RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: IDY-W11

Managing Self-Sovereign Identities: A Relying Party Perspective

George Fletcher

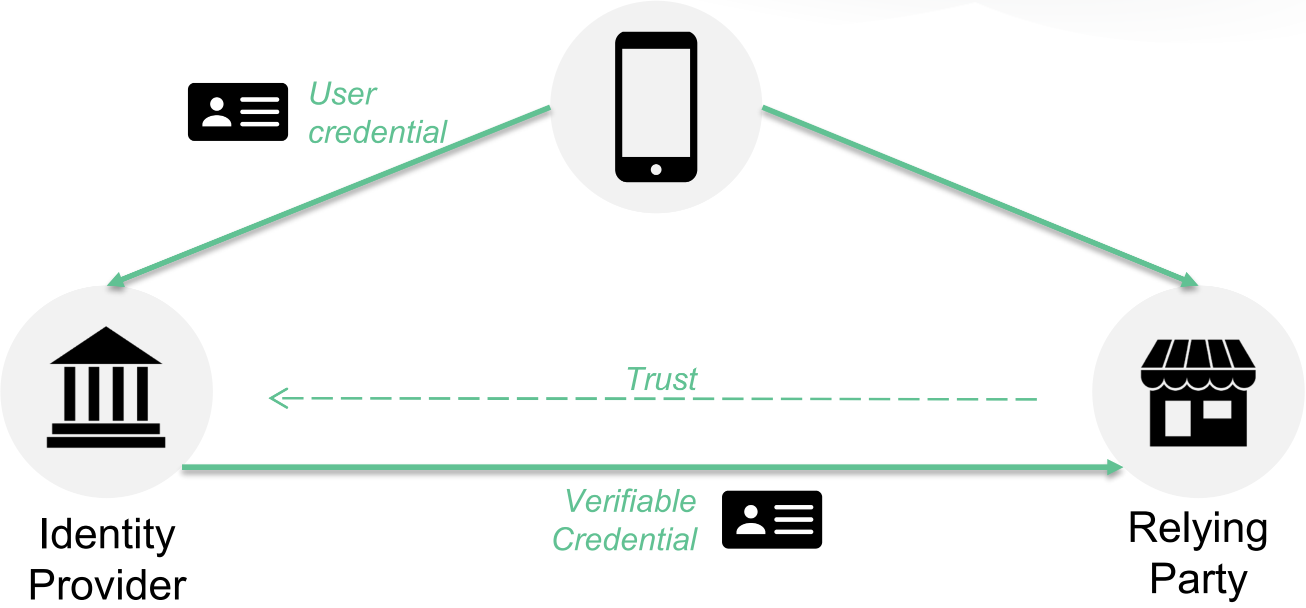
Identity Standards Architect
Verizon Media Inc.
@gffletch

