25 years of OpenID

~ at the 10th Anniversary of the OpenID Connect Final

崎村夏彦 | Nat Sakimura

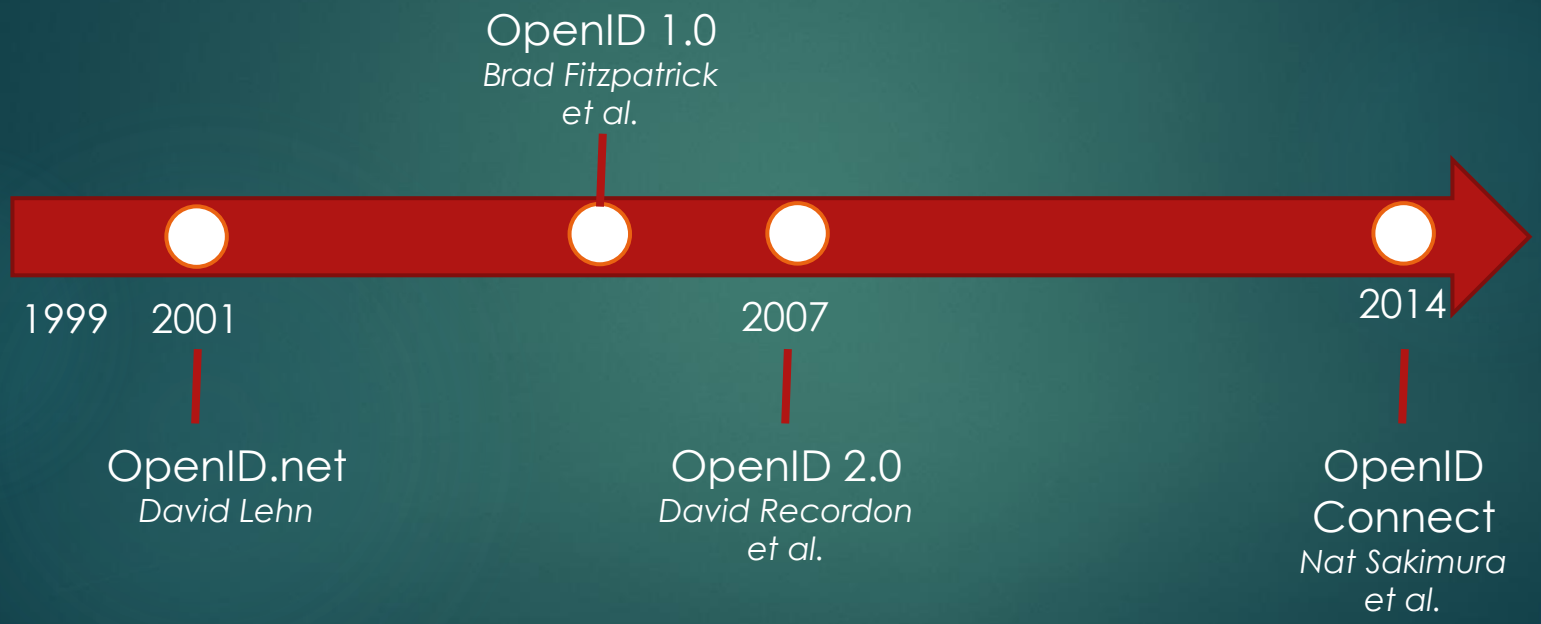
Chairman of the board, OpenID Foundation

_nat

https://www.sakimura.org

https://youtube.com/@55id

https://www.linkedin.com/in/natsakimura


OpenID 1.0
Brad Fitzpatrick
et al.
1999
2001
2007
2014
OpenID.net
David Lehn
OpenID 2.0
David Recordon
et al.
OpenID
Connect
Nat Sakimura
et al.

