OpenID

Lessons Learned from OpenID Connect

Torsten Lodderstedt

SPRIND, OWF

What can people in standardization learn from the success of OpenID Connect?

OpenID

- Easy to use - for developers but also for users
- However, OpenID Connect can also be used for complex scenarios - up to LOA High, FAPI
- Cooperation - OpenID Connect was built on top of OAuth and JWT (IETF)
- Amazing interoperability
  - Connect OP: 575, Connect RP: 112
  - conformance testing is standard now at OIDF
- Outstanding security through formal security analysis
  - Systematic and formal security analysis are standard now at OIDF
- Open Standard
- Approachable community

Celebrating Ten Years of OpenID Connect

June 7, 2024

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

OpenID

- 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

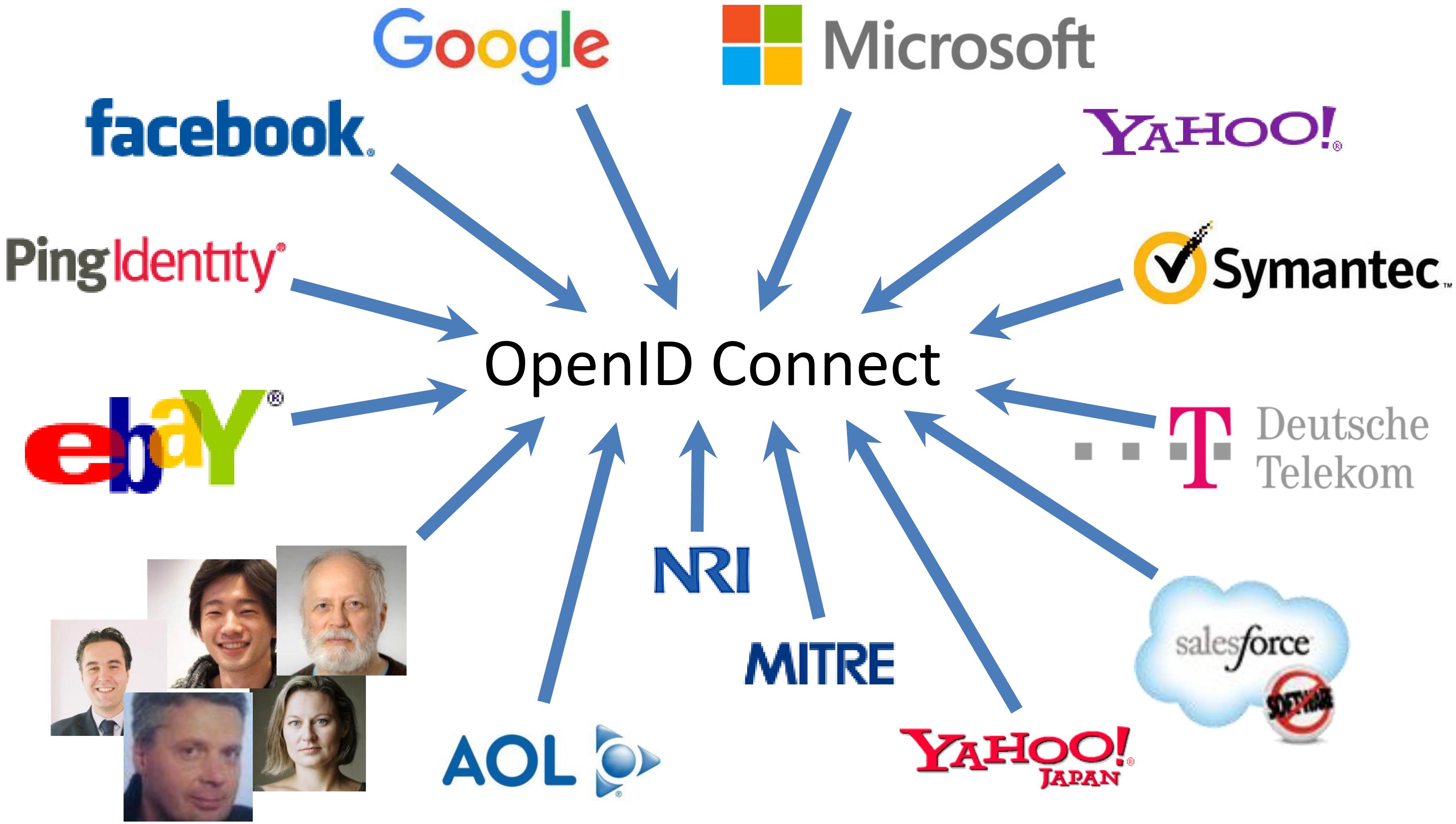
- Keep simple things simple
- Make complex things possible