#RSAC

Introduction

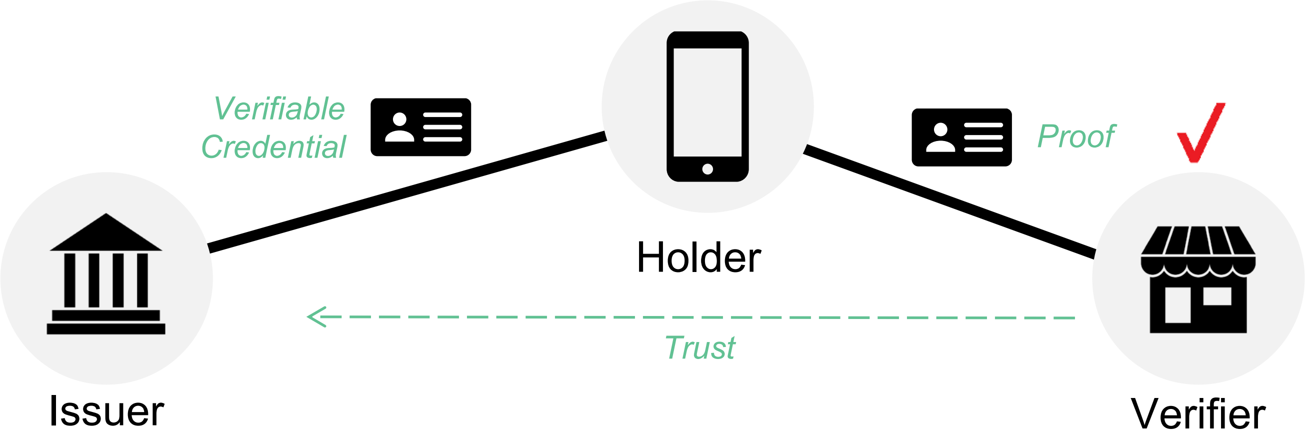
Quick SSI Introduction

Federated Identity Model



What is Self-Sovereign Identity?

High Level SSI Model



Decentralized Identifier -- DID

did:example:123456789abcdefghi →

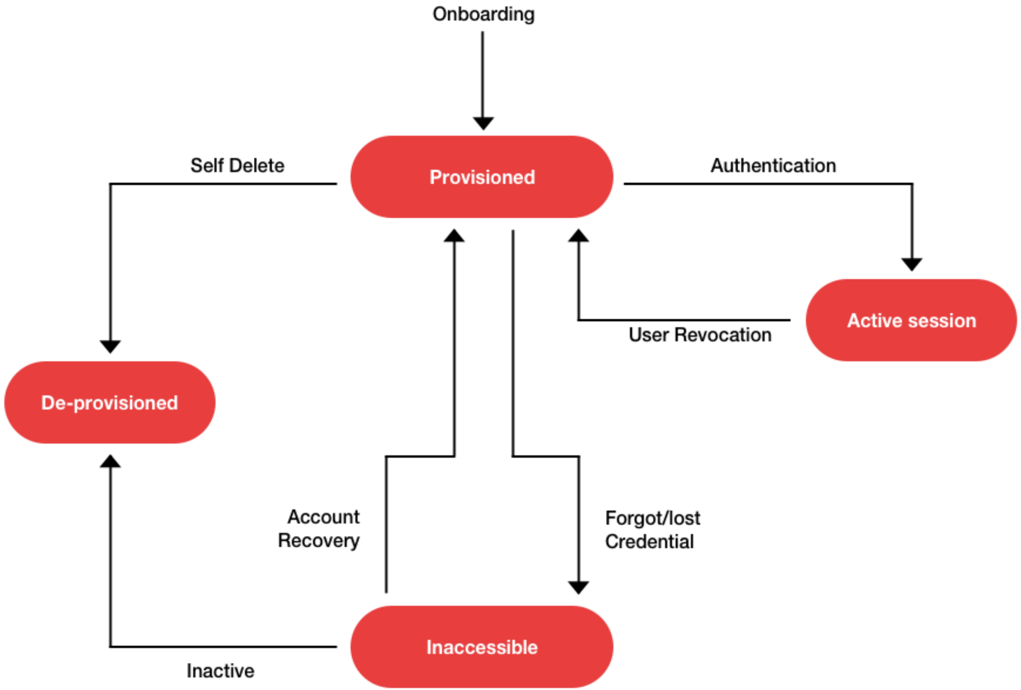
```
{
 "@context": "https://w3id.org/did/v1",
 "id": "did:example:123456789abcdefghi",
 "authentication": [{
   // this key can be used to authenticate as did:...fghi
   "id": "did:example:123456789abcdefghi#keys-1",
   "type": "RsaVerificationKey2018",
   "controller": "did:example:123456789abcdefghi",
   "publicKeyPem": "-----BEGIN PUBLIC KEY...END
PUBLIC KEY-----\r\n"
 }],
 "service": [{
   "type": "ExampleService",
   "serviceEndpoint":
"https://example.com/endpoint/8377464"
 }]
}
```

Why change the model?

