

# **RSA**Conference2022

San Francisco & Digital | June 6 – 9

## **TRANSFORM**

SESSION ID: IDY-W09

## **Managing Decentralized Identities: A Relying Party Perspective**

**George Fletcher**

Identity Standards Architect  
Capital One  
@gffletch



# Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.



# Introduction

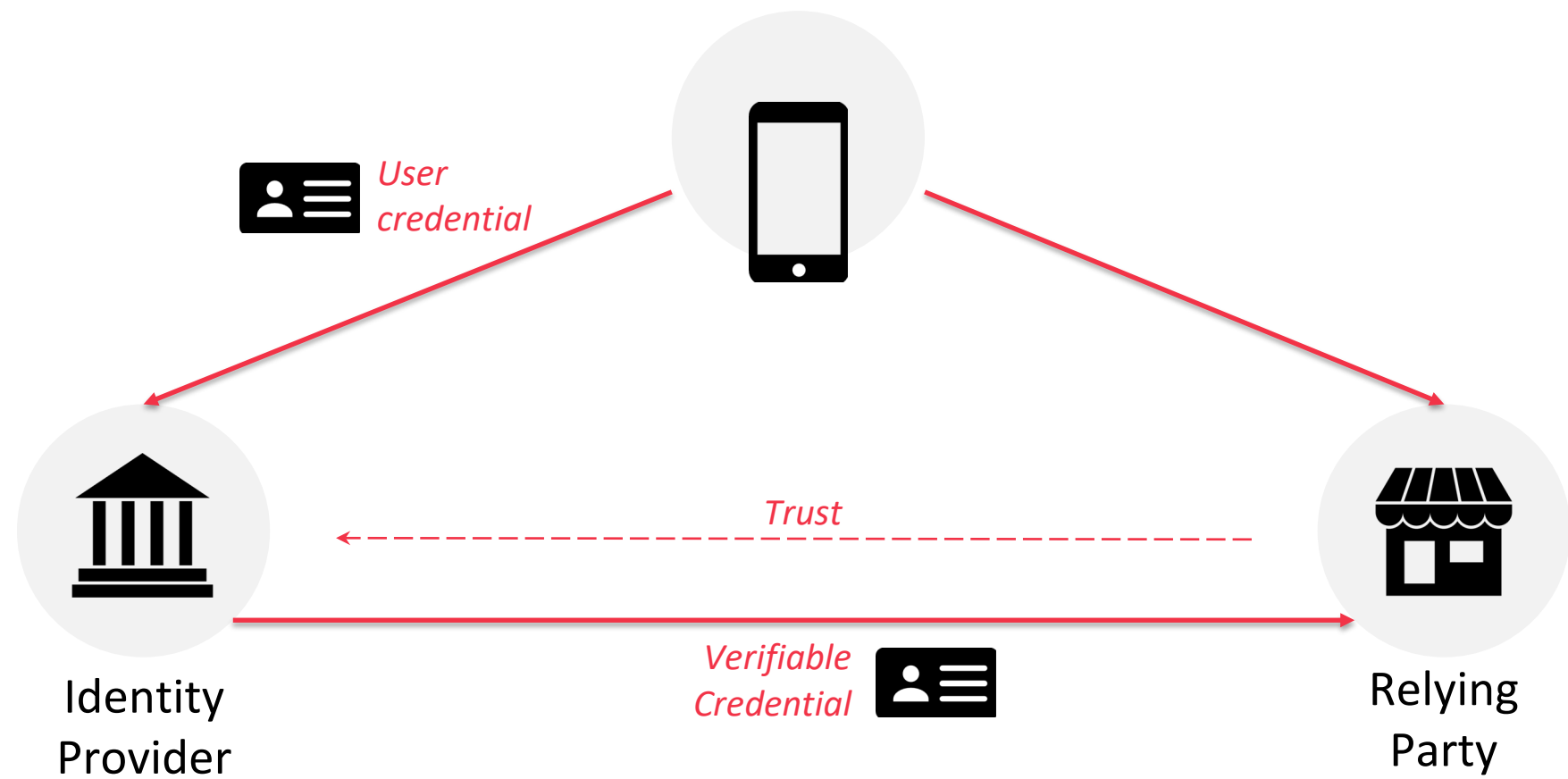


# RSA<sup>®</sup>Conference2022

## Identity Patterns



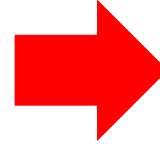