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



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

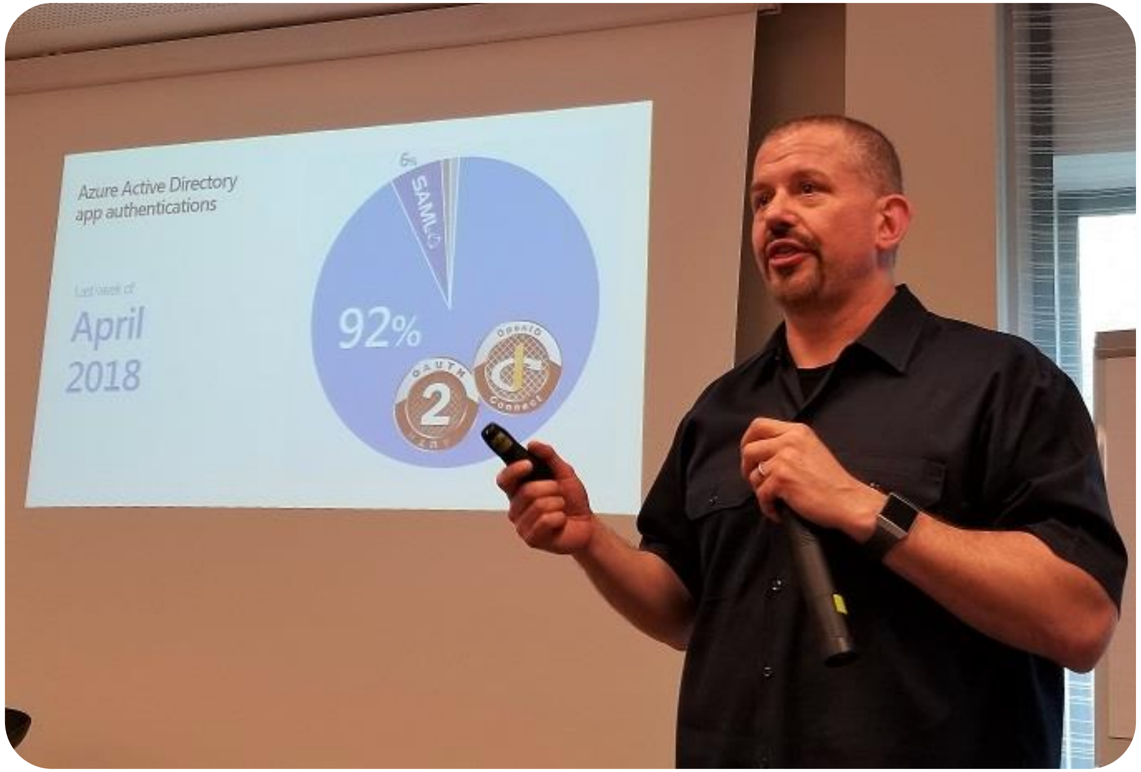
- Indeed, many successful Connect (and OAuth) extensions have been created and deployed
  - Including logout and identity assurance

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

OpenID

- 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

Oh, Its Damn Complex?!