- Better end-to-end cryptographic trust
- Possible privacy concern with the Federated Identity Provider knowing where (which sites) the user is authenticating
  - Also which claims were presented to that relying party
- Easy conceptual model for users

Relying Parties

Relying Party Life-Cycle Management



Identifier indirection at the RP

Identities

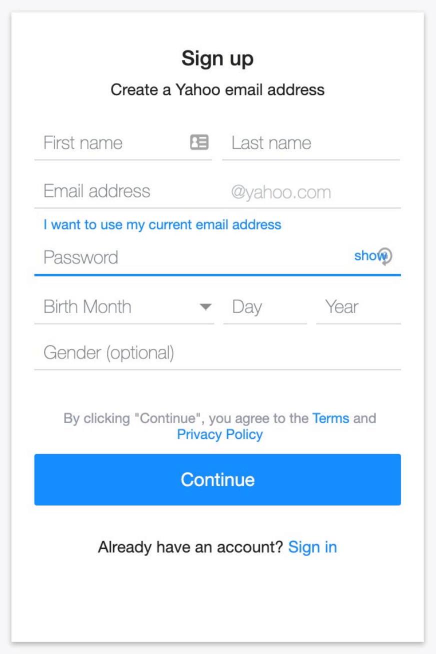
RPID	First Name	Last Name	Gender	…
1234	George	Fletcher	Male	…

IDP	Username	AuthN	Credential	RPID
SSI	gffletch	DID-Auth	DID	1234
Google	13443453	OIDC		2345

Credentials

Registration

Common Pattern: Registration



Sign up

Create a Yahoo email address

First name | Last name

Email address @yahoo.com

I want to use my current email address

Password show

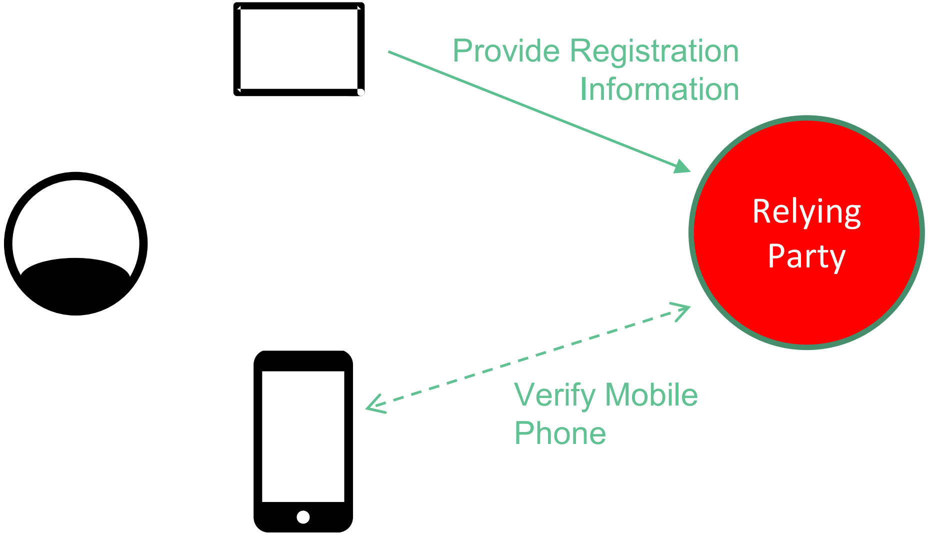
Birth Month | Day | Year

Gender (optional)

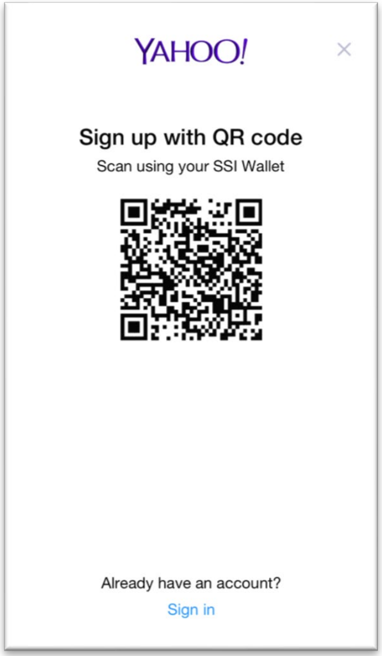
By clicking "Continue", you agree to the Terms and Privacy Policy