New Tab

http://openid.net

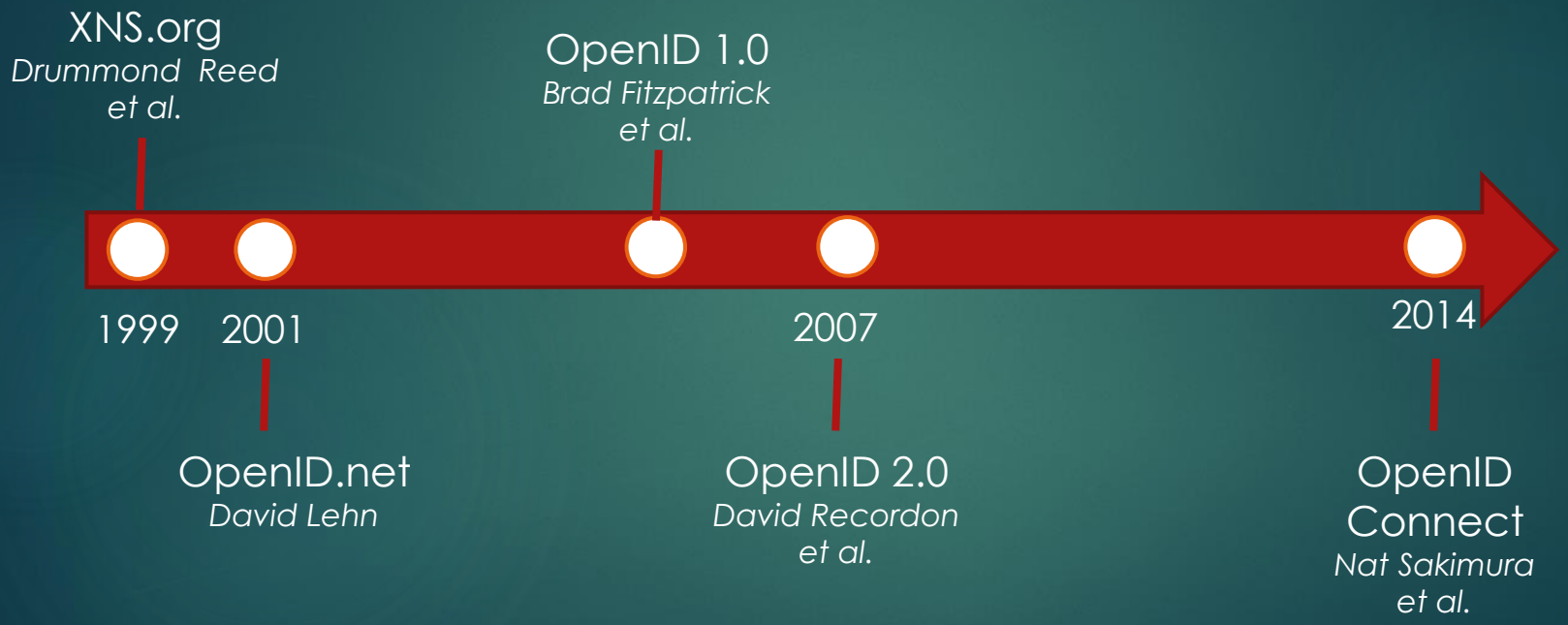
OpenID Homepage

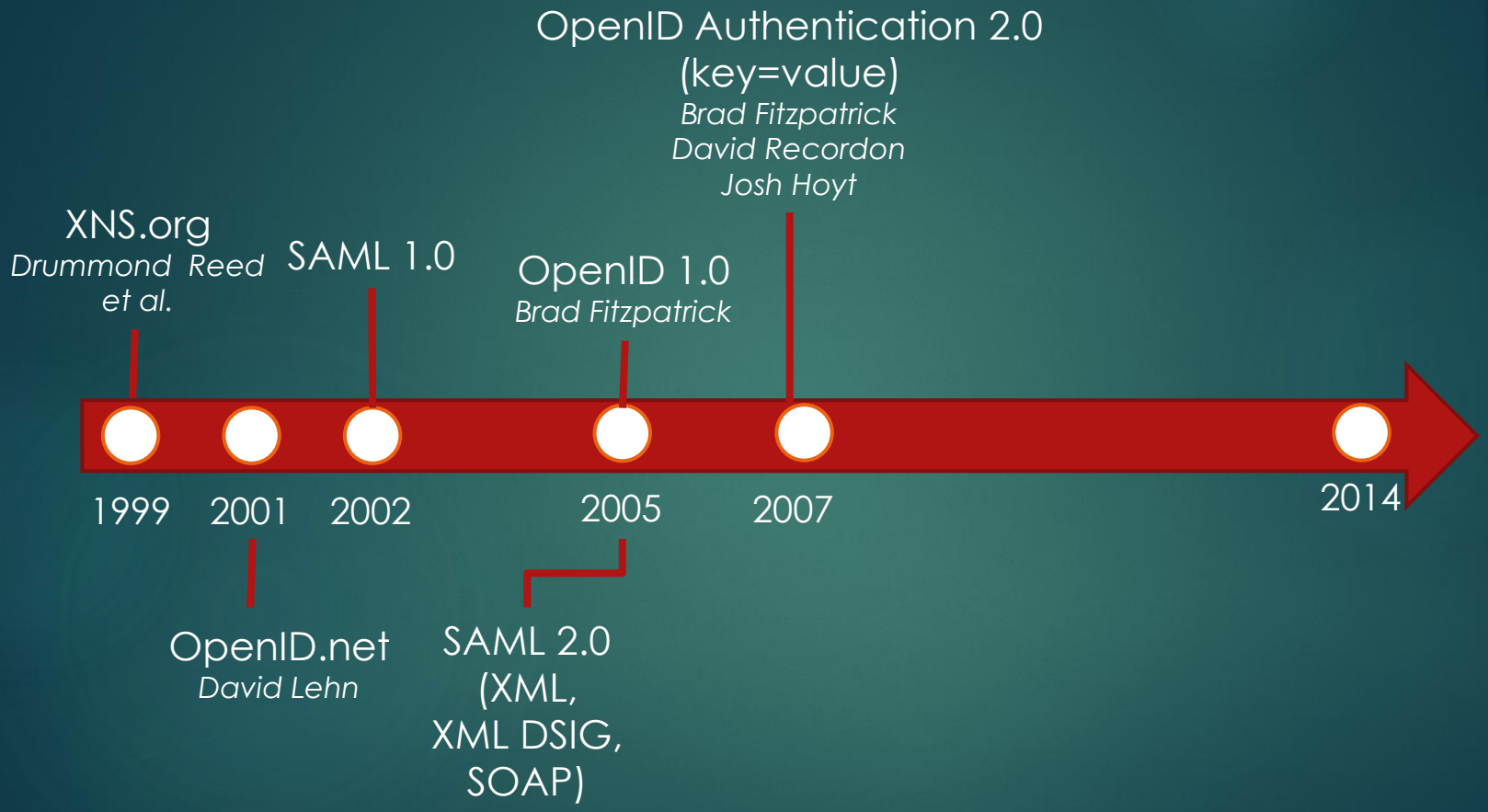
Info

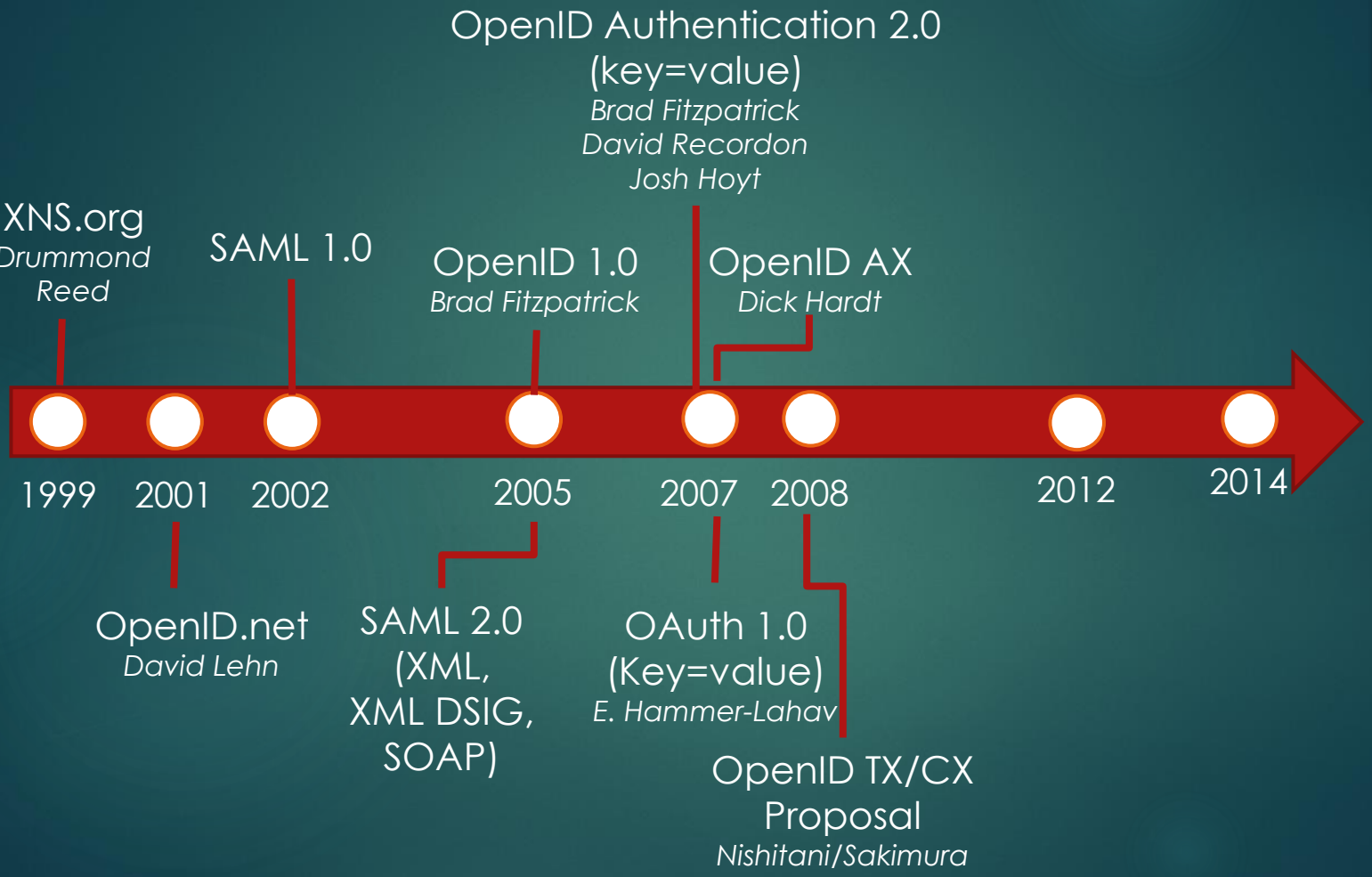
Send me some email for more

Links

- SourceForge Project Sit
- DotGNU
- XNSORG


XNS.org
Drummond Reed
et al.
OpenID 1.0
Brad Fitzpatrick
et al.
1999
2001
2007
2014
OpenID.net
David Lehn
OpenID 2.0
David Recordon
et al.
OpenID
Connect
Nat Sakimura
et al.


OpenID Authentication 2.0
(key=value)
Brad Fitzpatrick
David Recordon
Josh Hoyt
XNS.org
Drummond Reed
et al.
SAML 1.0
OpenID 1.0
Brad Fitzpatrick
1999
2001
2002
2005
2007
2014
OpenID.net
David Lehn
SAML 2.0
(XML,
XML DSIG,
SOAP)


OpenID Authentication 2.0
(key=value)
Brad Fitzpatrick
David Recordon
Josh Hoyt
XNS.org
Drummond Reed
SAML 1.0
OpenID 1.0
Brad Fitzpatrick
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