# Federated Identity Model



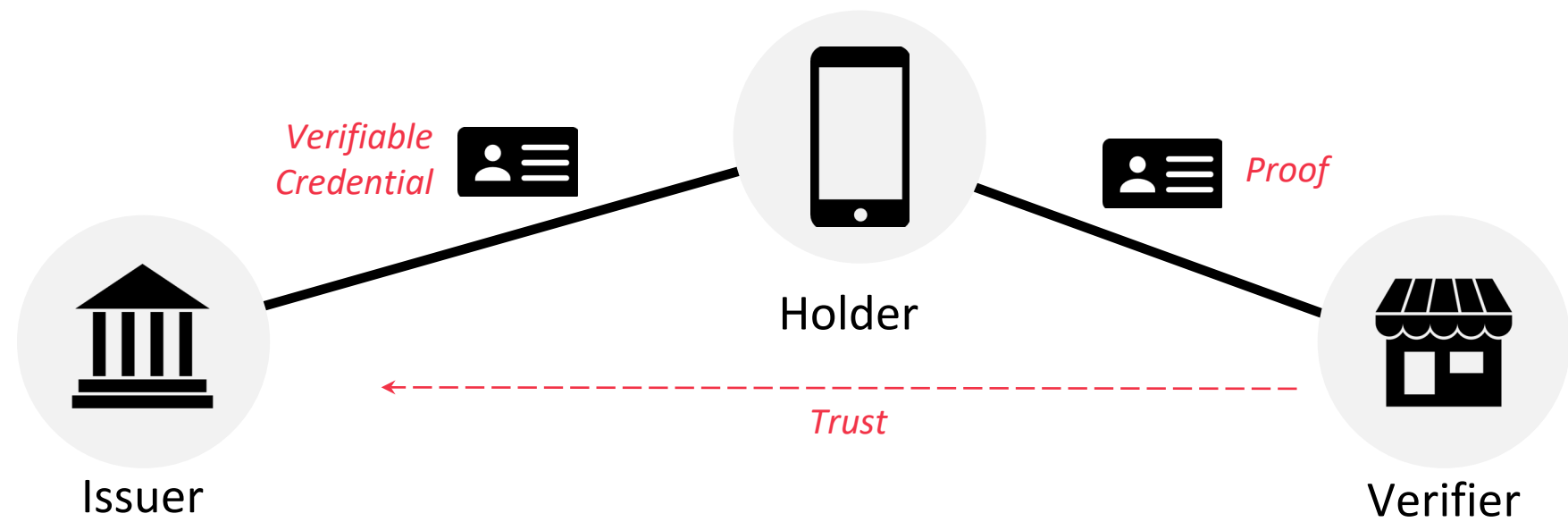


# What is Decentralized Identity?

#RSAC



# High Level Decentralized Identity 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?

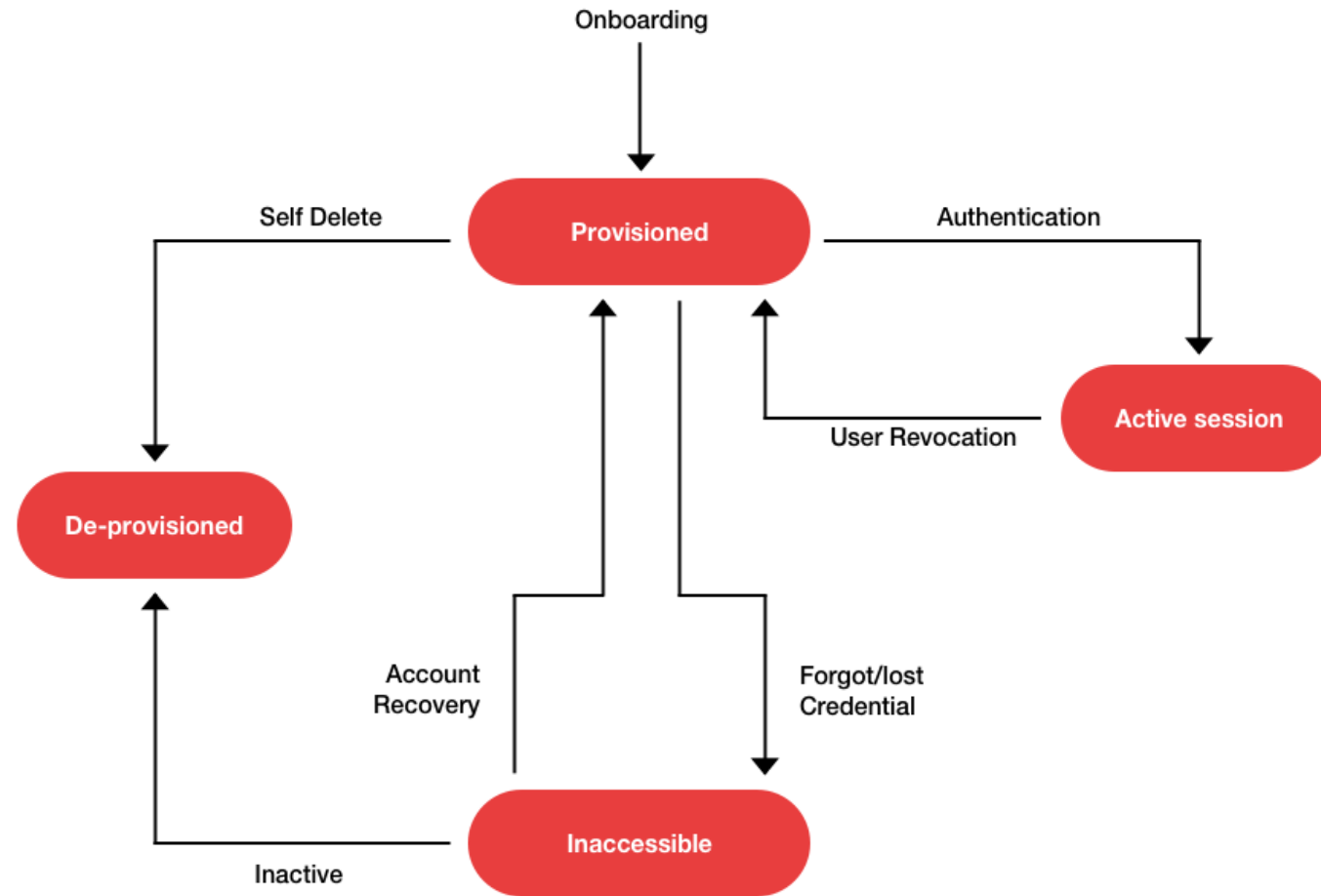
- Better end-to-end cryptographic trust
- Possible privacy concern with the Federated Identity Provider knowing where (which sites) the user is authenticating
  - Also which claims were presented to that relying party
- Easy conceptual model for users

# RSA<sup>®</sup>Conference2022

## 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



# RSA<sup>®</sup>Conference2022

## Registration



# Common Pattern: Registration

## Sign Up

Create your account

First name

Last name

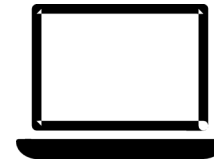
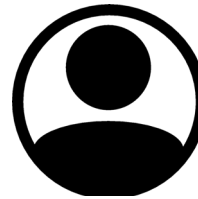
Email address

Password

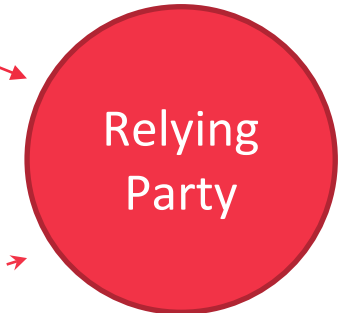
☐ I've read and agree to the [Terms & Conditions](#) and [Privacy Policy](#).