Continue

Already have an account? Sign in



Possible SSI Registration Flow

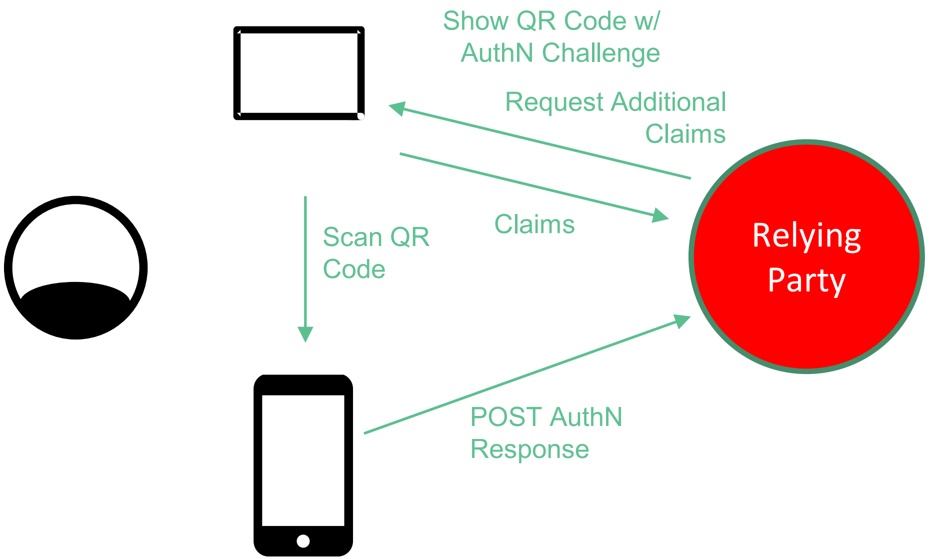


Sign up with QR code

Scan using your SSI Wallet

Already have an account?

Sign in



What’s Different: Data / Claims / Attributes

Data Availability

- What to require/request?
- Zero Knowledge Proofs

Verified vs Unverified

- Which claims can be self -asserted?
- Which claims does the RP want to be verifiable?
- Who do you trust to verify a claim?

Lessons learned from the OpenID Connect rollout

What’s Different: Protocol

Challenge / Response for registration

- Based on DID -Auth
- UX is closer to a “social login” or federation flow for registration

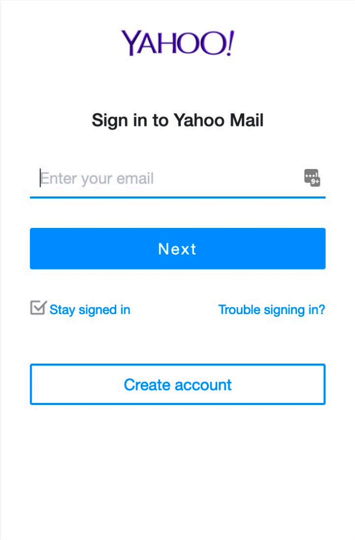
Lack of standardization

- No standard for requesting claims

RSAConference2020

Authentication

Common Pattern: Authentication



YAHOO!

Sign in to Yahoo Mail

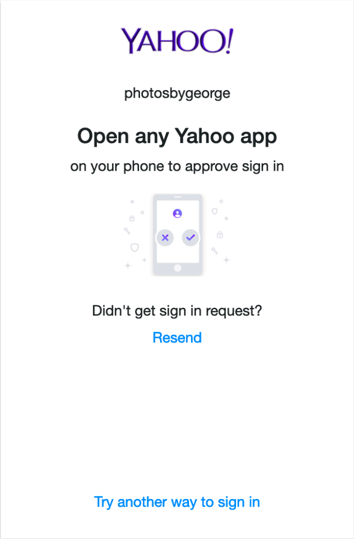
Enter your email

Next

☑ Stay signed in

Trouble signing in?