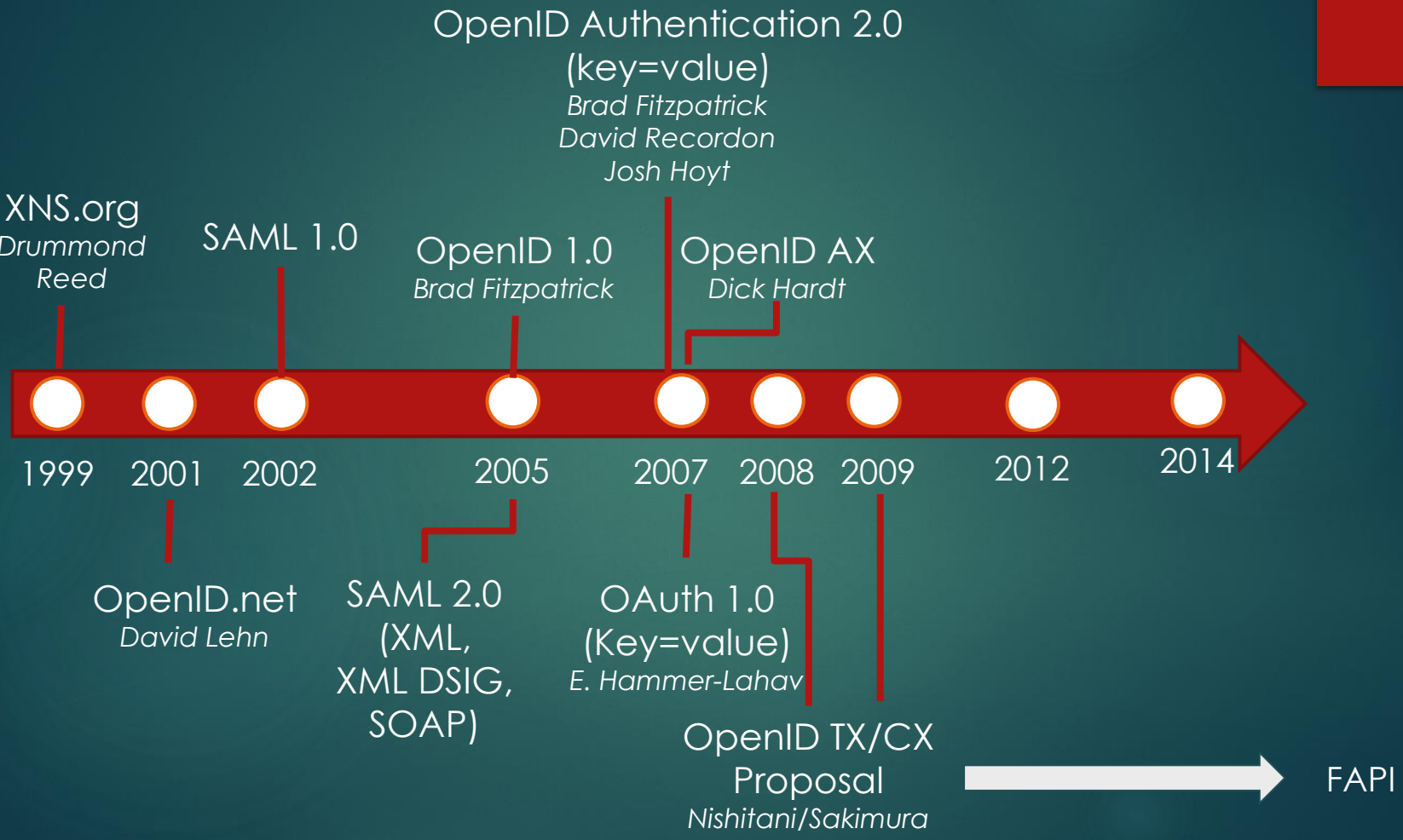
Give passwords (full right) to all of them?