Continue

Already have an account? [Sign in instead](#)

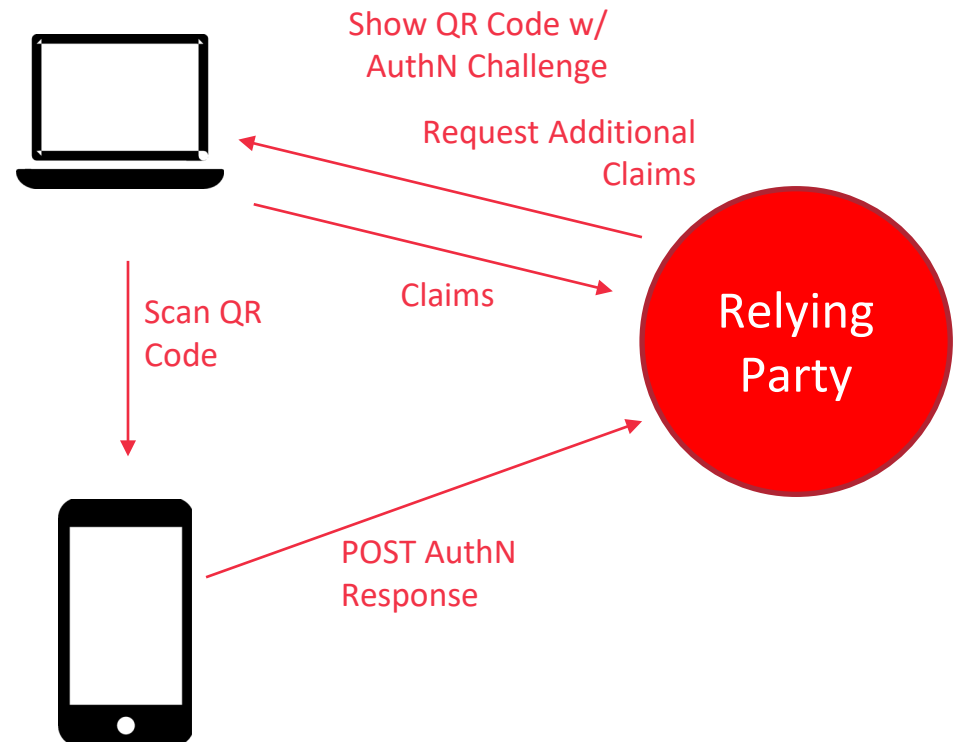
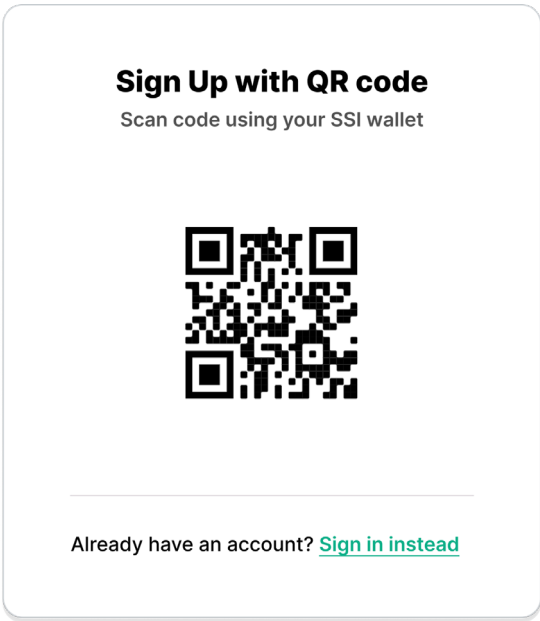