Nat Sakimura

NAT Consulting ETC

_nat
_nat_en

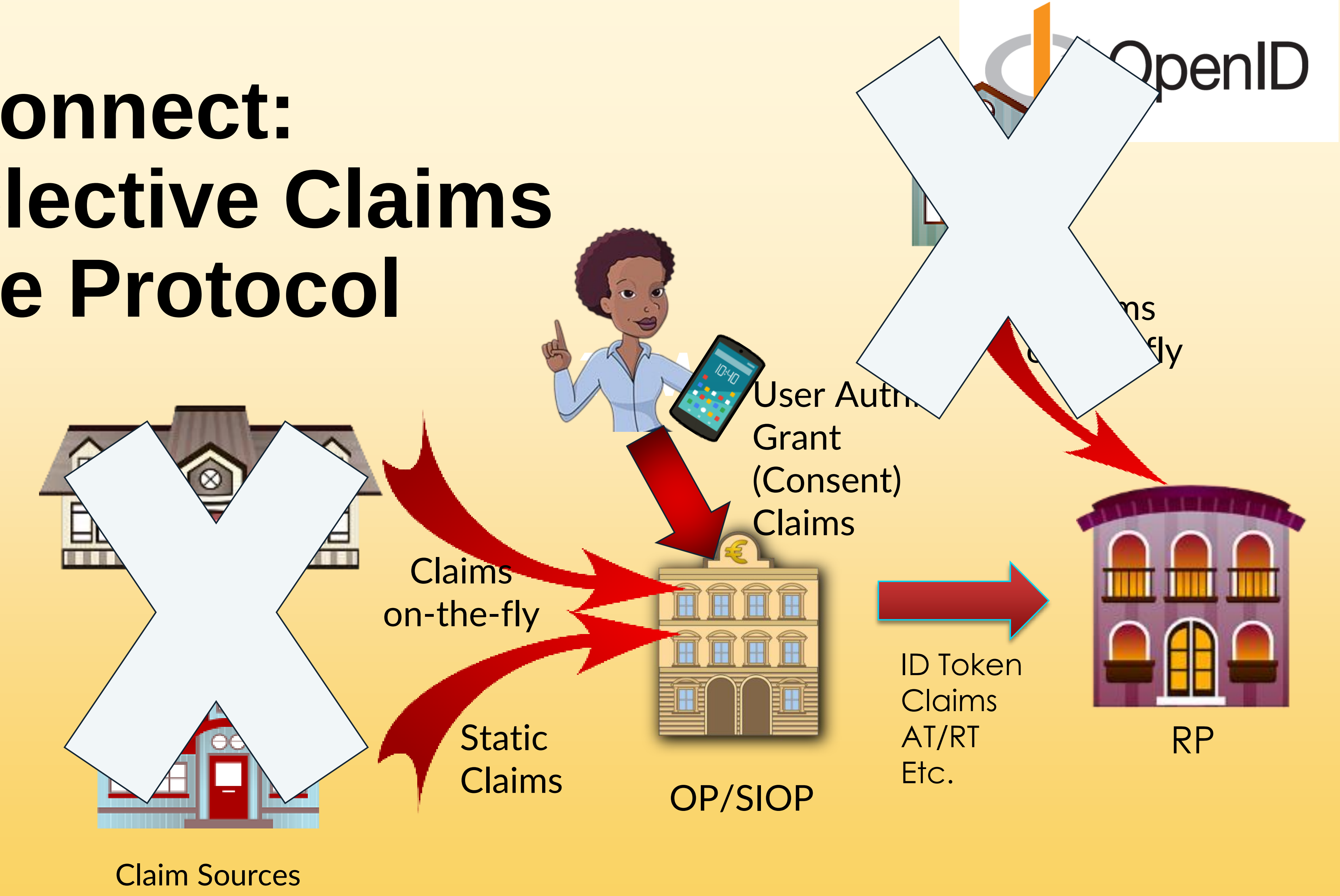
https://www.sakimura.org
https://nat.sakimura.org

https://youtube.com/@NatSakimura

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

OpenID Connect: Online Selective Claims Disclosure Protocol

Which also forms Basis for ABAC.



OpenID

ms

fly

User Auth

Grant

(Consent)

Claims

Claims on-the-fly

Static Claims

OP/SIOP

ID Token

Claims

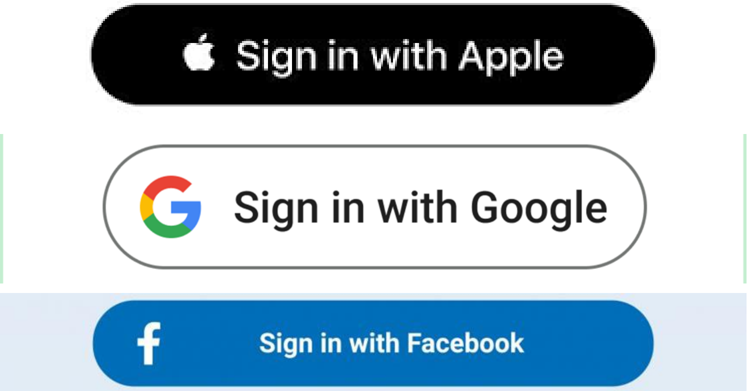
AT/RT

Etc.

