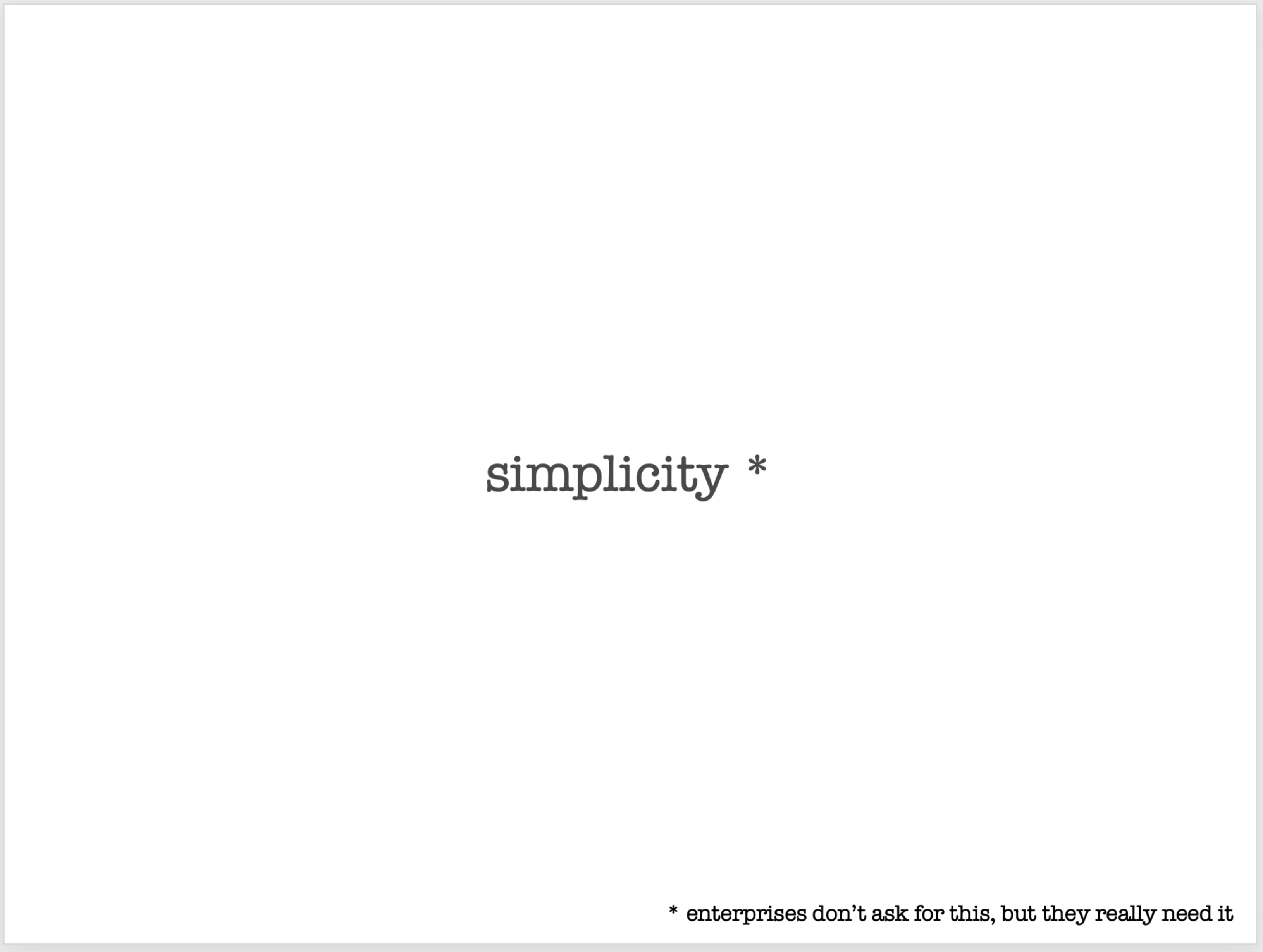
Cloud Identity Summit 2011



does openid work for the enterprise?

no*

*not in current form



simplicity *

* enterprises don’t ask for this, but they really need it

What I think I was saying:

- Canonicalization is hard regardless of serialization
- We are unwilling to implement WS-* and need an objection handler.

What actually happened:

- Simplicity won: WS-* was replaced*
- We created the Basic Implementors draft

*and almost all of the same patterns exist in our current standards stack oauth based for data services

What I think I was saying:

Enterprises are adopting iPhones and we’re not ready

- We need fine grained control over app and data access
- We need to federate with mobile apps

What actually happened:

- Application frameworks for contextual policy
- Embedded WebView in mobile apps == reuse of web federation

artifact profiles

What I think I was saying:

- The firewall is moving around and loosing importance
- Core services, including identity, will move to the cloud

What actually happened:

Artifact profiles that actually scale

SSO get tokens

Applications become composites

claims-centric

What I think I was saying:

- Cloud adoption is just-in-time for certain users/companies
- SAML JIT works but integration heavy
- I miss LDAP and it’s standard yet extensible schema

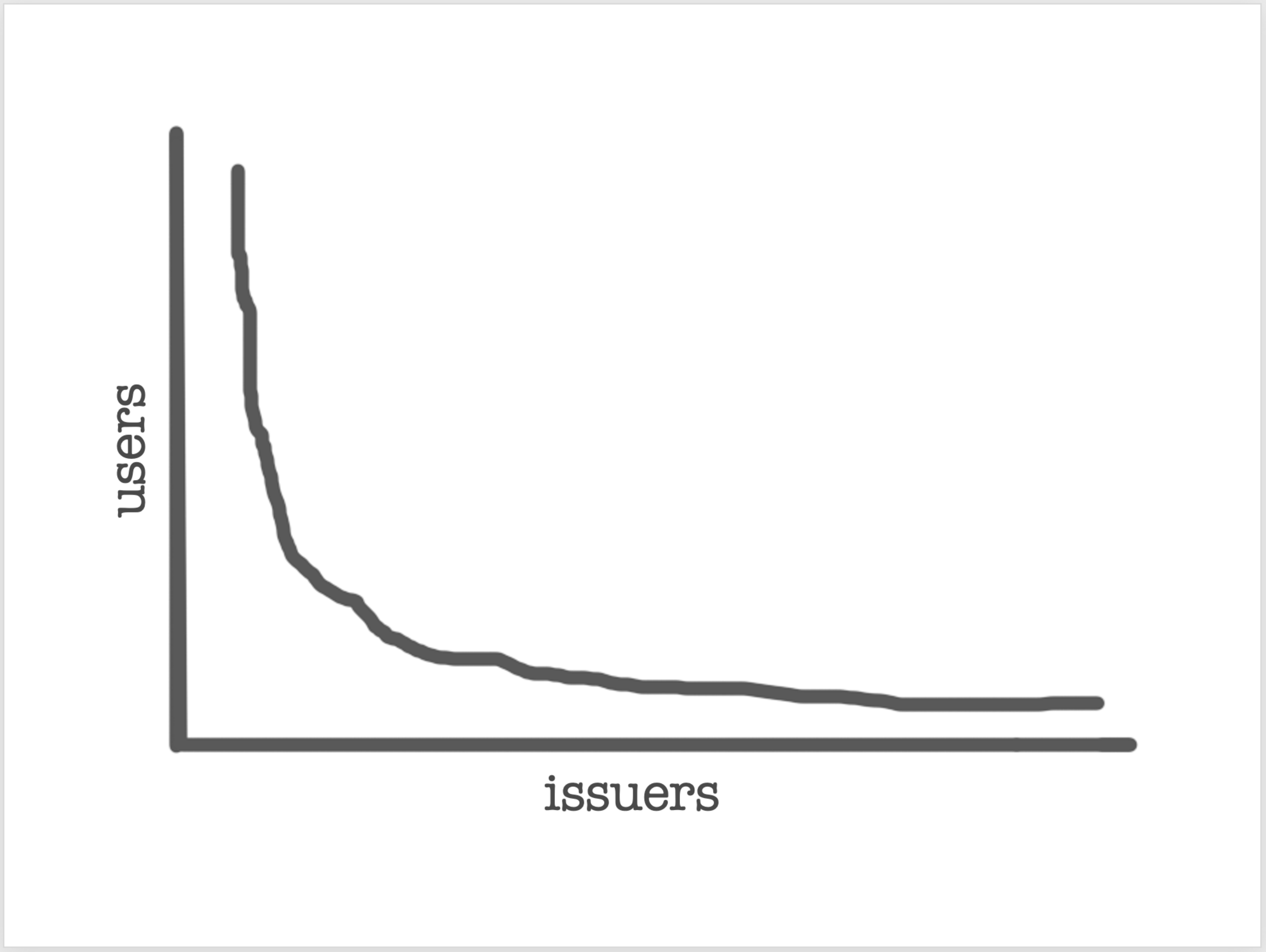
What actually happened:

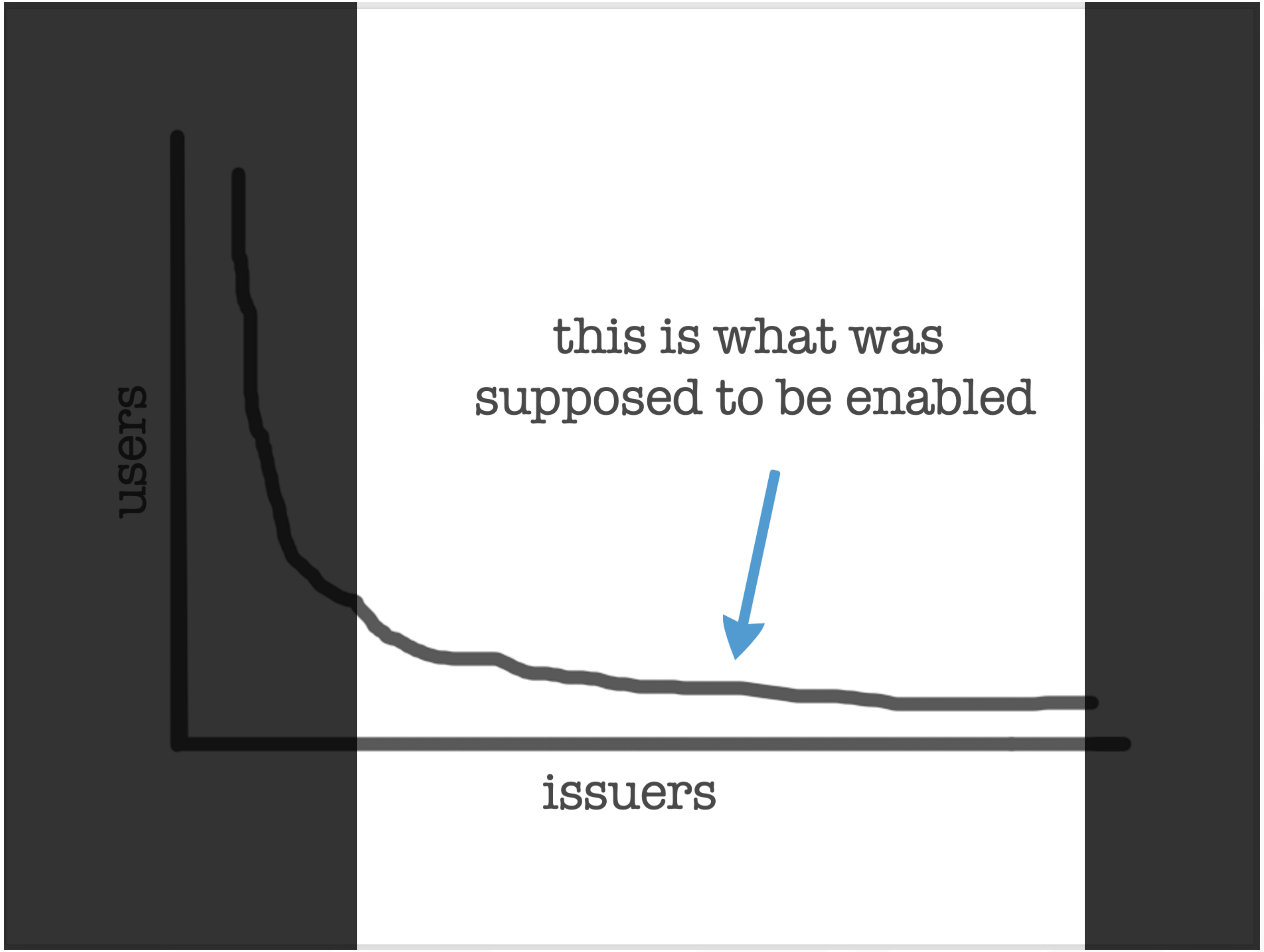
- Standardized schema
- SCIM

user’s don’t identify with URLs

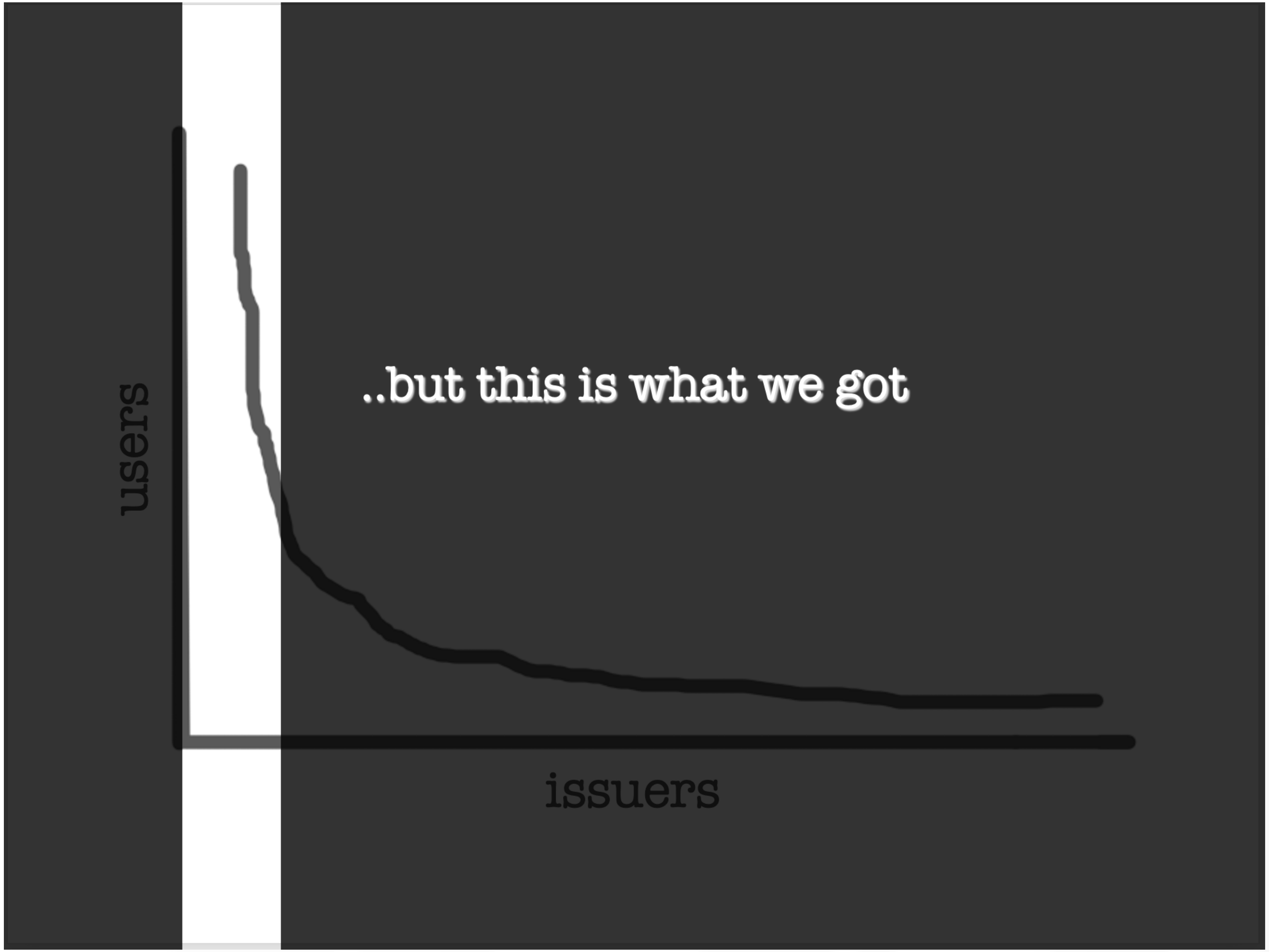
consumer trust ≈ brand

rp’s economics favor op’s of scale

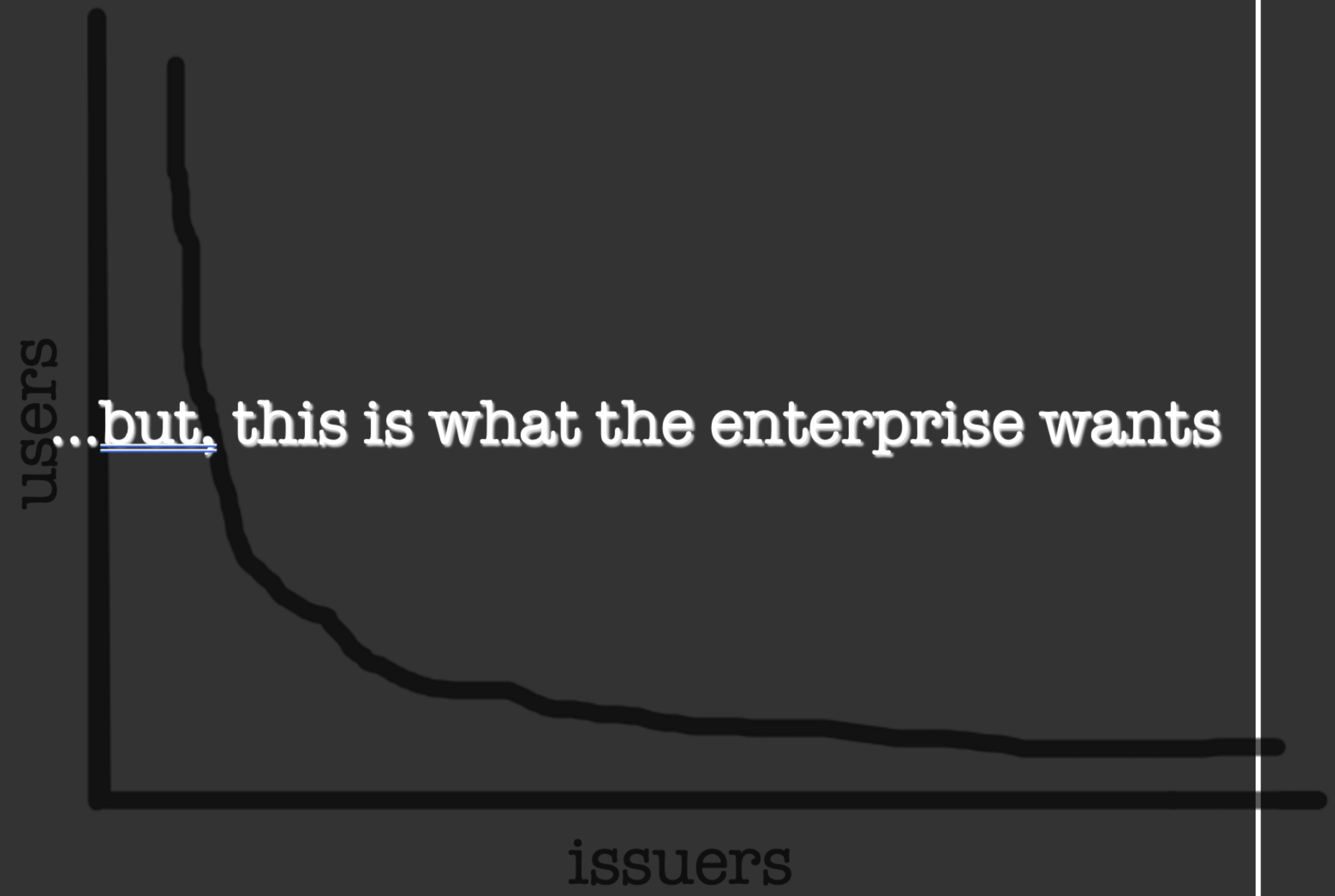

users
issuers



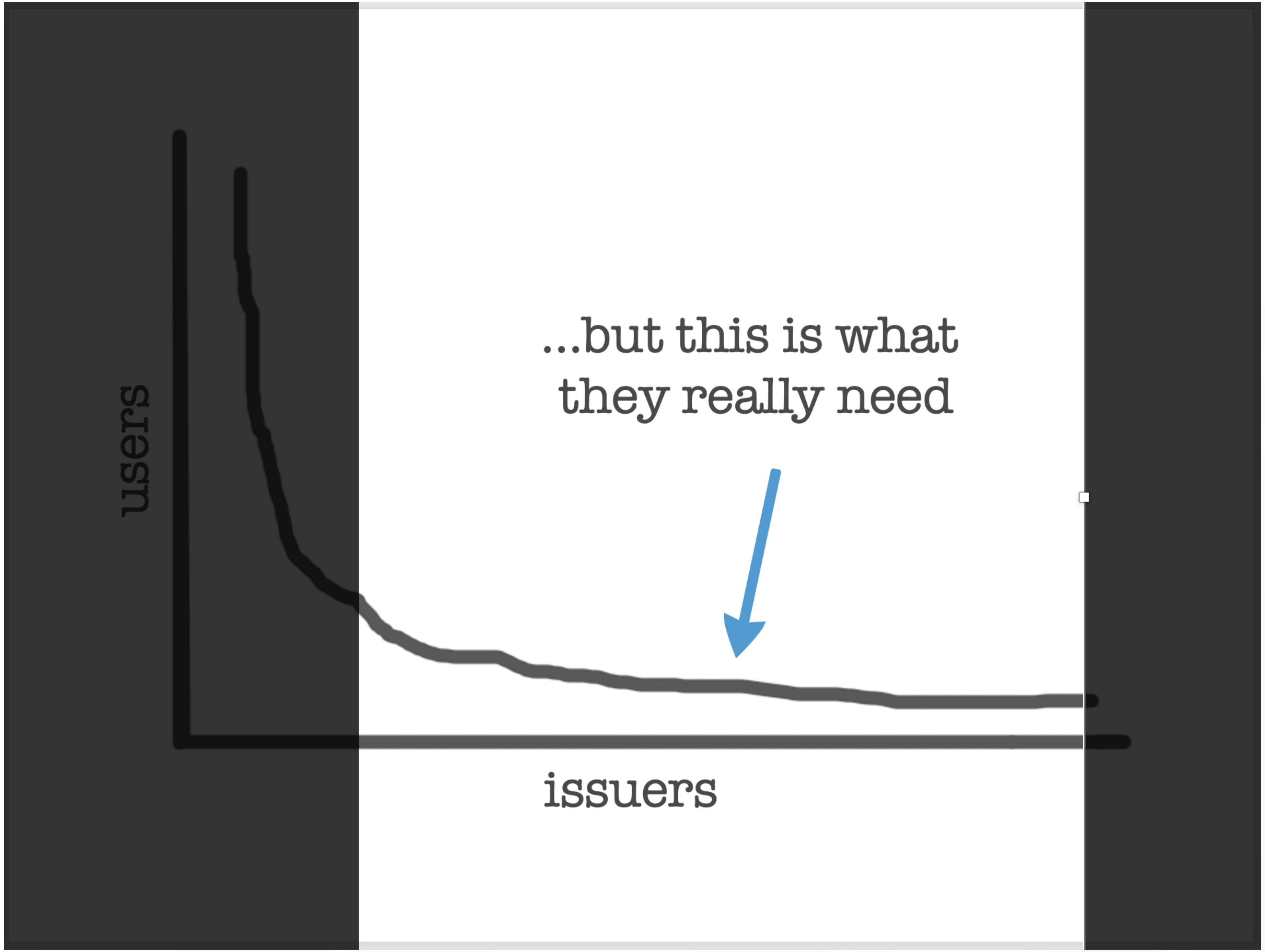
this is what was supposed to be enabled



..but this is what we got



...but, this is what the enterprise wants



...but this is what they really need

What I think I was saying:

- Enterprises are complex ecosystems and 1 IDP doesn’t cut it
- Despite empirical lack of success, user-centric is important

What actually happened:

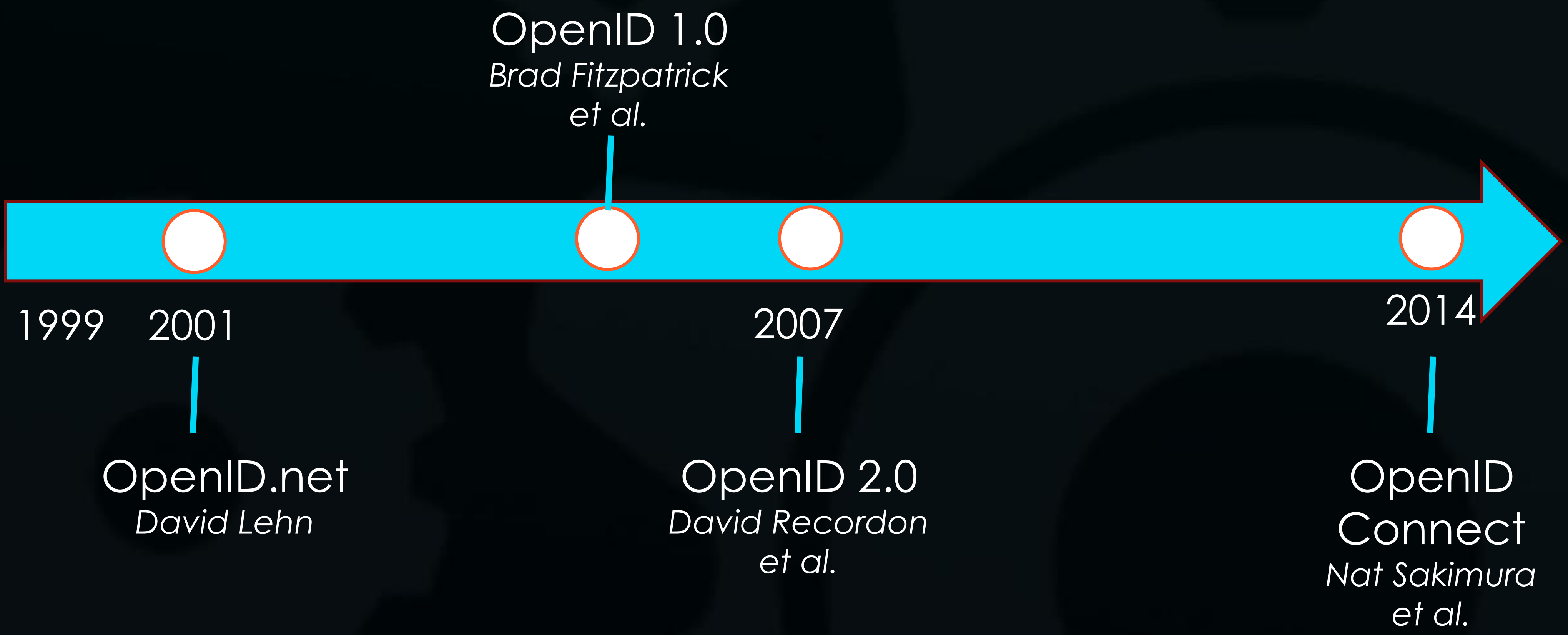
- Cloud IDPs
- New Types of Identity Discovery
- User-centric becomes SSI and it still seeking scale

25 years of OpenID

~ at the 10th Anniversary of the OpenID Connect Final

Nat Sakimura