Create account



YAHOO!

photosbygeorge

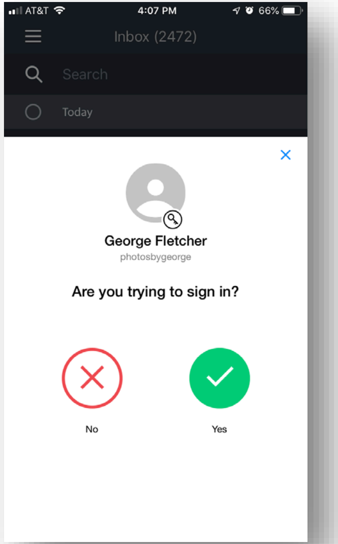
Open any Yahoo app

on your phone to approve sign in

Didn't get sign in request?

Resend

Try another way to sign in



AT&T 4:07 PM 66%

Inbox (2472)

Search

Today

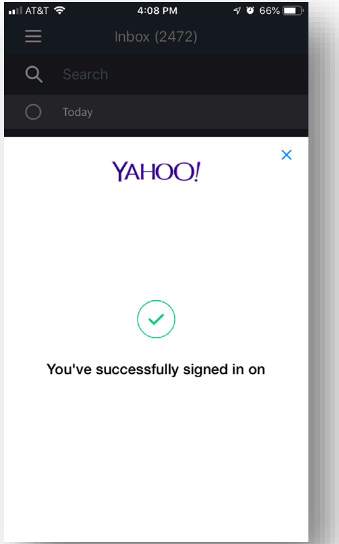
George Fletcher

photosbygeorge

Are you trying to sign in?

No

Yes



AT&T 4:08 PM 66%

Inbox (2472)

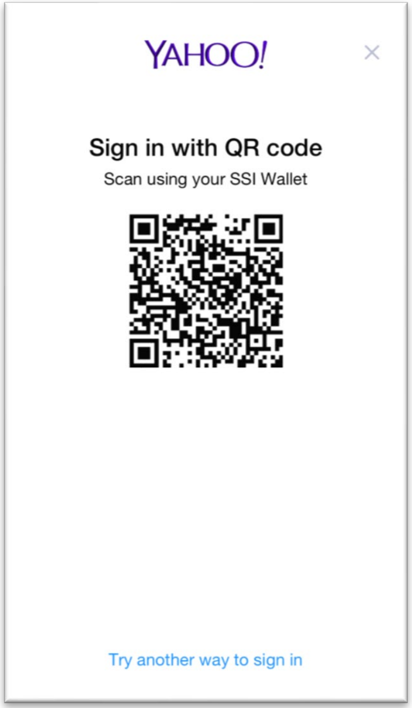
Search

Today

YAHOO!

You've successfully signed in on

Possible SSI Authentication Flow

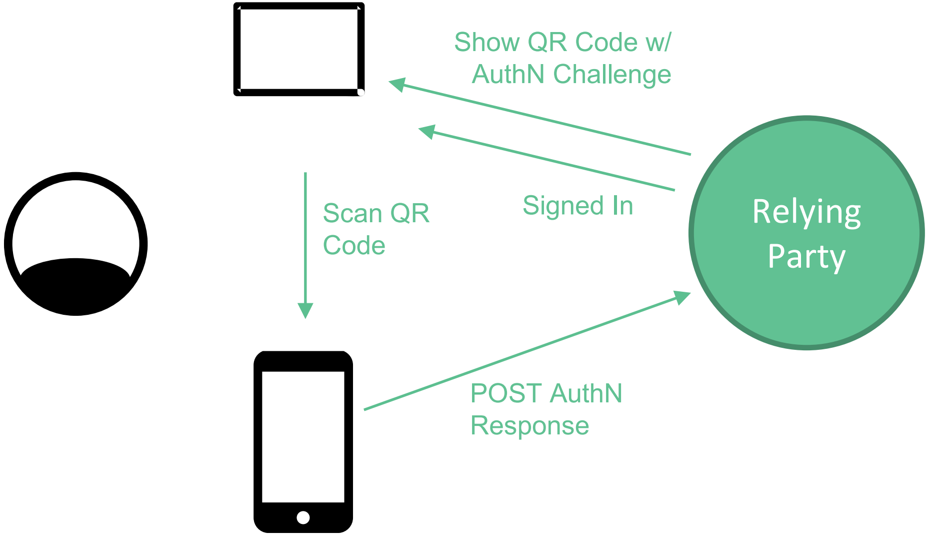


YAHOO!