Provide Registration Information



Verify Mobile Phone

# Possible SSI Registration Flow



# 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

- Not “redirect based”; passive action by the RP (e.g. show QR code)
- UX and Consent managed by the user’s wallet
- New protocols being developed in multiple organizations
- OpenID Foundation is working on a number of specifications to help in this space
  - [Self-Issued OpenID Provider v2](#)
  - [OpenID Connect for Verifiable Presentations](#)
- Decentralized Identity Foundation
  - [Presentation Exchange 2.0.0](#)

Lack of wallet content knowledge

# RSA<sup>®</sup>Conference2022

## Authentication



# Common Pattern: Authentication

### Sign in

Sign in to your account

Email address

---

☐ Keep me signed in

[Continue](#)

[I forgot my password](#)

Don't have an account? [Sign up now](#)

### Authenticate in the App

Open your authenticator app to confirm this sign in attempt

Request didn't come through?

[Send again](#)

---

Not working? [Sign in another way](#)

9:41

**Confirm sign in attempt**


Someone is attempting to sign in to your account from Falls Church, VA.

Chrome on MacOS at 9:40 am

[No, that was not me](#)

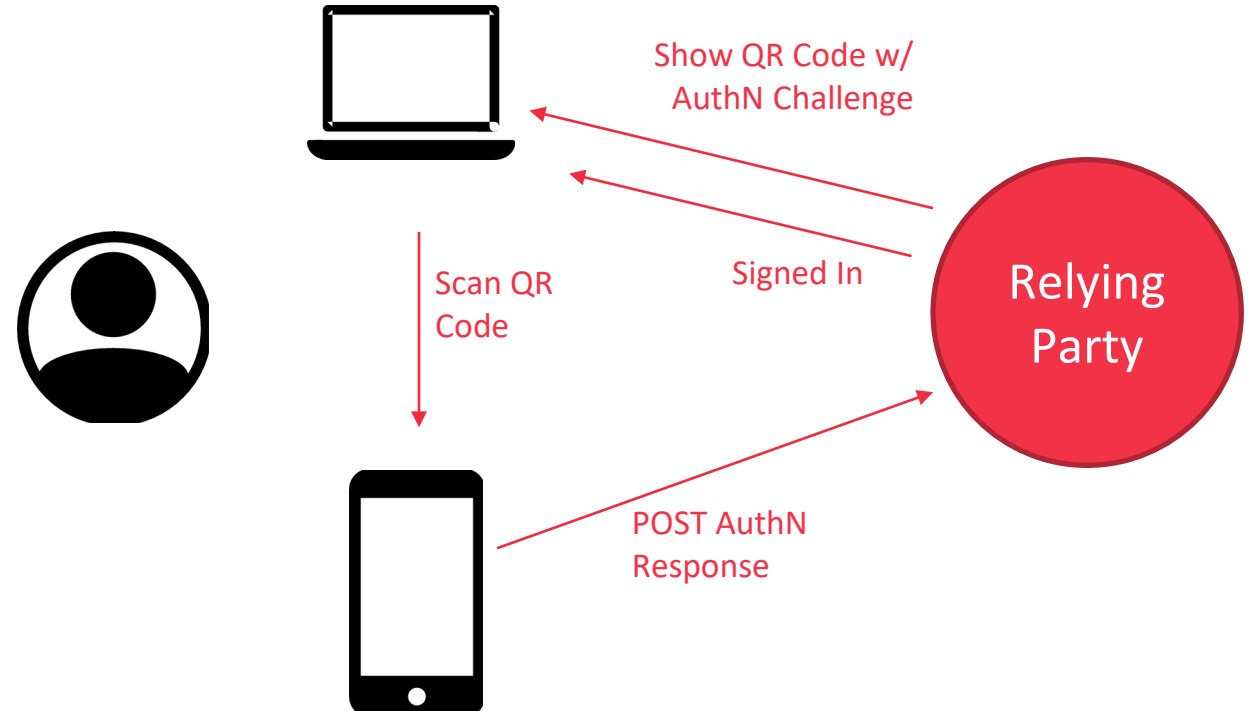
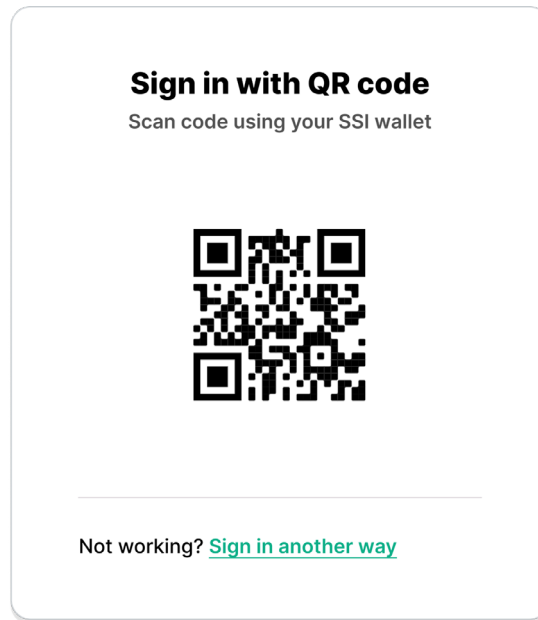
[Yes, that's me](#)