RP

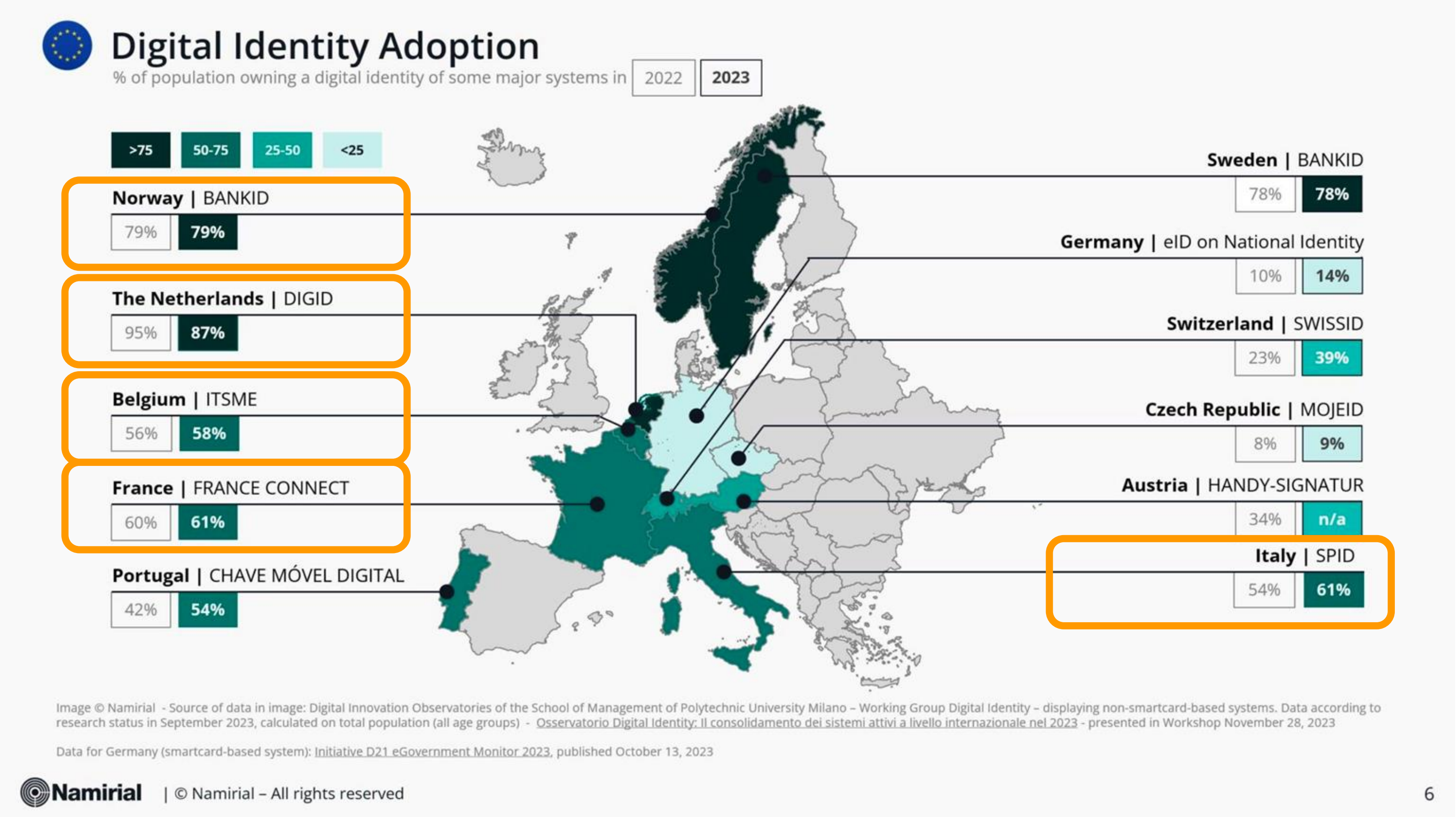
Claim Sources

Used in wide array of use cases



acct:

openid./



Digital Identity Adoption

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

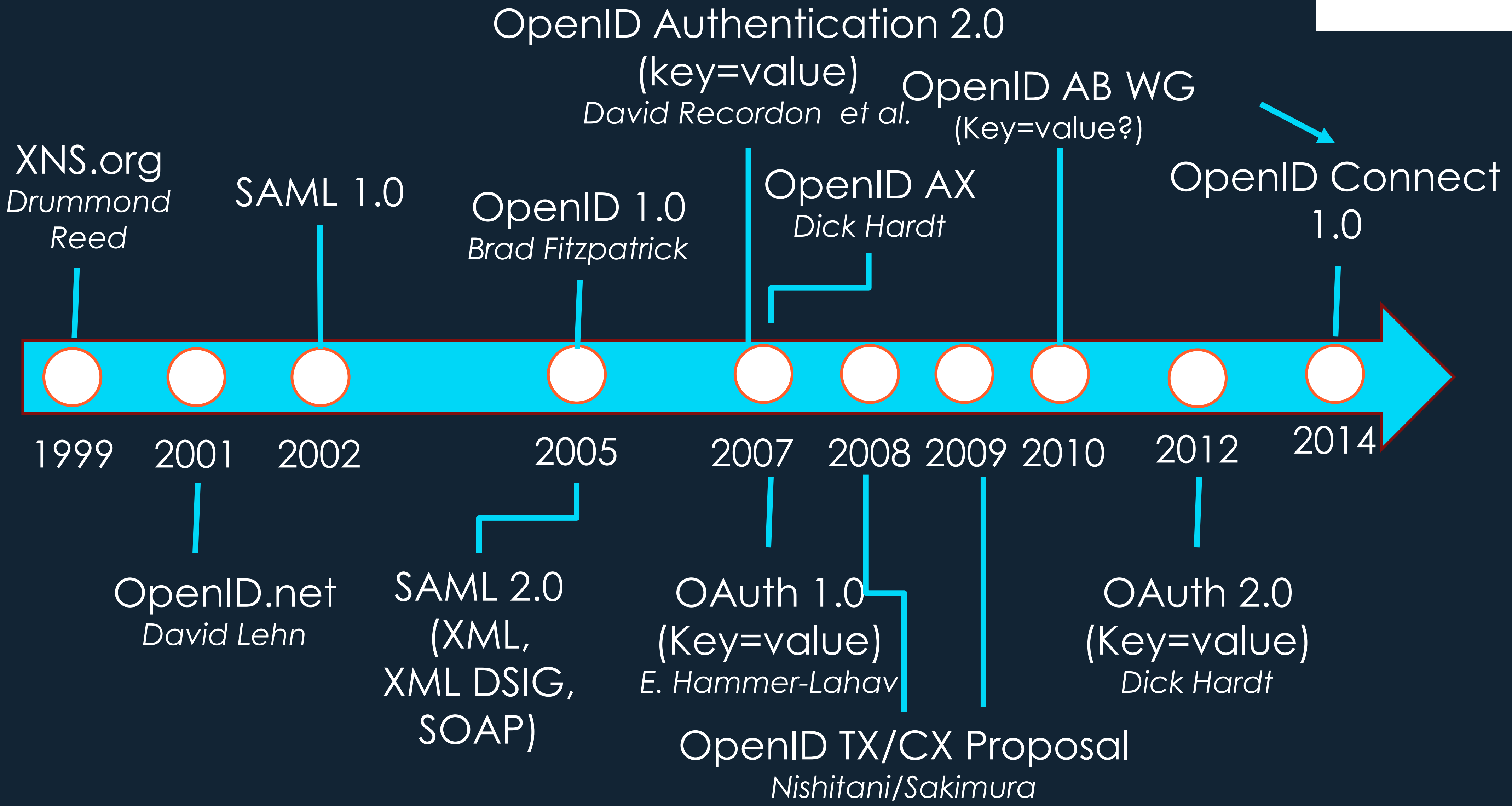
	2022	2023
Norway | BANKID	79%	79%
The Netherlands | DIGID	95%	87%
Belgium | ITSME	56%	58%
France | FRANCE CONNECT	60%	61%
Portugal | CHAVE MÓVEL DIGITAL	42%	54%
Sweden | BANKID	78%	78%
Germany | eID on National Identity	10%	14%
Switzerland | SWISSID	23%	39%
Czech Republic | MOJEID	8%	9%
Austria | HANDY-SIGNATUR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

Learning from the history



XNS.org
Drummond Reed

SAML 1.0

OpenID 1.0
Brad Fitzpatrick

OpenID Authentication 2.0
(key=value)
David Recordon et al.

OpenID AX
Dick Hardt

OpenID AB WG
(Key=value?)