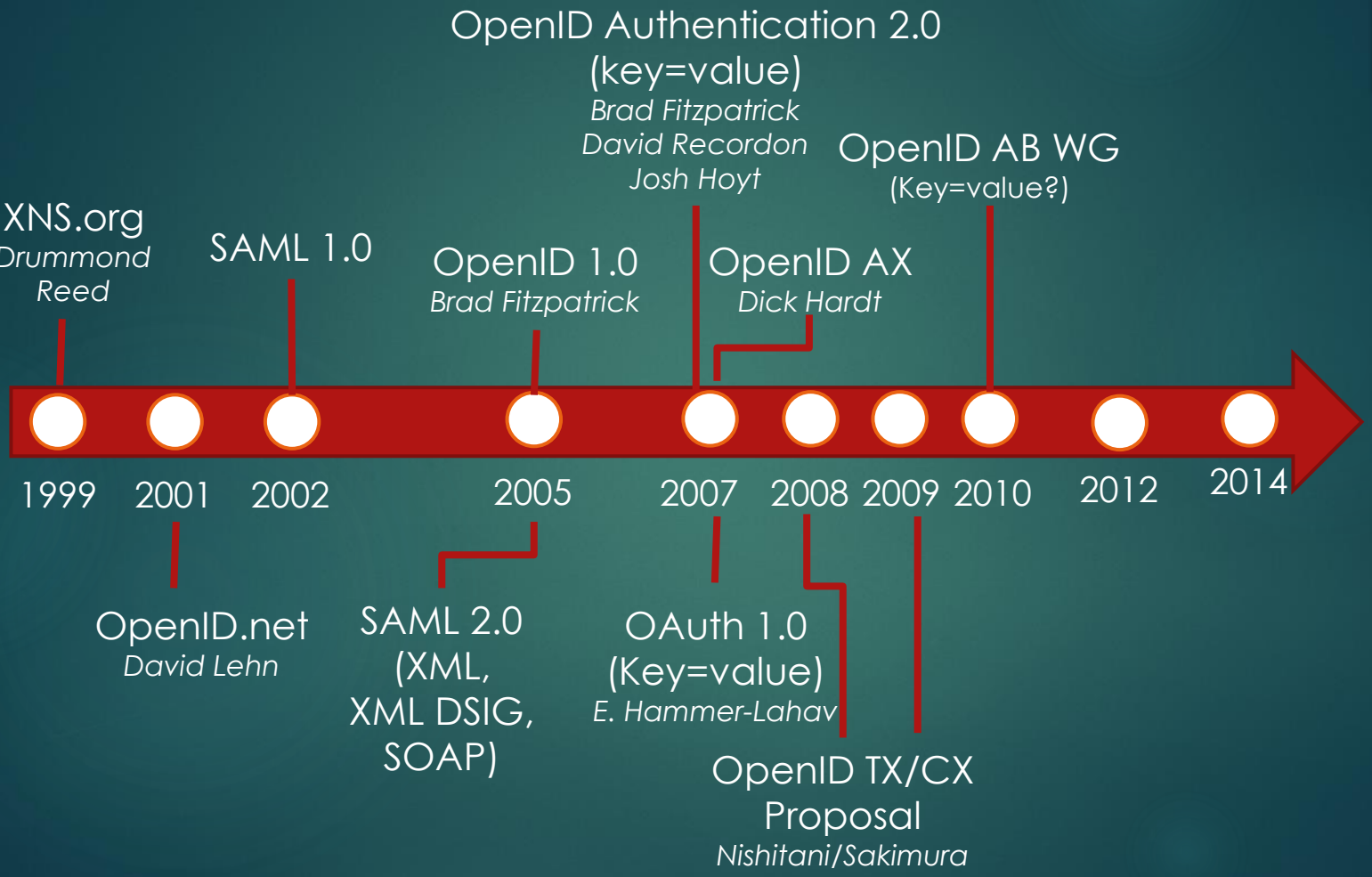
Bad Idea

Audienced identity
&
Minimum access authorization

ID Token
&
Access Token

Problems of SAML, OpenID Authentication 2.0, OAuth 1.0


OpenID Authentication 2.0
(key=value)
Brad Fitzpatrick
David Recordon
Josh Hoyt
XNS.org
Drummond Reed
SAML 1.0
OpenID 1.0
Brad Fitzpatrick
OpenID AX
Dick Hardt
1999
2001
2002
2005
2007
2008
2009
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
FAPI


OpenID Authentication 2.0
(key=value)
Brad Fitzpatrick
David Recordon
Josh Hoyt
OpenID AB WG
(Key=value?)
XNS.org
Drummond
Reed
SAML 1.0
OpenID 1.0
Brad Fitzpatrick
OpenID AX
Dick Hardt
1999
2001
2002
2005
2007
2008
2009
2010
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

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:

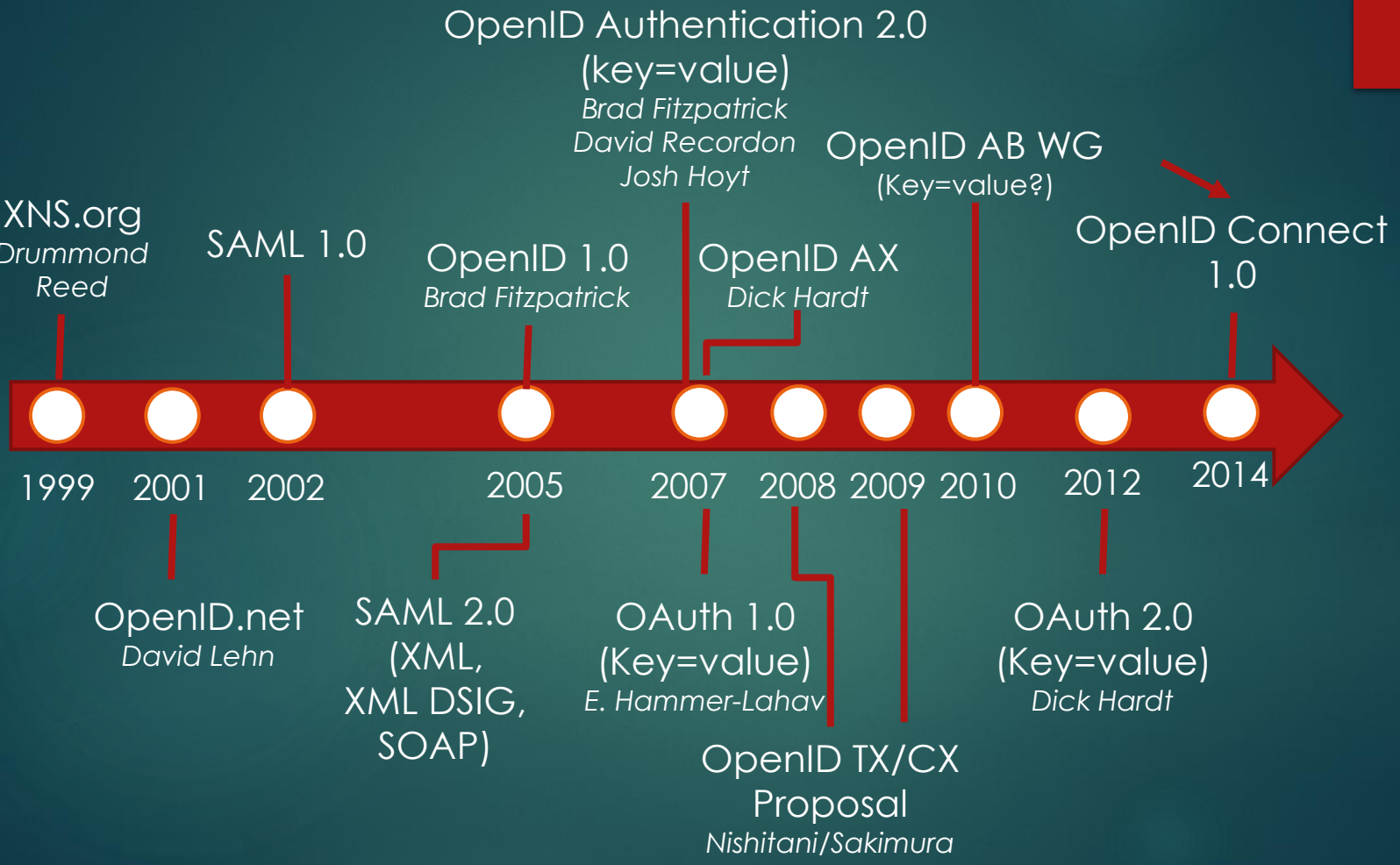
1. No canonicalization
2. ASCII Armoring
3. JSON
4. REST
5. JWx