Chairman of the board, OpenID Foundation

_nat https://www.sakimura.org
https://youtube.com/@55id
https://www.linkedin.com/in/natsakimura



OpenID 1.0
Brad Fitzpatrick et al.

1999

2001

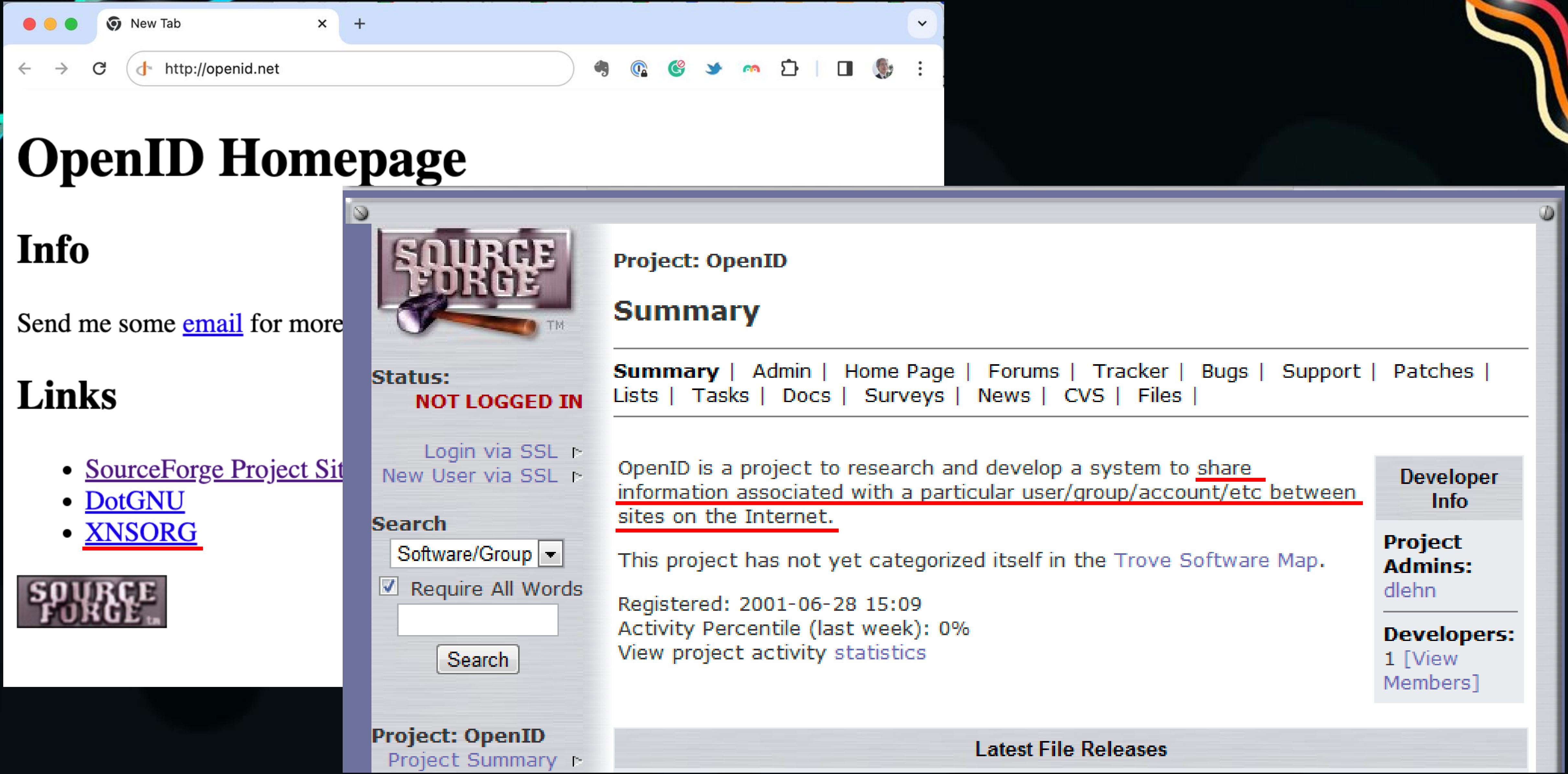
OpenID.net
David Lehn

2007

OpenID 2.0
David Recordon et al.

2014

OpenID Connect
Nat Sakimura et al.



OpenID Homepage

Info

Send me some email for more

Links

- SourceForge Project Sit
- DotGNU
- XNSORG

Status:
NOT LOGGED IN

Project: OpenID

Project: OpenID

Summary

Summary | Admin | Home Page | Forums | Tracker | Bugs | Support | Patches | Lists | Tasks | Docs | Surveys | News | CVS | Files |

OpenID is a project to research and develop a system to share information associated with a particular user/group/account/etc between sites on the Internet.

This project has not yet categorized itself in the Trove Software Map.