9:41



We've signed you in.

# Possible SSI Authentication Flow





# Possible SSI Authentication Flow

**Sign in**  
Sign in to your account

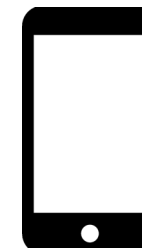
Email address

☐ Keep me signed in

Continue

[I forgot my password](#)

Don't have an account? [Sign up now](#)



Request  
Username

Signed In

Push AuthN  
Challenge

AuthN  
Response

Relying  
Party

# 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)

## Standardization

- OpenID Foundation: Self-Issued OpenID Provider v2 (SIOPv2)
- Decentralized Identity Foundation: DID Authentication
  - Merged work with the OpenID Foundation in December 2020

Should multiple authentication methods be supported?

# RSA<sup>®</sup>Conference2022

## Account Recovery



# Common Pattern: Account Recovery

**Reset Password**

Email address

Continue

[Recover my account another way](#)

**Reset Password**

Check your email for a link to reset your password and recover your account.

[Recover my account another way](#)



# 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)
- Back up mechanism defined by the Wallet provider

## 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?

# RSA<sup>®</sup>Conference2022

## Account Linking

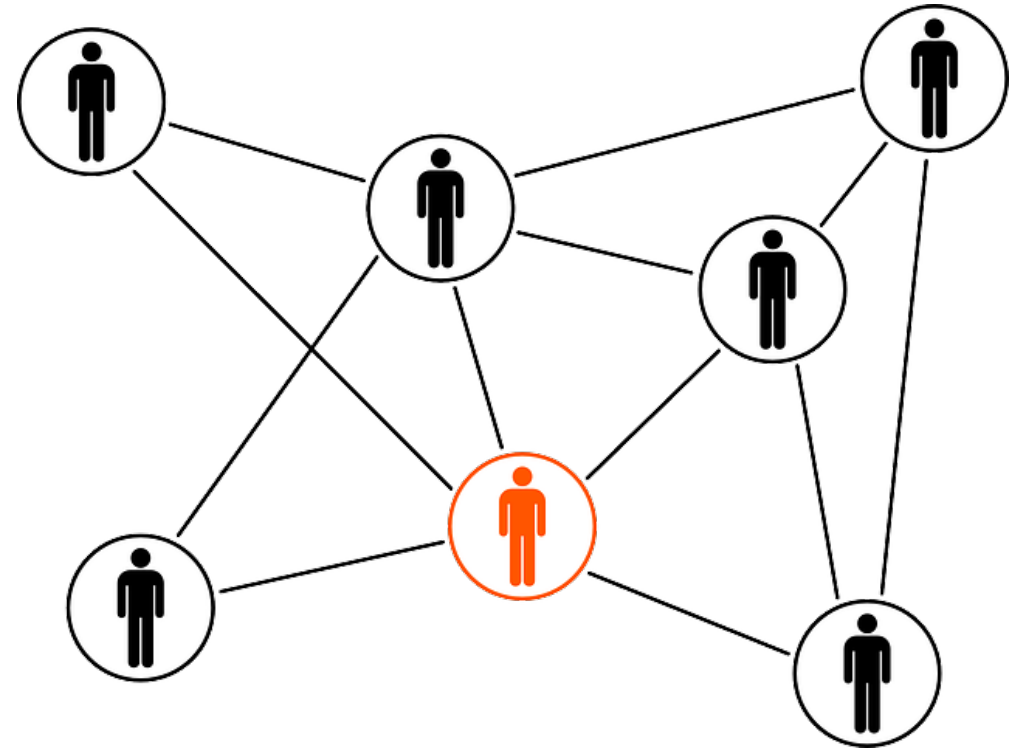


# Account Linking

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?