Early design decisions:

1. No canonicalization
2. ASCII Armoring
3. JSON
4. REST
5. JWx
6. Base on OAuth ~~WRAP~~ 2.0

Dick Hardt

Allen Tom


OpenID Authentication 2.0
(key=value)
Brad Fitzpatrick
David Recordon
Josh Hoyt
OpenID AB WG
(Key=value?)
XNS.org
Drummond
Reed
SAML 1.0
OpenID 1.0
Brad Fitzpatrick
OpenID AX
Dick Hardt
OpenID Connect
1.0
1999
2001
2002
2005
2007
2008
2009
2010
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
OAuth 2.0
(Key=value)
Dick Hardt

What we have achieved

ID Token

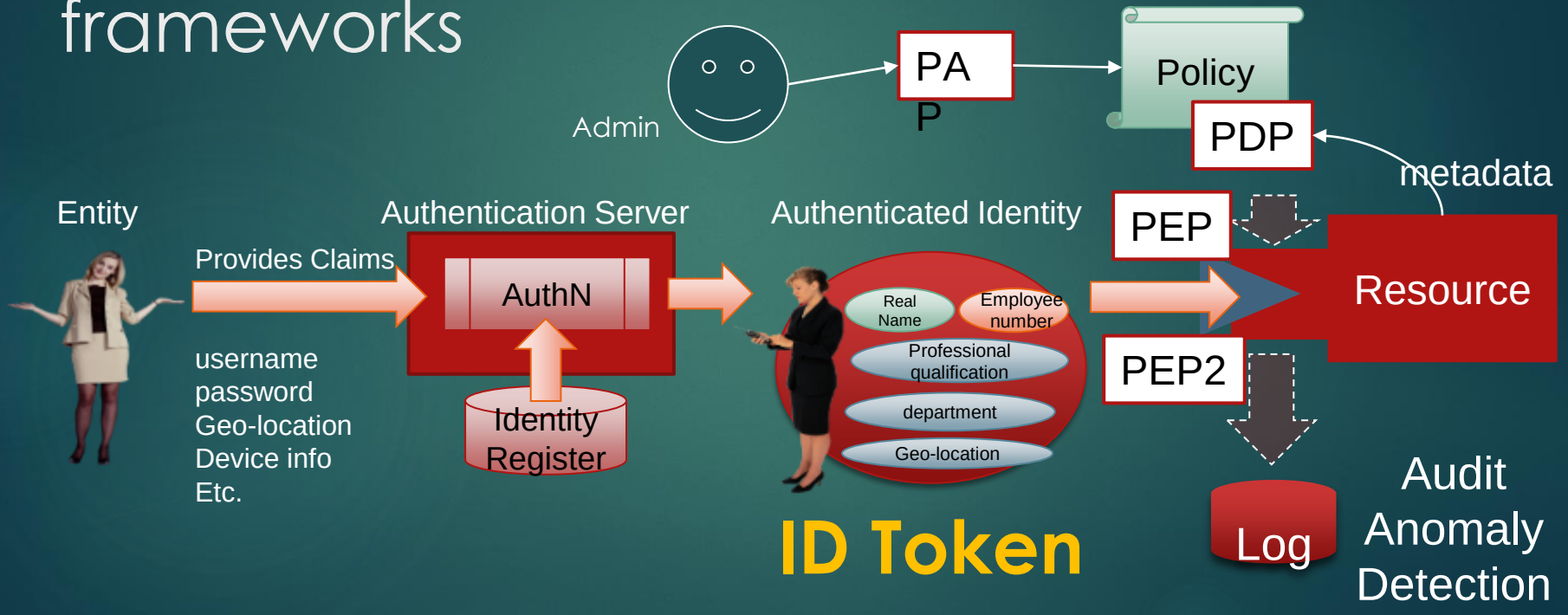
JWS/JWE/JWKS

OAuth 2.0

HTTPS

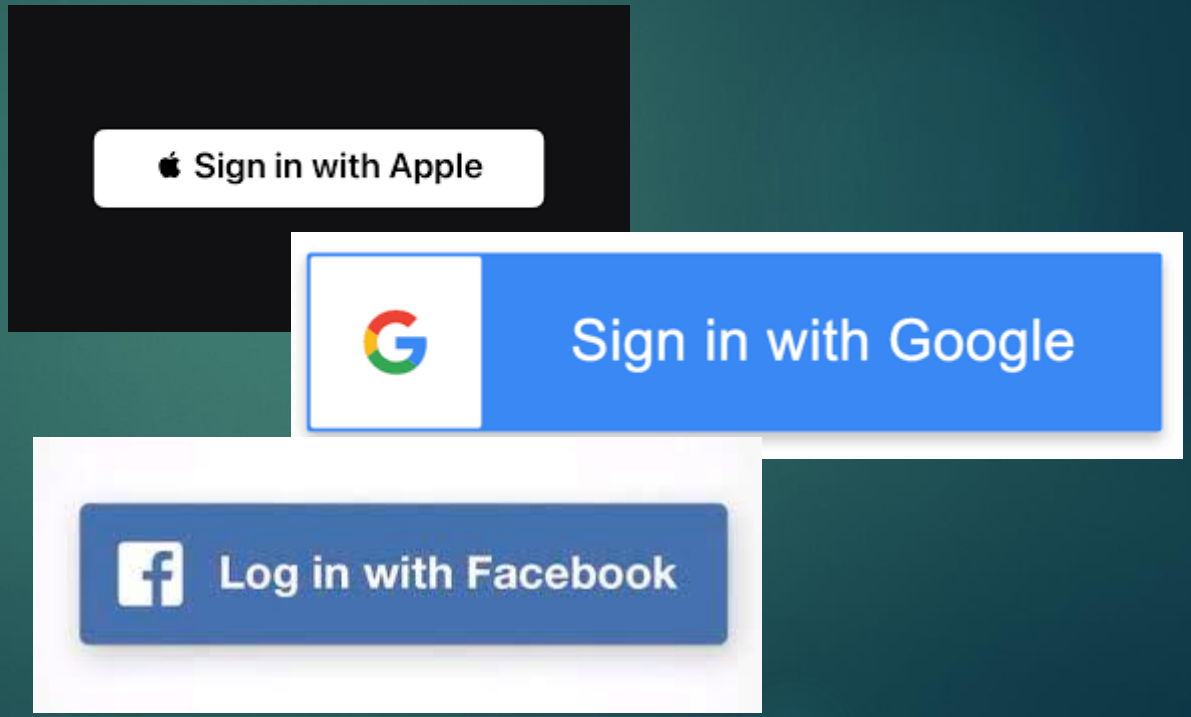
A protocol that defines for a client how to request and for the server to provide the ID Token

That is perfectly fit for modern identity and access control frameworks



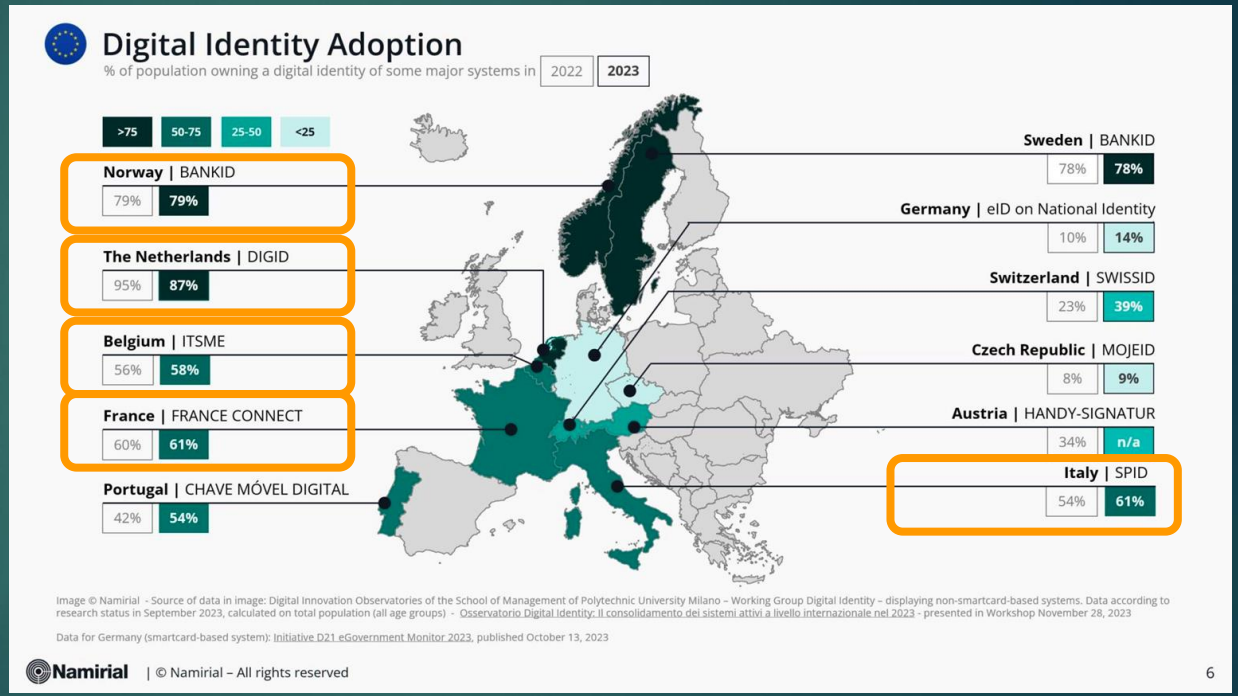
The mainstream federated identity system