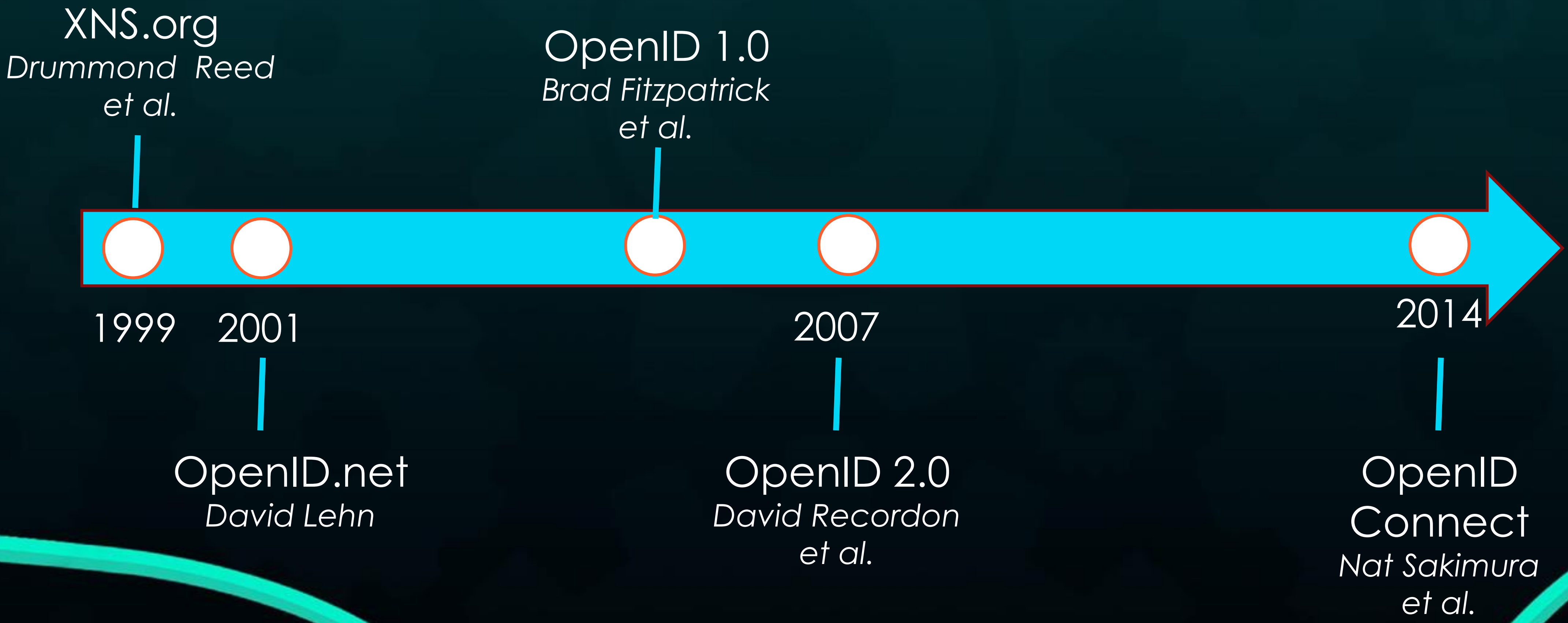
Registered: 2001-06-28 15:09
Activity Percentile (last week): 0%
View project activity statistics

Developer Info

Project Admins:
dlehn

Developers:
1 [View Members]

Latest File Releases



1999

XNS.org
Drummond Reed
et al.

2001

OpenID.net
David Lehn

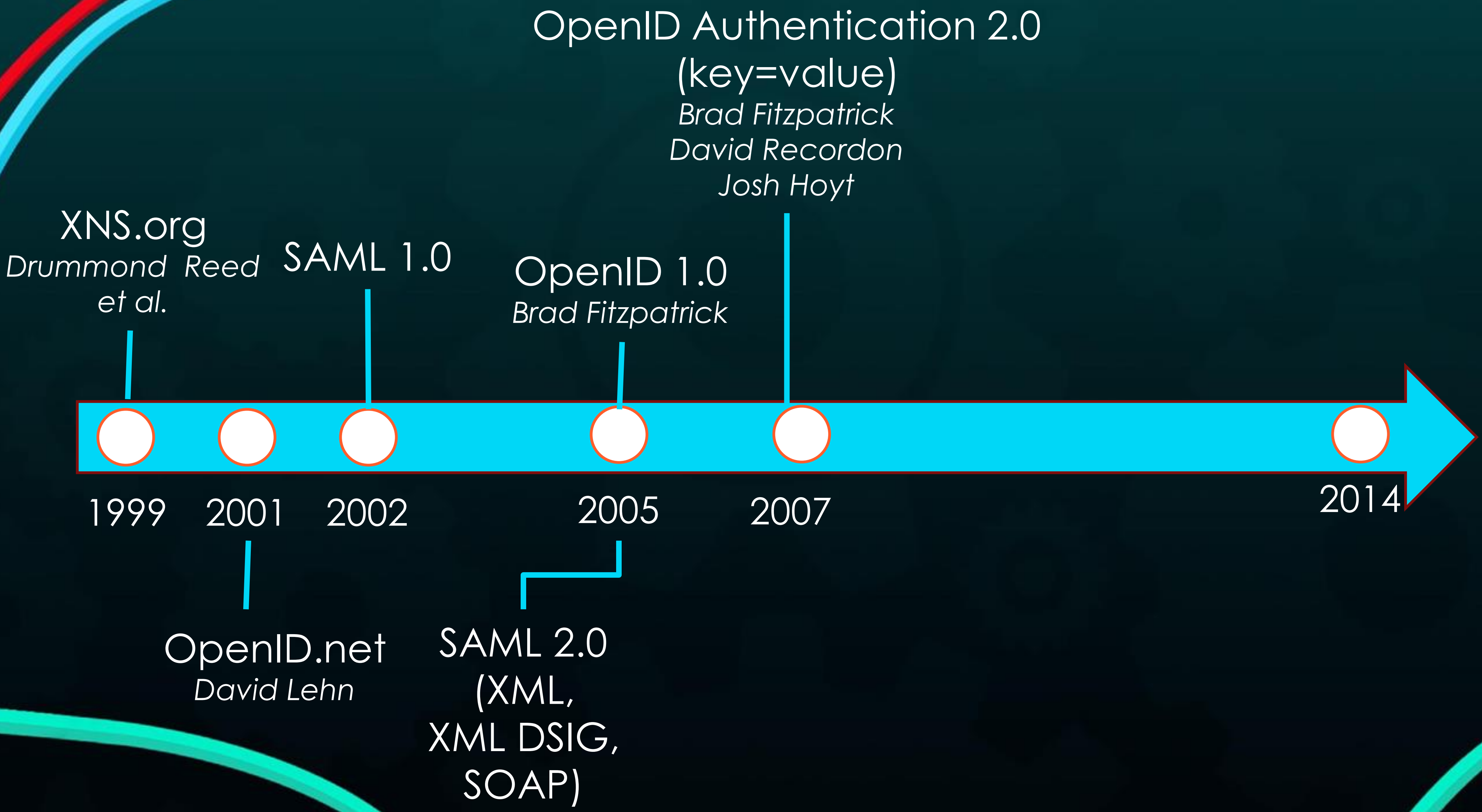
OpenID 1.0
Brad Fitzpatrick
et al.

2007

OpenID 2.0
David Recordon
et al.

2014

OpenID Connect
Nat Sakimura
et al.



1999

XNS.org
Drummond Reed et al.

2001

OpenID.net
David Lehn

2002

SAML 1.0

2005

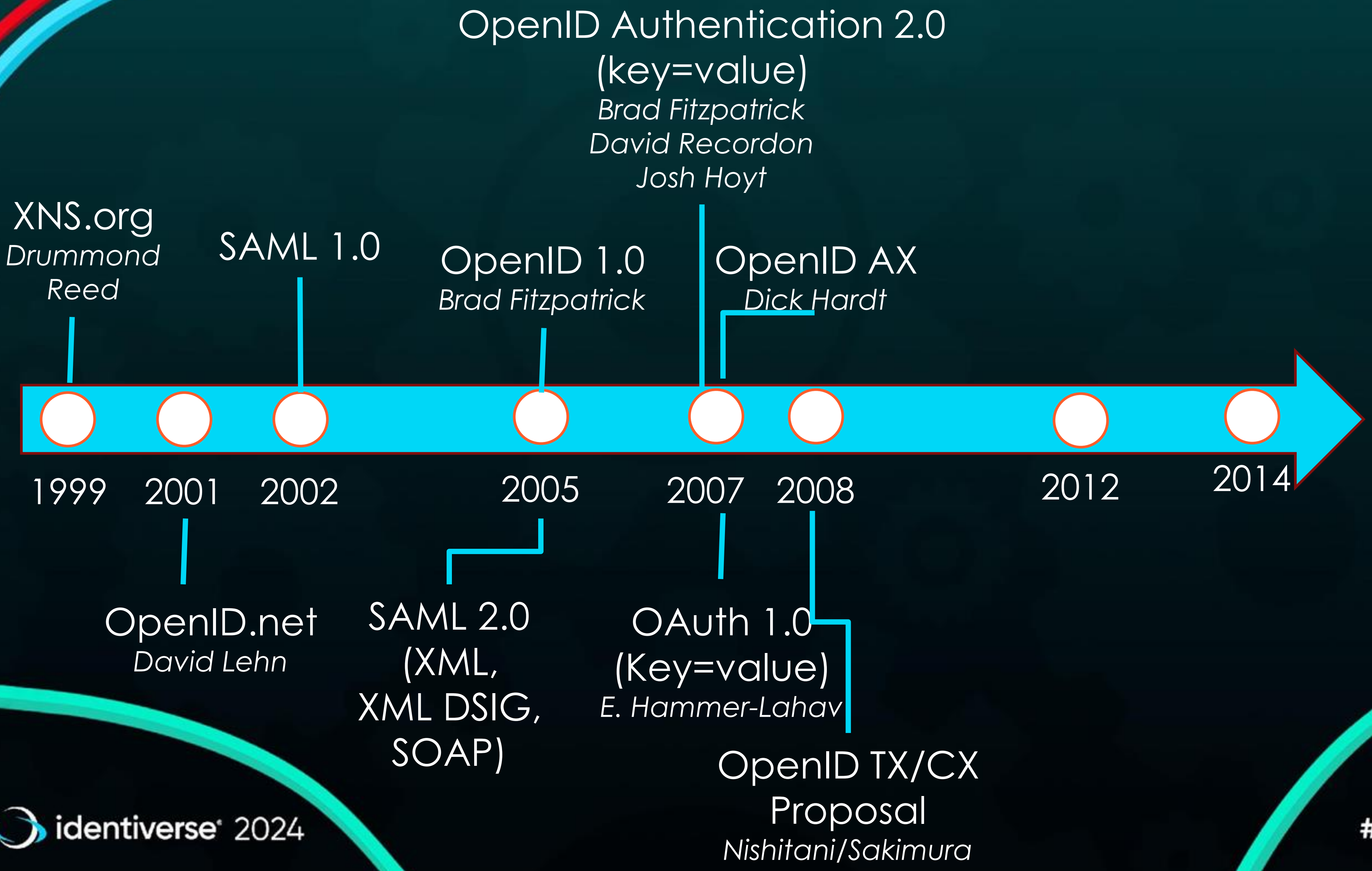
OpenID 1.0
Brad Fitzpatrick

SAML 2.0
(XML,
XML DSIG,
SOAP)