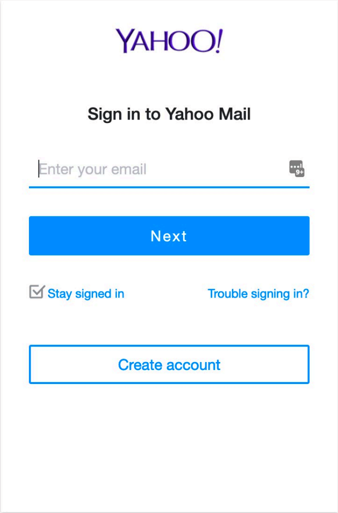
Sign in with QR code

Scan using your SSI Wallet

Try another way to sign in



Possible SSI Authentication Flow



YAHOO!

Sign in to Yahoo Mail

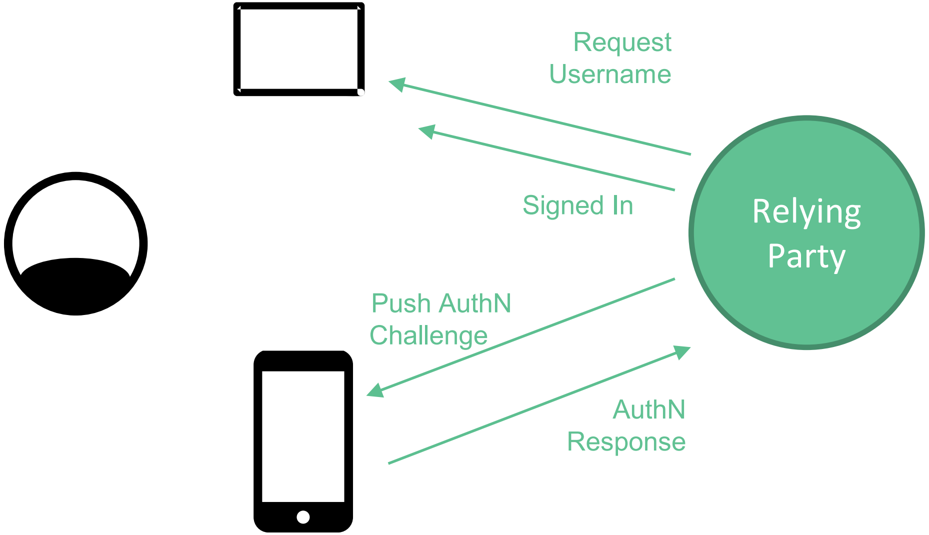
Enter your email

Next

☑ Stay signed in

Trouble signing in?

Create account



What’s Different: Protocol

Authentication Protocol

- Can use an “identifier first” flow to make the UX very similar
- Options for direct connection to the SSI “wallet” (Agent)

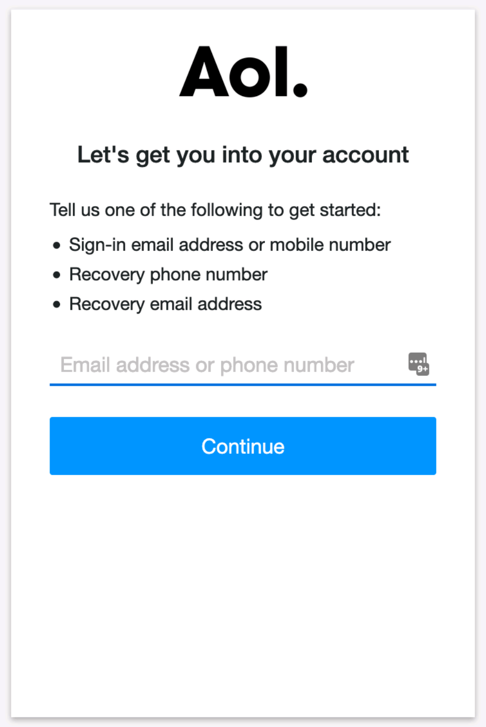
Lack of standardization

- DID-Auth defines the structure of the flow
- Each DID method defines its own syntax