# RSA<sup>®</sup>Conference2022

## Privacy





# The Coffee Shop Chronicles



# Recognize & Serve

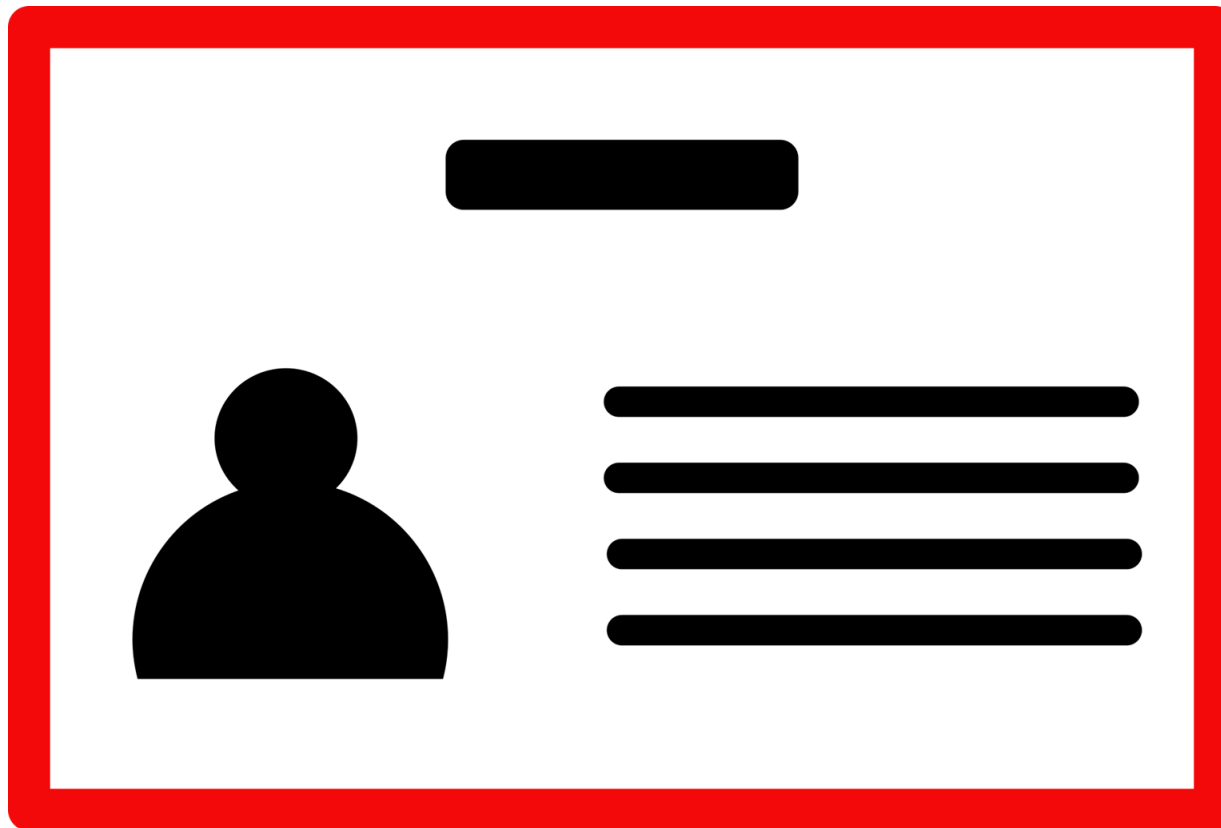




# Trust



# Selective Disclosure



# RSA<sup>®</sup>Conference2022

## Other Topics



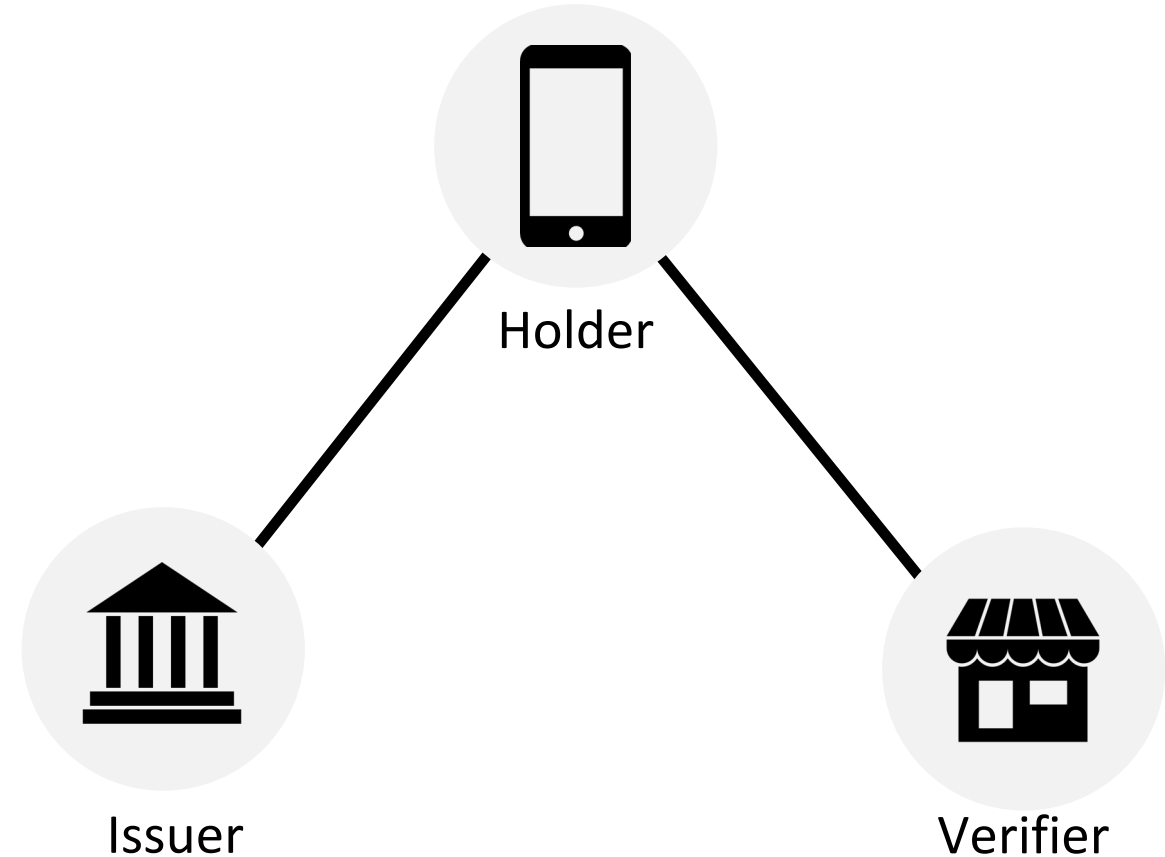
# Wallet Security & Trust

## Software Trust

- Is the software a digital wallet I trust?

## Device Trust

- Is the software running on a device I'm willing to trust?







# 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 Architect

[george.fletcher@capitalone.com](mailto:george.fletcher@capitalone.com)