2007

OpenID Authentication 2.0
(key=value)
Brad Fitzpatrick
David Recordon
Josh Hoyt

2014



XNS.org
Drummond Reed

SAML 1.0

OpenID 1.0
Brad Fitzpatrick

OpenID Authentication 2.0
(key=value)
Brad Fitzpatrick
David Recordon
Josh Hoyt

OpenID AX
Dick Hardt

1999

2001

2002

2005

2007

2008

2012

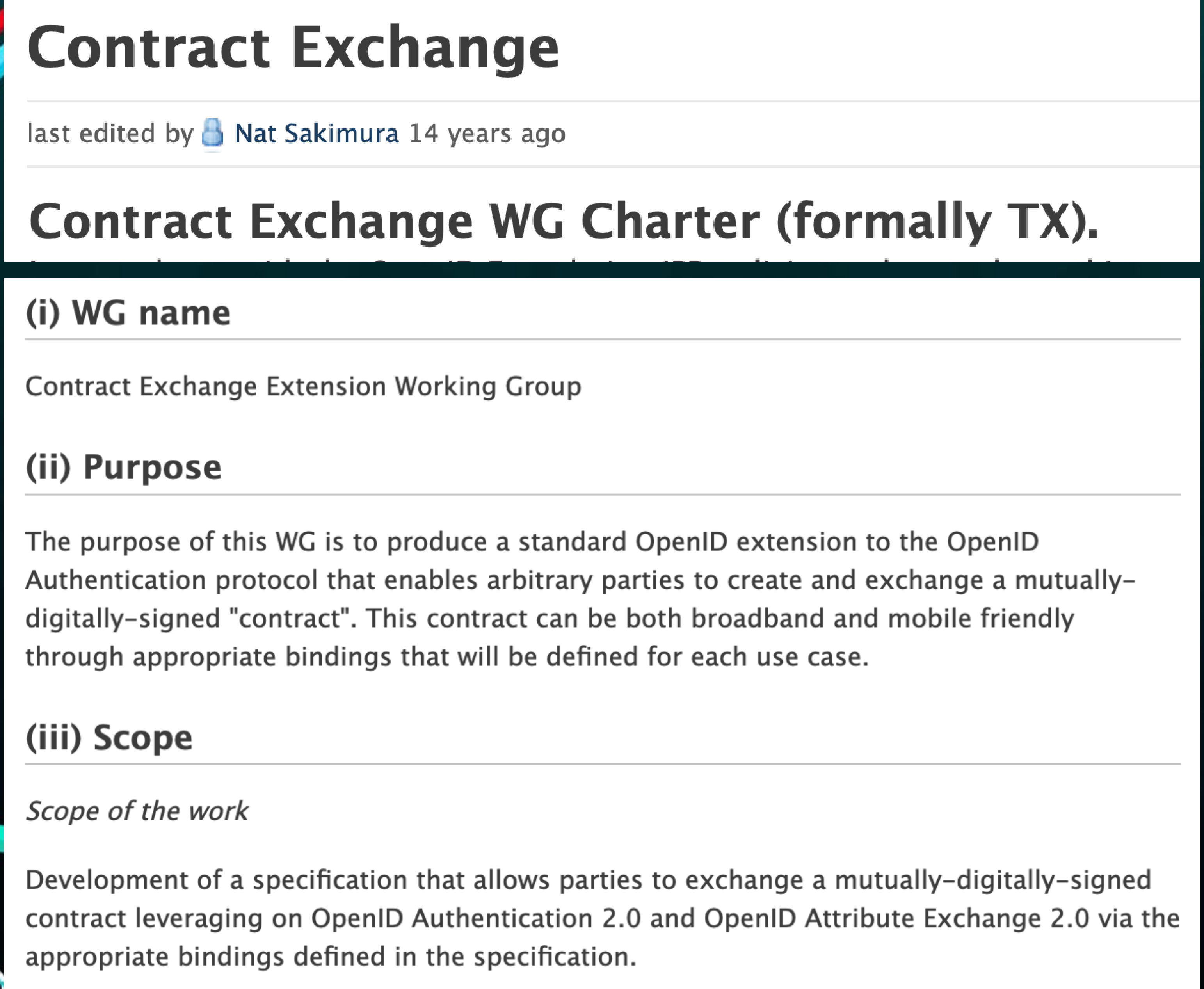
2014

OpenID.net
David Lehn

SAML 2.0
(XML,
XML DSIG,
SOAP)

OAuth 1.0
(Key=value)
E. Hammer-Lahav

OpenID TX/CX
Proposal
Nishitani/Sakimura



Contract Exchange

last edited by Nat Sakimura 14 years ago

Contract Exchange WG Charter (formally TX).

(i) WG name

Contract Exchange Extension Working Group

(ii) Purpose

The purpose of this WG is to produce a standard OpenID extension to the OpenID Authentication protocol that enables arbitrary parties to create and exchange a mutually-digitally-signed "contract". This contract can be both broadband and mobile friendly through appropriate bindings that will be defined for each use case.

(iii) Scope

Scope of the work

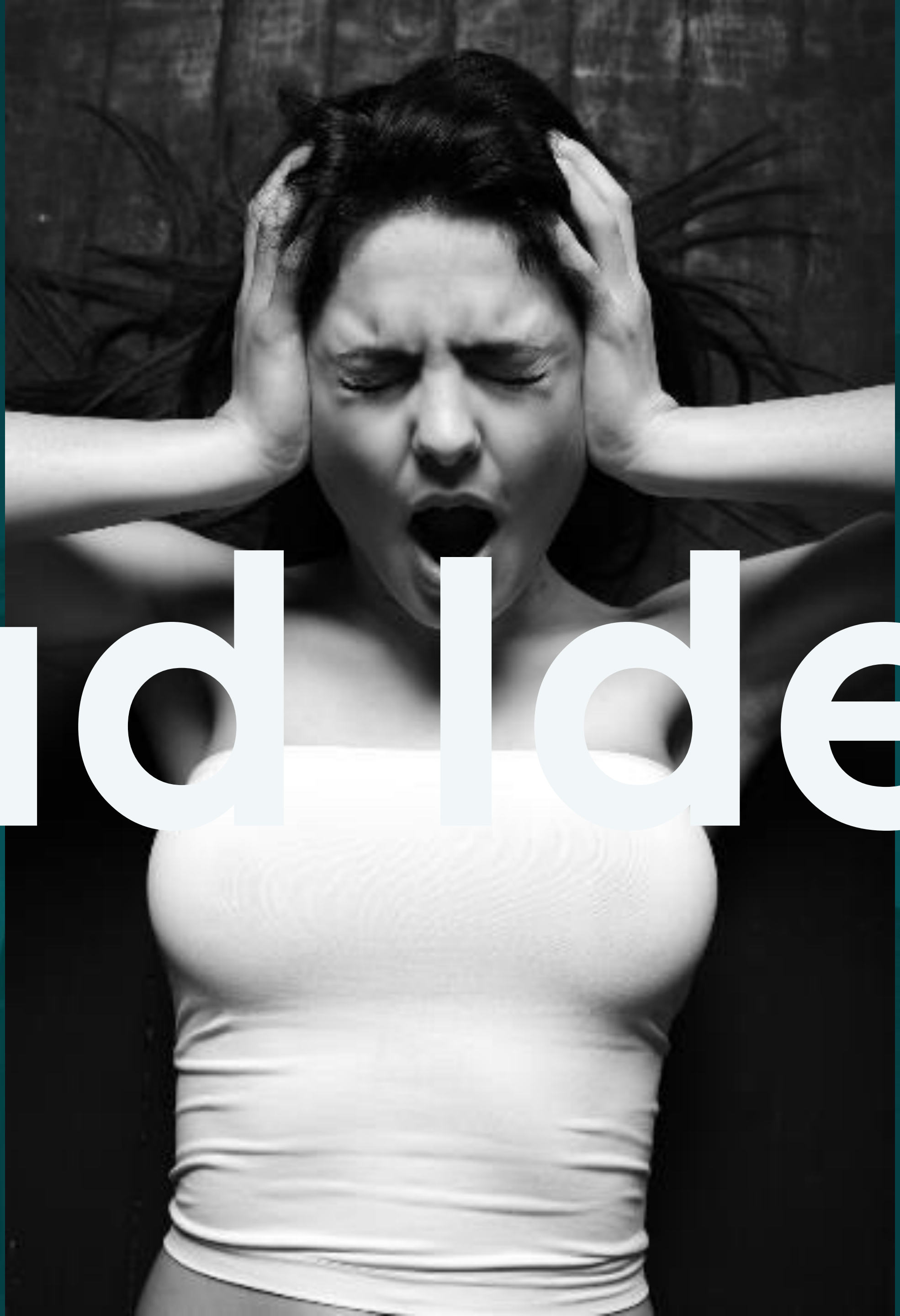
Development of a specification that allows parties to exchange a mutually-digitally-signed contract leveraging on OpenID Authentication 2.0 and OpenID Attribute Exchange 2.0 via the appropriate bindings defined in the specification.

2008

Untrusted Apps

Give password them?

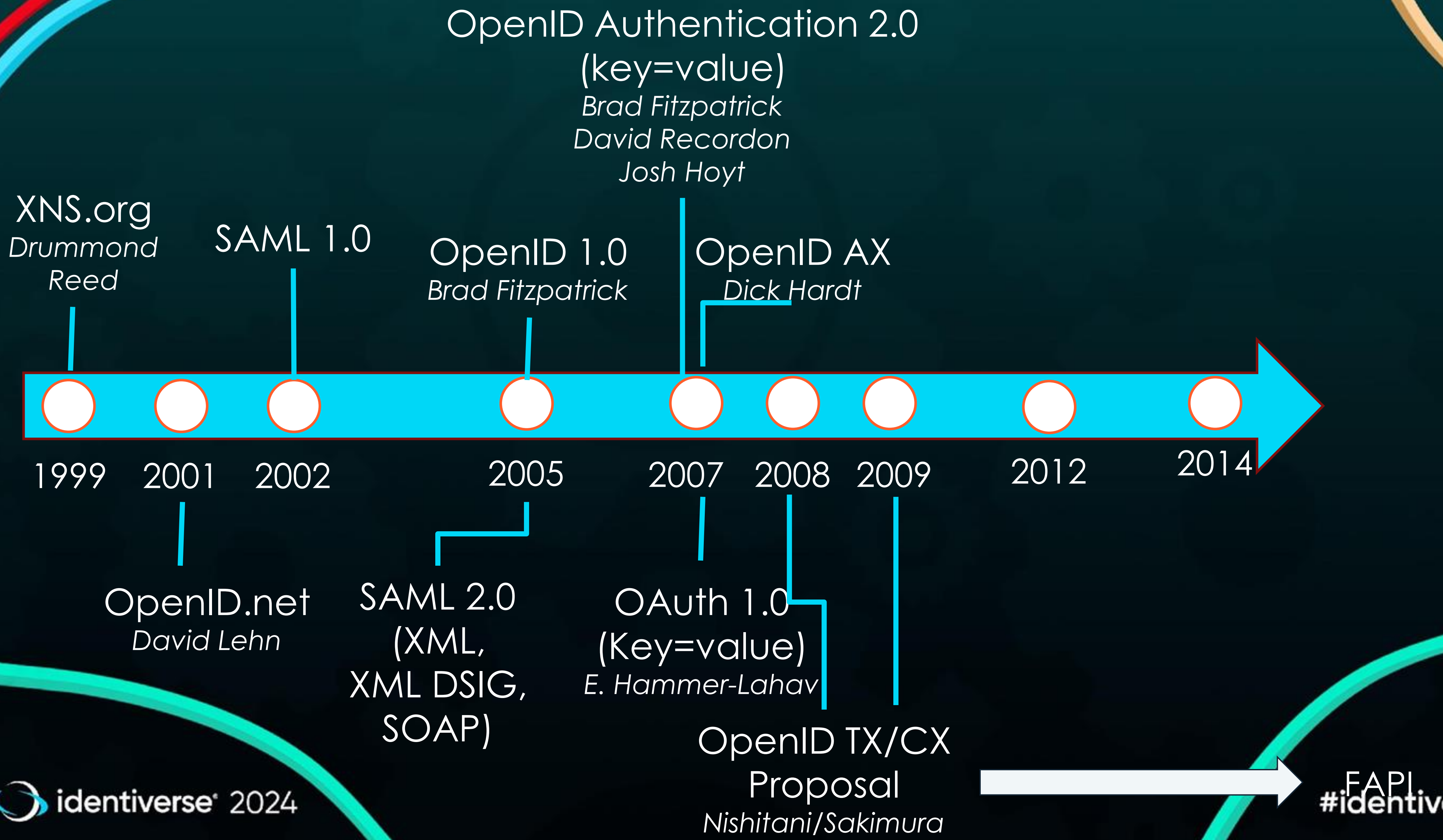
Bad Idea



Audienced identity & Minimum access authorization

ID Token
&
Access Token

Problems of SAML, OpenID Authentication 2.0, OAuth 1.0



XNS.org
Drummond Reed

1999

2001

OpenID.net
David Lehn

SAML 1.0

2002

OpenID 1.0
Brad Fitzpatrick

2005

SAML 2.0
(XML,
XML DSIG,
SOAP)