- Social Login
- National Identity



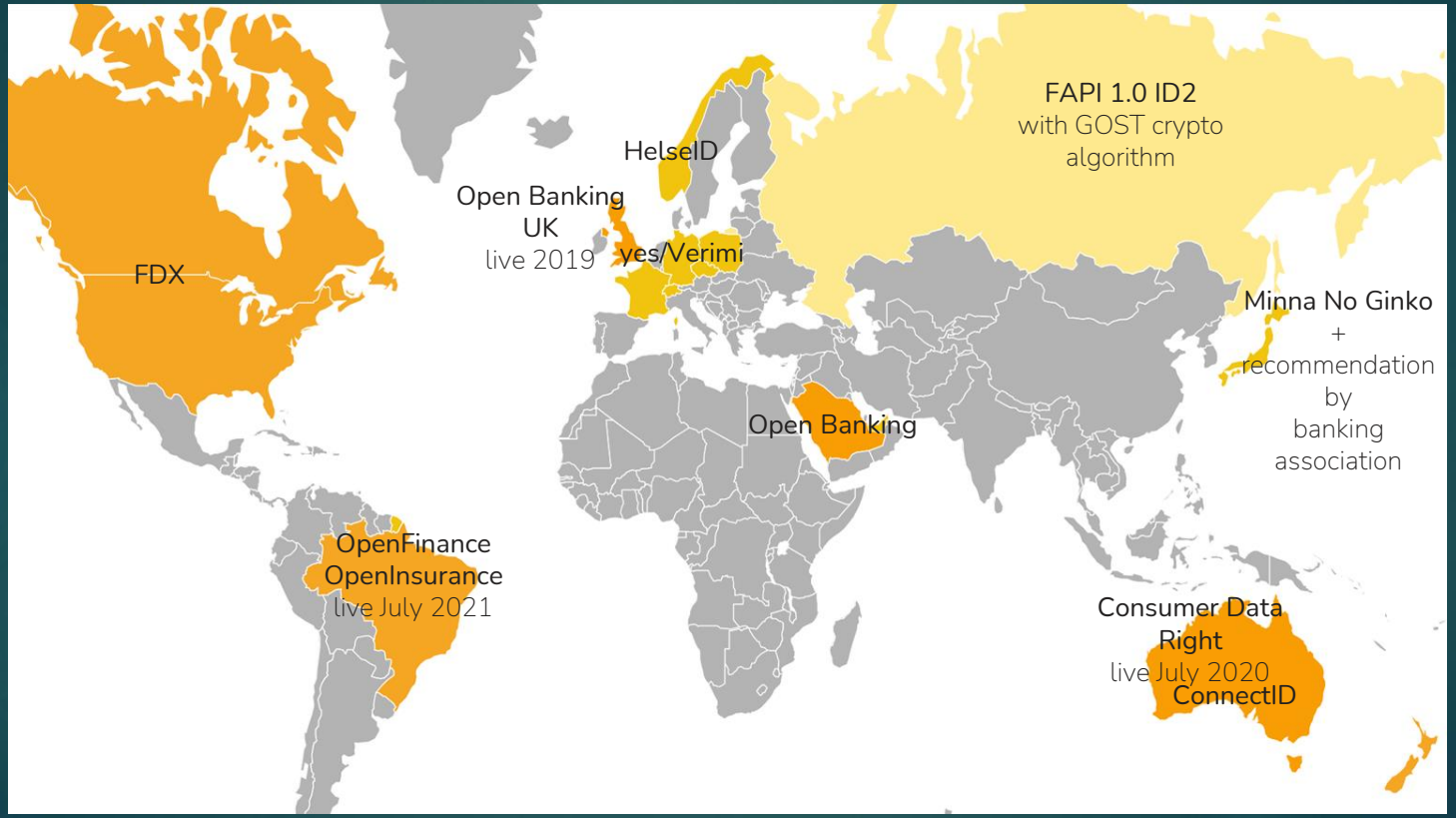
The mainstream federated identity system

- Social Login
- National Identity



(Source) Based on https://www.namirial.com/en/news/state-of-play-on-adoption-of-digital-identity-in-italy-2023-all-roads-lead-to-the-wallets/

Formed the basis of Open Finance



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

開発者のフィードバックに耳を傾ける
解決できなかったことを解決する
正規化しない
シンプルなユースケースのためのデッド・シンプル
セキュリティとプライバシー機能

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

教訓

- 歴史に学べ
- 粘り強さは金～金は粘り強さの素
- シンプルなものはシンプルに
- 開発者の声を聞け
- 成功するまで何度でも繰り返せ
  - ただし、改善しながら
- 序盤では注目を浴びない方が良い
  - 注目は、基礎を固めてから
- テストスイート大事
  - なければ繋がらない
- Formal Analysis 大事 (今日は触れなかったが)
  - 思わぬ落とし穴がある

Youtubeでのフル版
https://bit.ly/4bdWHOG