Should multiple authentication methods be supported?

Account Recovery

Common Pattern: Account Recovery

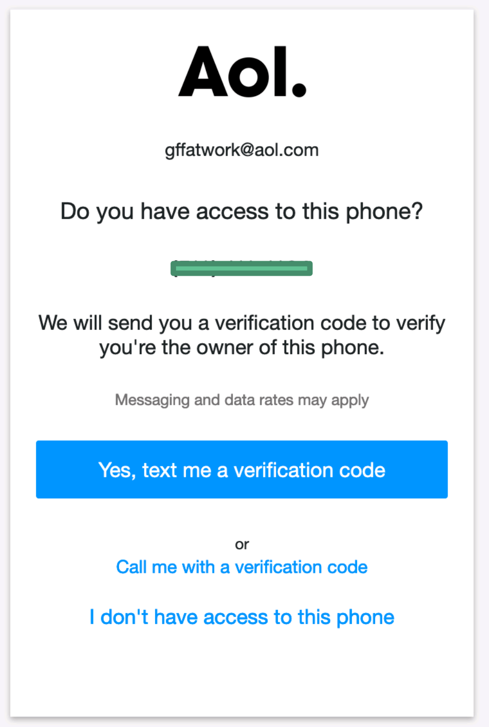


Aol.

Let's get you into your account

Tell us one of the following to get started:

- Sign-in email address or mobile number
- Recovery phone number
- Recovery email address



Aol.

gffatwork@aol.com

Do you have access to this phone?

[redacted]

We will send you a verification code to verify you're the owner of this phone.

Messaging and data rates may apply

Yes, text me a verification code
or
Call me with a verification code
I don't have access to this phone

Possible SSI Account Recovery Flow

This Page Intentionally Left   blank

What’s Different: Recovery Methods

Current SSI defined methods

- back up private keys (e.g. DON’T LOSE THEM)

Is this really viable for a relying party?

- What about purchase recovery via credit -card on file?

What are the implications of allowing other recovery methods?

What are the best methods to use?

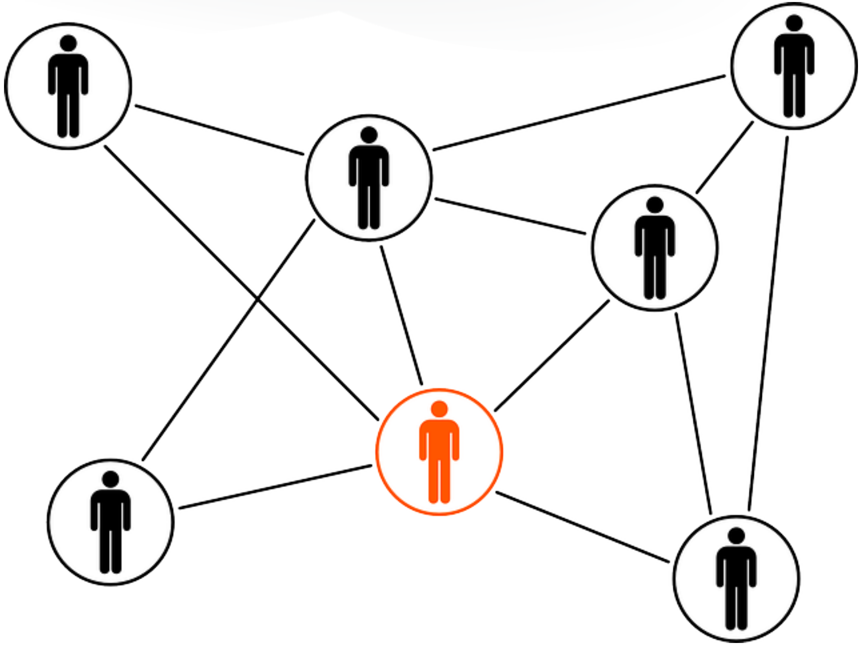
Account Linking

Account Linking

Connecting SSI identities to existing users:

- Normal user authN + DID-Auth and then a link action
- RP needs to link the DID as a valid identifier (alias) on the user’s existing identity

Is this a registration time only event? If so, how does the RP offer this to the user?



RSAConference2020

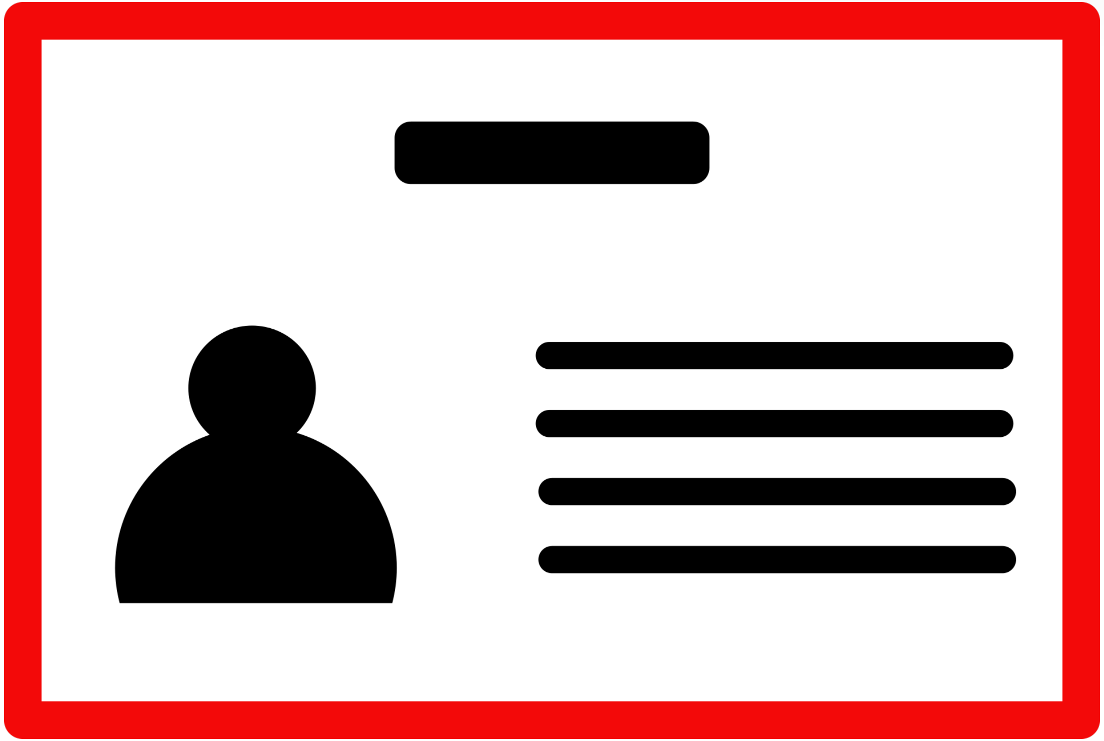
Privacy

The Coffee Shop Chronicles

Recognize & Serve

Trust

Selective Disclosure



RSAConference2020

Other Topics

Fraud / Anti-abuse

Opportunities

Relying Parties will need to…

Final Thoughts

- Support both identity models in parallel
- Minimize infrastructure impact
- Deal with rapid innovation in the space
- Handle the lack of standardization in the near term

Treat the Self -Sovereign Identifier (DID) as a reference to the RP Identity

Q&A

George Fletcher
Identity Standards Architect

george.fletcher@verizonmedia.com