OpenID Authentication 2.0
(key=value)
Brad Fitzpatrick
David Recordon
Josh Hoyt

OpenID AX
Dick Hardt

2007

OAuth 1.0
(Key=value)
E. Hammer-Lahav

2008

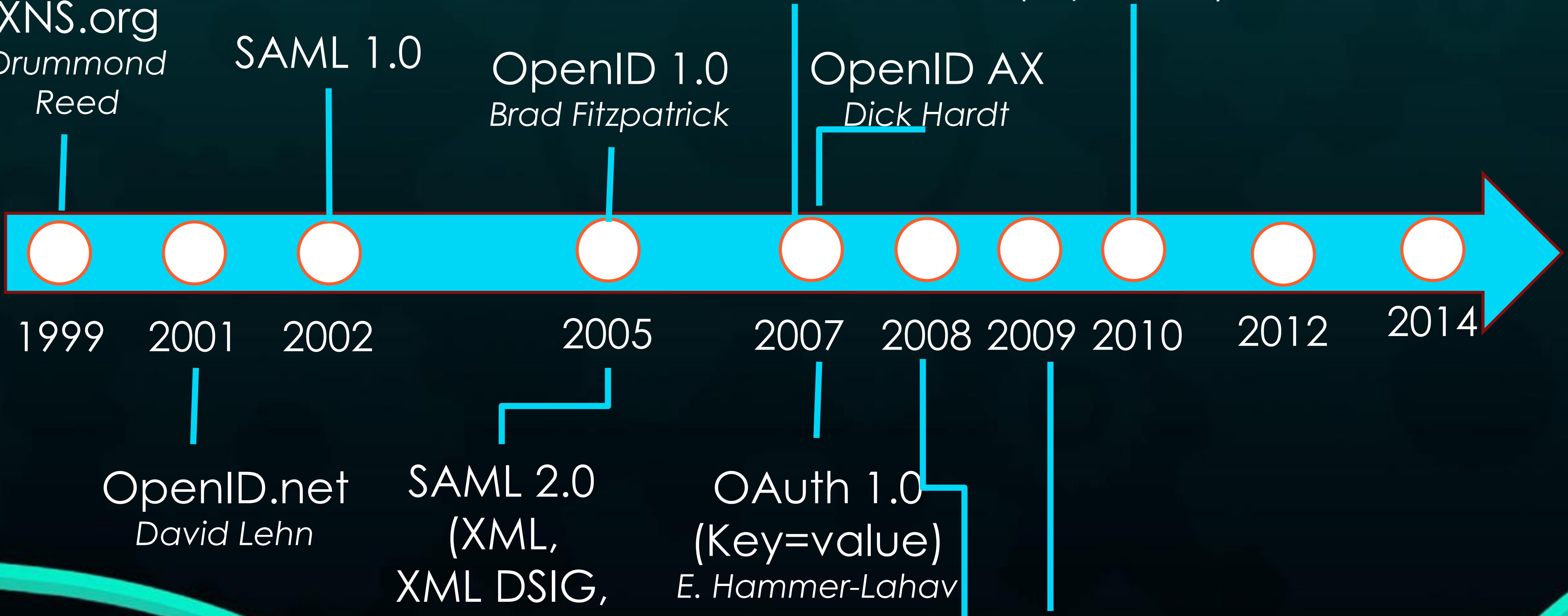
2009

OpenID TX/CX
Proposal
Nishitani/Sakimura

2012

2014

FAPI



1999 2001 2002 2005 2007 2008 2009 2010 2012 2014

XNS.org
Drummond Reed

OpenID.net
David Lehn

SAML 1.0

OpenID 1.0
Brad Fitzpatrick

SAML 2.0
(XML,
XML DSIG,
SOAP)

OpenID Authentication 2.0
(key=value)
Brad Fitzpatrick
David Recordon
Josh Hoyt

OAuth 1.0
(Key=value)
E. Hammer-Lahav

OpenID AX
Dick Hardt

OpenID TX/CX
Proposal
Nishitani/Sakimura

OpenID AB WG
(Key=value?)

Nat Sakimura
(NRI [当時])

John Bradley
(Mercenary working for NRI [当時])

Breno de Madeiros
(Google)

Nat Sakimura
(NRI [当時])

John Bradley
(Mercenary working
for NRI [当時])

Breno de Madeiros
(Google)

Ryo Ito
(Yahoo! Japan [当時])

Hideki Nara
(Tact [当時])

Early design decisions:

1. No canonicalization
2. ASCII Armoring
3. JSON
4. REST

JSON Simple Signature (JSS) & Encryption (JSE)

Then, there was a parallel work

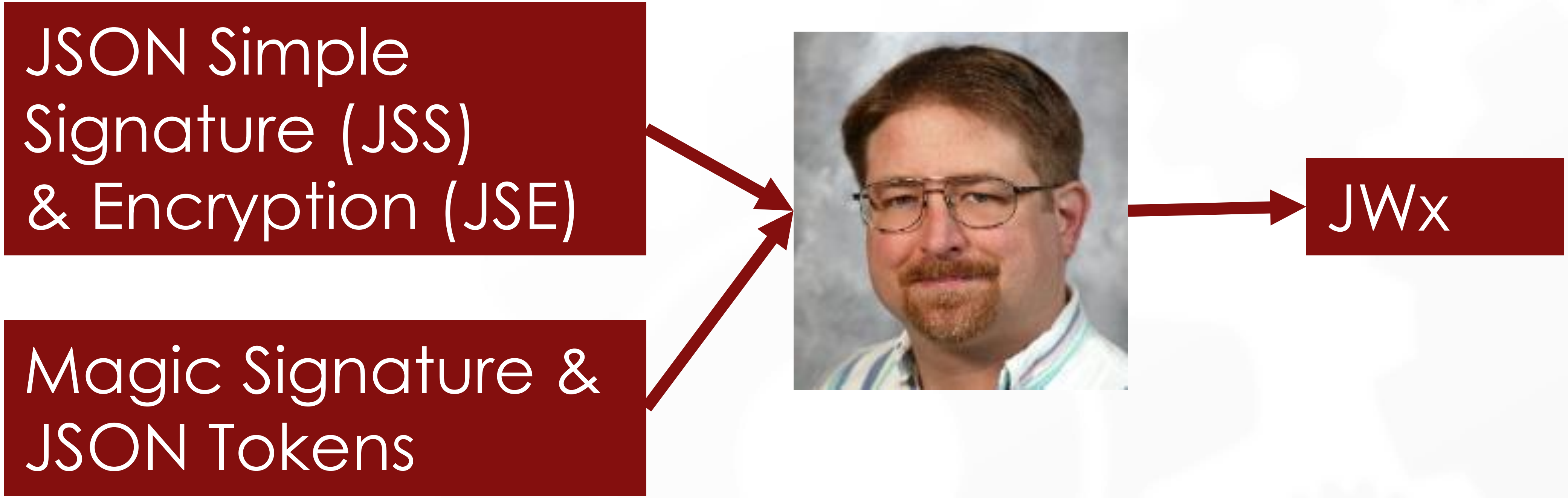
Magic Signature & JSON Token

Dirk Balfanz

John Panzer

And there came Mike Jones

- “You guys should come together and standardize it at IETF. Don’t worry. I can take care of the editing!”



JSON Simple Signature (JSS) & Encryption (JSE)

Magic Signature & JSON Tokens

JWx

JWx

- JWS: JSON Web Signature
- JWE: JSON Web Encryption
- JWT: JSON Web Token etc.

Early design decisions:

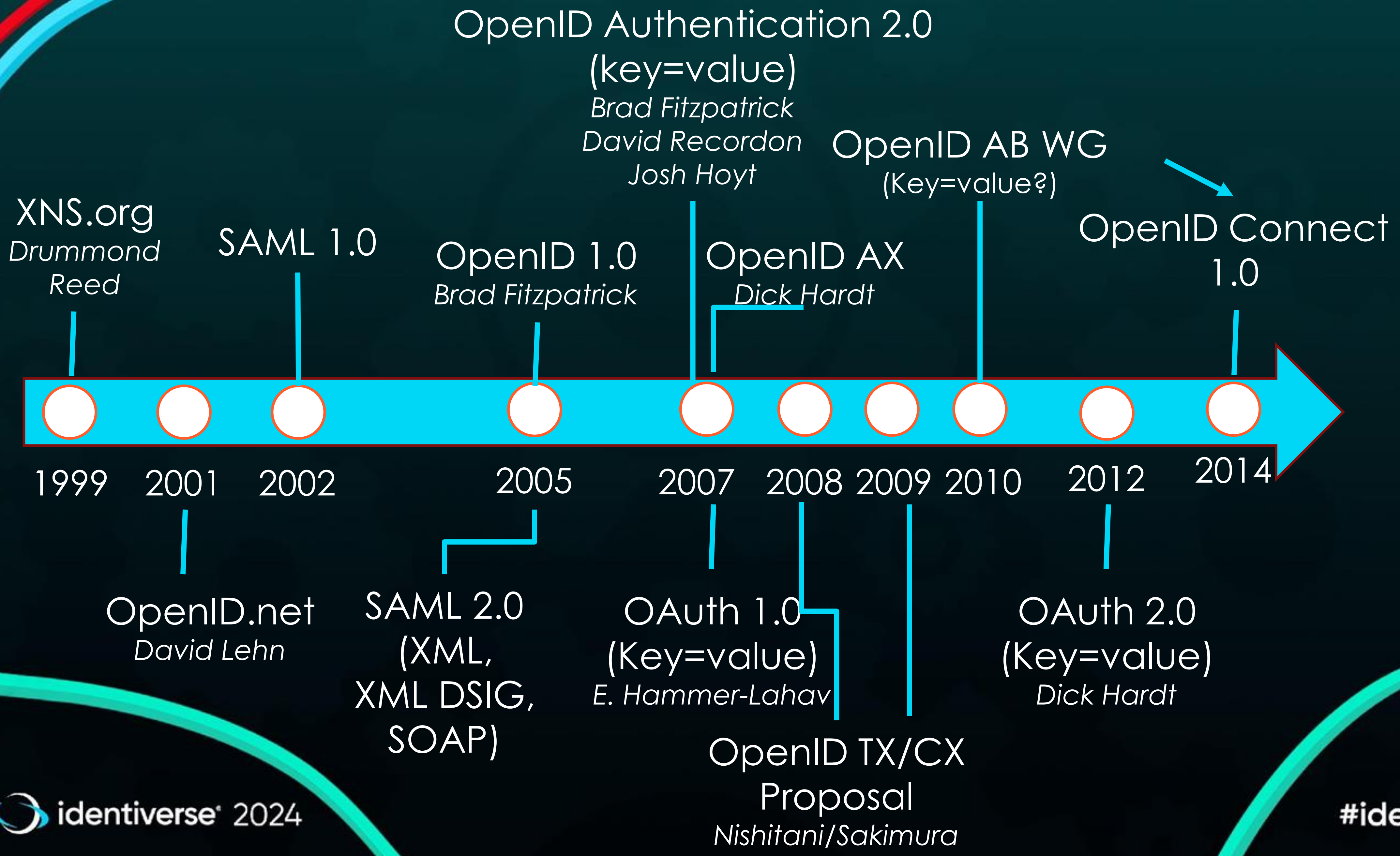
1. No canonicalization
2. ASCII Armoring
3. JSON
4. REST
5. JWx