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

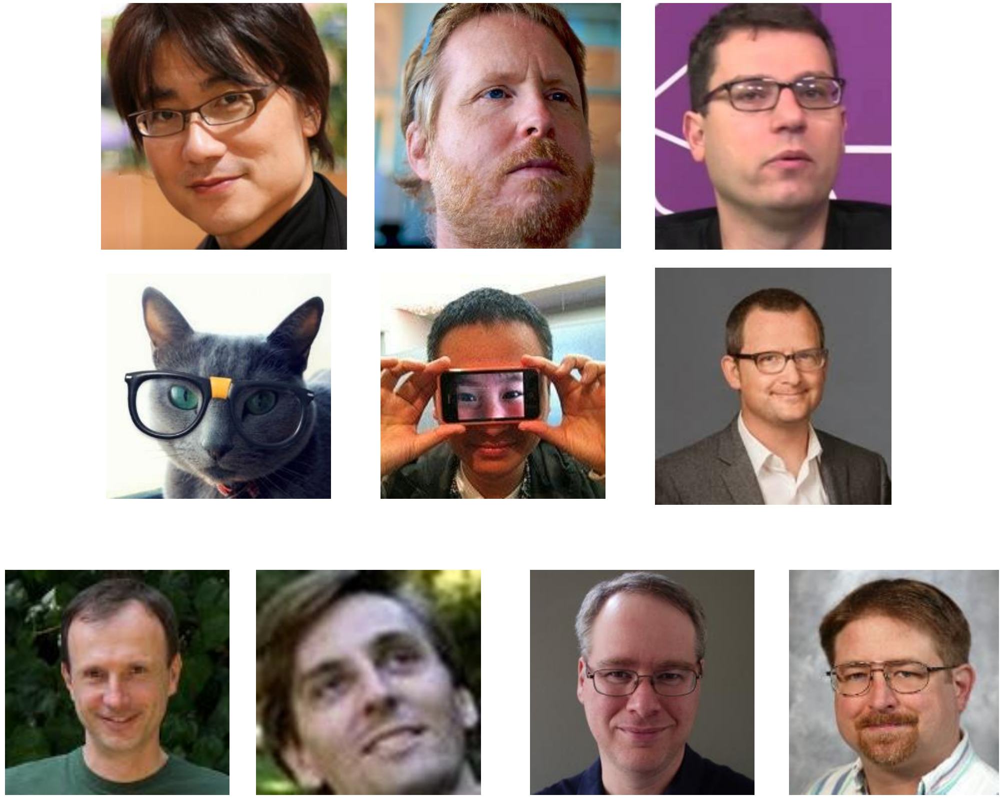
OAuth 2.0
(Key=value)
Dick Hardt

Early design decisions:

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

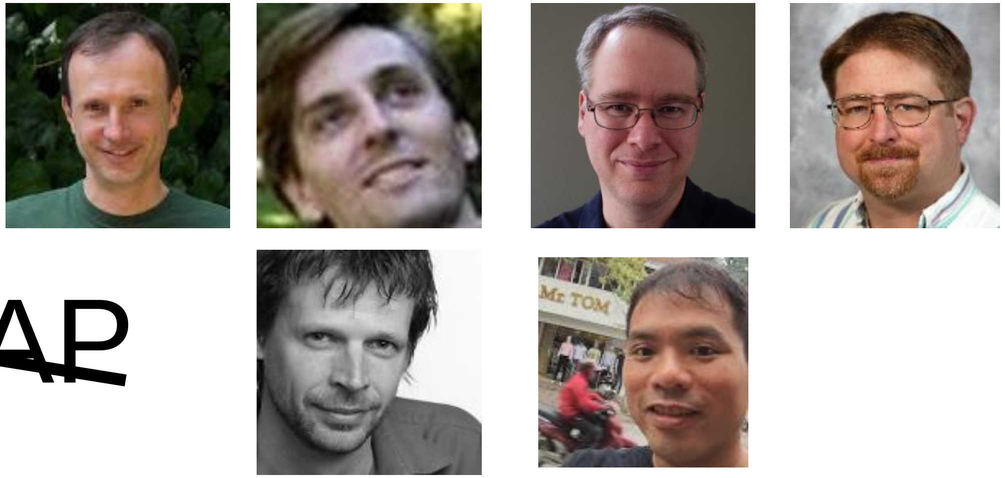
Early design decisions:

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



Early design decisions:

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



Features not widely used or seen

1. Aggregated and Distributed Claims
2. Granular Claims Request
3. Essential/Optional Claims
4. AcctURI
5. policy_url
6. Request Object (Started to see this only after FAPI)

Oh,

It's

Damn

Complex

What lessons we learned that could apply to other initiatives

- Be persistent - till you succeed
- Learn from history
    - Fix what was not done well
    - Find the developer pain and solve it
- Make it simple to read, simple to implement for the minimum viable case

OpenID

OpenID: There is no spoon

John Bradley

Principal Architect, Yubico

a.k.a. Mercenary

OpenID is more than a single specification or Idea

Insert insightful comment….