Early design decisions:

1. No canonicalization
2. ASCII Armoring
3. JSON
4. REST
5. JWx
6. Base on OAuth WRAP

Dick Hardt

Allen Tom



1999
XNS.org
Drummond Reed

2001
OpenID.net
David Lehn

2002
SAML 1.0

2005
OpenID 1.0
Brad Fitzpatrick

SAML 2.0
(XML,
XML DSIG,
SOAP)

2007
OpenID Authentication 2.0
(key=value)
Brad Fitzpatrick
David Recordon
Josh Hoyt

OpenID AX
Dick Hardt

OAuth 1.0
(Key=value)
E. Hammer-Lahav

2008
OpenID TX/CX
Proposal
Nishitani/Sakimura

2009

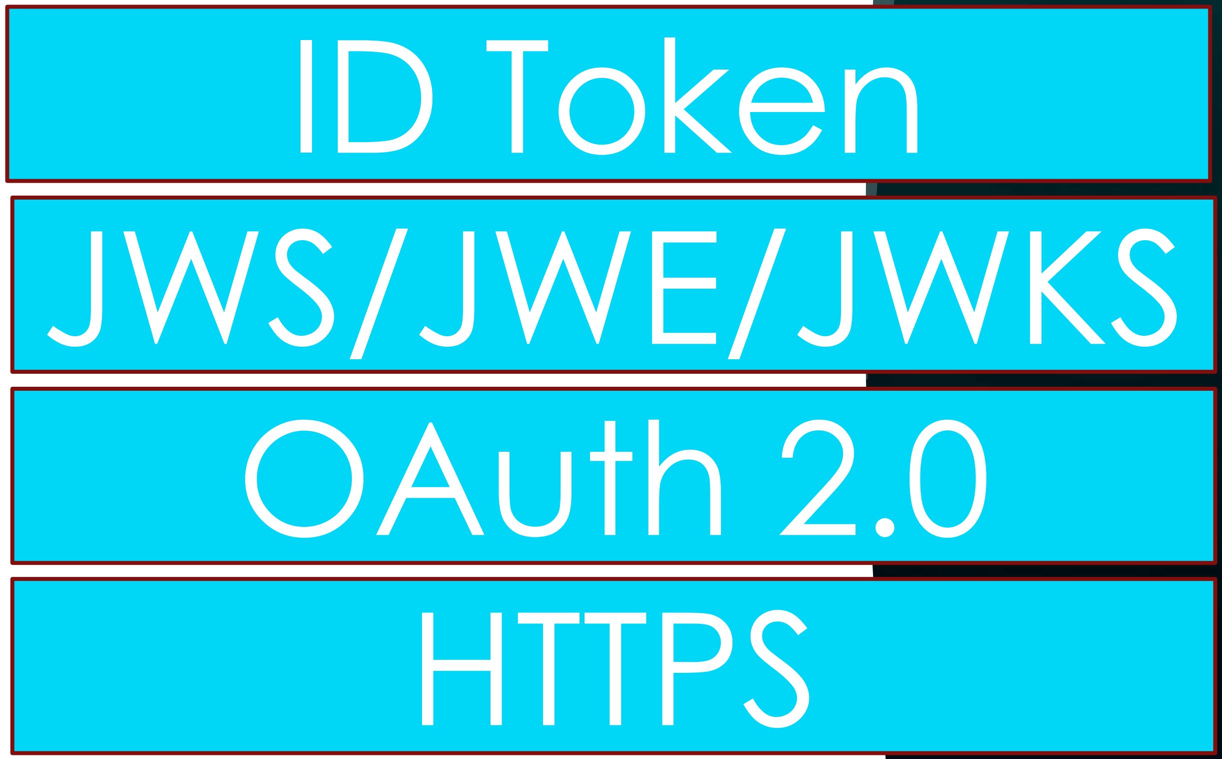
2010
OpenID AB WG
(Key=value?)

2012
OAuth 2.0
(Key=value)
Dick Hardt

2014
OpenID Connect
1.0

What we have achieved

OpenID Connect



ID Token

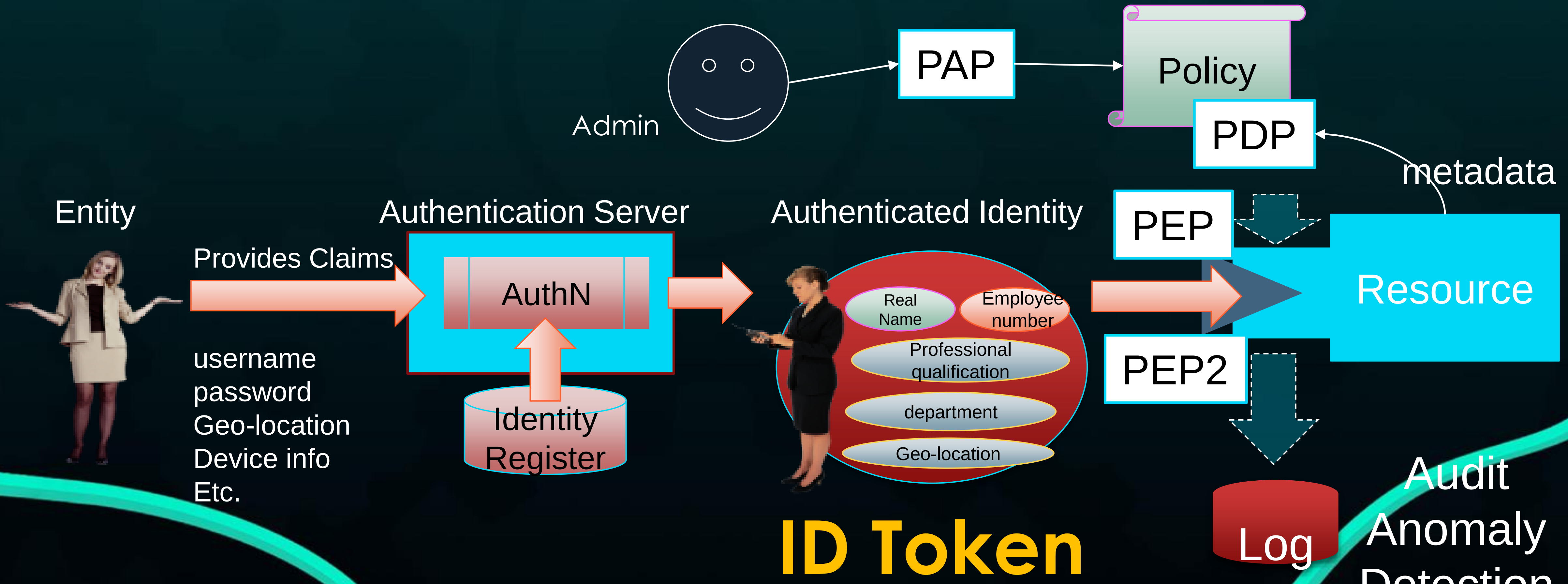
JWS/JWE/JWKS

OAuth 2.0

HTTPS

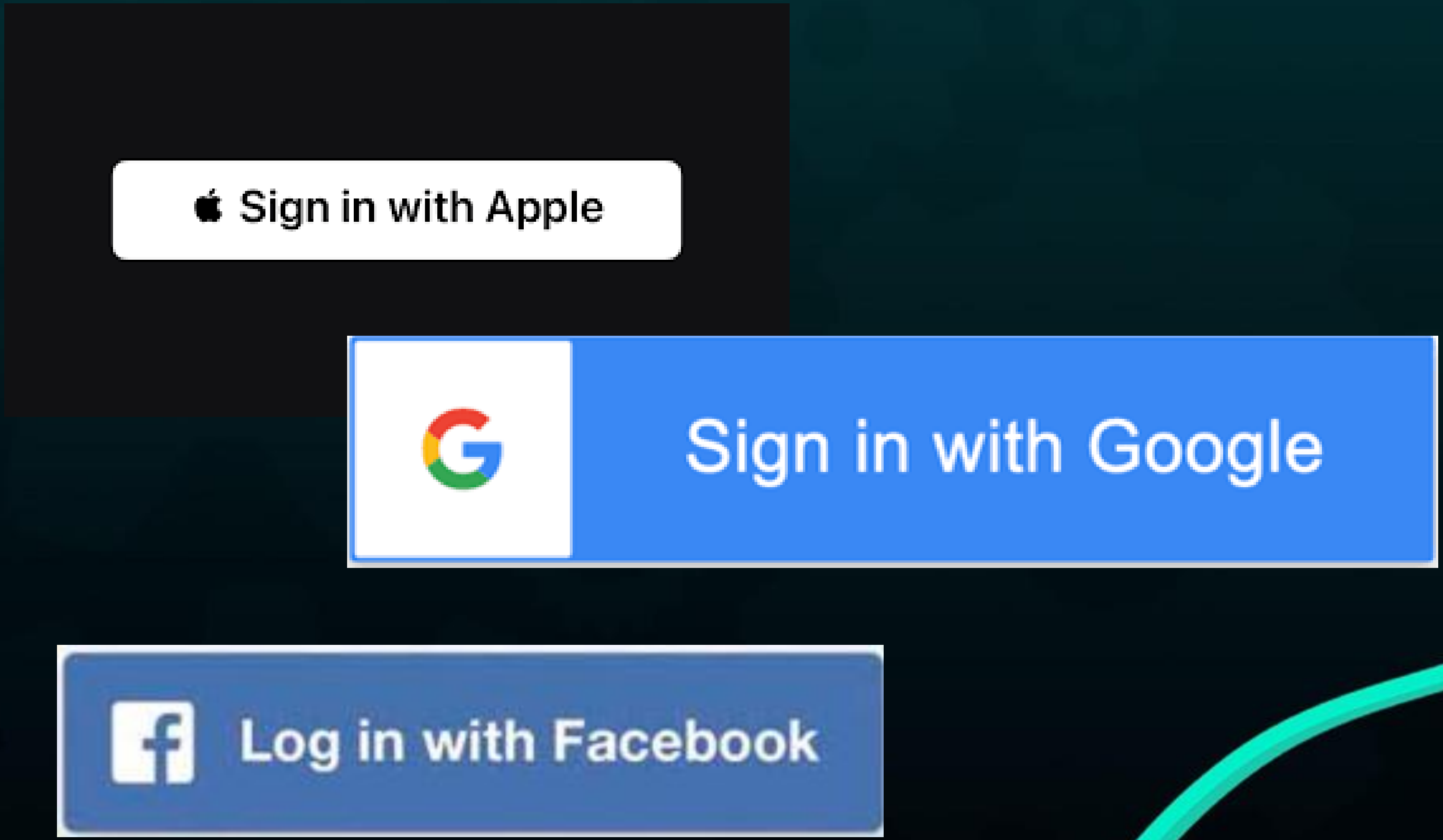
A protocol that defines for a client how to request and for the server to provide the ID Token

That is perfectly fit for modern identity and access control frameworks



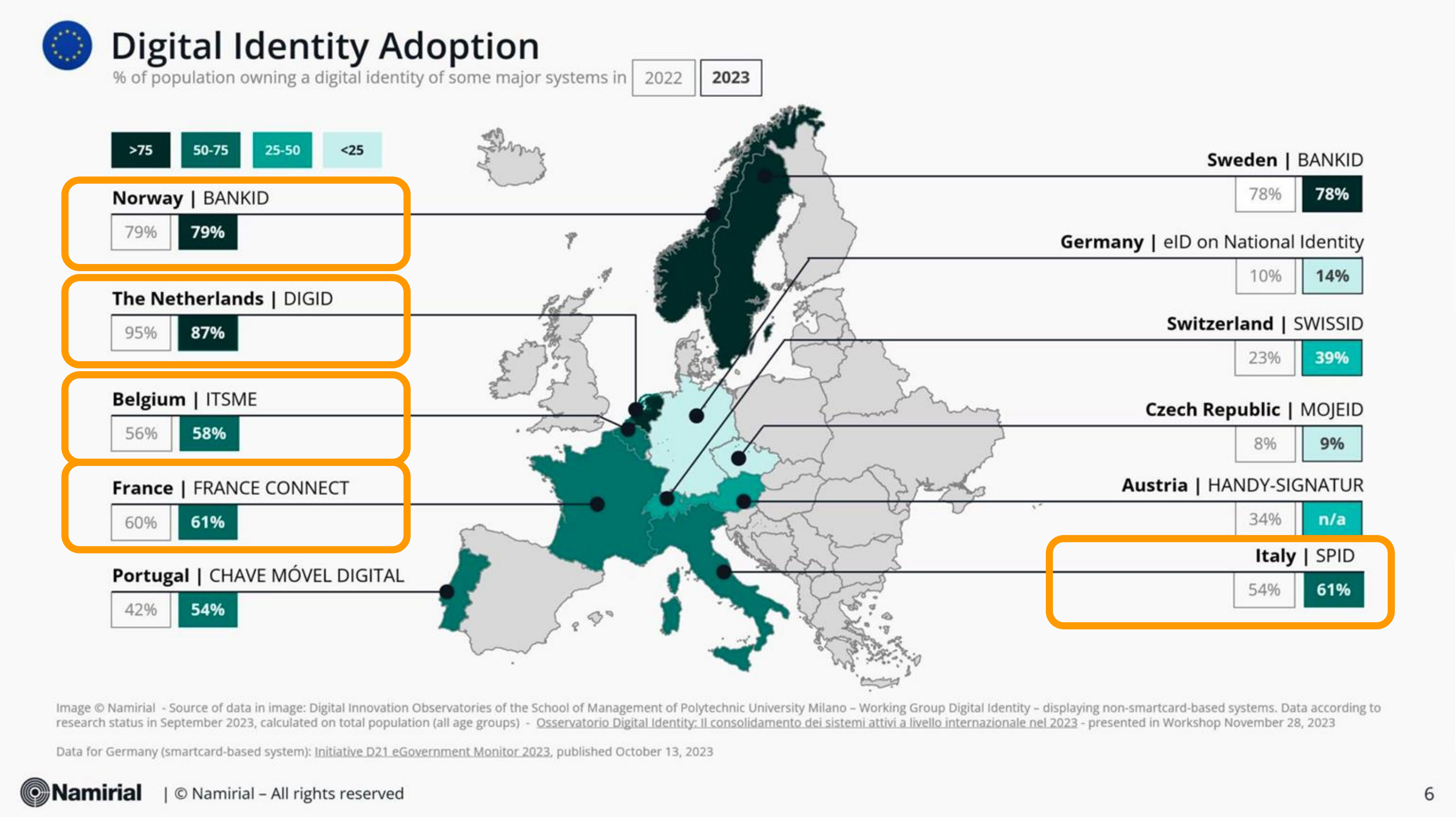
The mainstream federated identity system

- Social Login
- National Identity



The mainstream federated identity system

- Social Login
- National Identit



Digital Identity Adoption

% of population owning a digital identity of some major systems in 2022 **2023**

	2022	2023
Norway | BANKID	79%	**79%**
The Netherlands | DIGID	95%	**87%**
Belgium | ITSME	56%	**58%**
France | FRANCE CONNECT	60%	**61%**
Portugal | CHAVE MÓVEL DIGITAL	42%	**54%**
Sweden | BANKID	78%	**78%**
Germany | eID on National Identity	10%	**14%**
Switzerland | SWISSID	23%	**39%**
Czech Republic | MOJEID	8%	**9%**
Austria | HANDY-SIGNATUR	34%	**n/a**
Italy | SPID	54%	**61%**

Image © Namirial - Source of data in image: Digital Innovation Observatories of the School of Management of Polytechnic University Milano – Working Group Digital Identity – displaying non-smartcard-based systems. Data according to research status in September 2023, calculated on total population (all age groups) - Osservatorio Digital Identity: Il consolidamento dei sistemi attivi a livello internazionale nel 2023 - presented in Workshop November 28, 2023

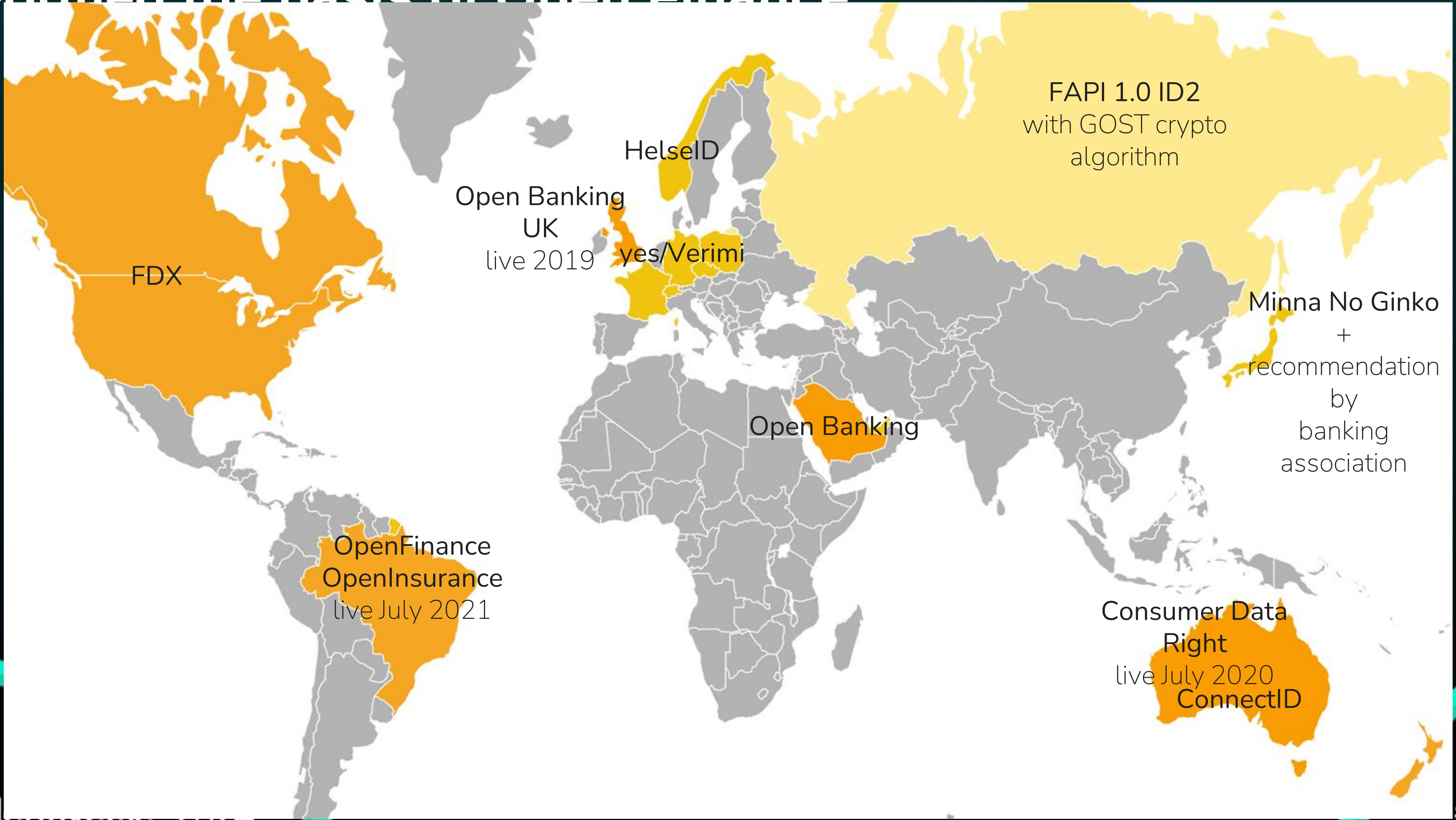
Data for Germany (smartcard-based system): Initiative D21 eGovernment Monitor 2023, published October 13, 2023

Namirial | © Namirial – All rights reserved

6

(Source): Bas[illegible]/www.namiri[illegible]m/news/[illegible]e-of-play-on-adoption-of-d[illegible]ity-in-italy-202[illegible]ds-[illegible]d-fo[illegible]-wallet/

Formed the basis of Open Finance



FDX

Open Banking UK
live 2019

HelseID

yes/Verimi

FAPI 1.0 ID2
with GOST crypto algorithm

Minna No Ginko
+
recommendation by banking association

Open Banking

OpenFinance
OpenInsurance
live July 2021

Consumer Data Right
live July 2020
ConnectID

How we achieved it

Listening to developer feedback

Solve what was not solved

No Canonicalisation

Dead Simple for simple use-cases

Security and Privacy Facilities

What lessons we learned that could apply to other initiatives

Learn from History

Make it simple to read, simple to implement for the minimum viable case

Find the developer pain and solve it

OpenID: there is no spoon

John Bradley

Principal Architect

Yubico

AKA Mercenary

OpenID is more than a single specification or Idea

Insert inciteful comment….