WebID

TPAC 2020
Ken Buchanan (kenrb@google.com)
Majid Valipour (majidvp@google.com)
Sam Goto (goto@google.com)
Agenda

- The Problem
  - Premise: federation is good, we want to preserve it.
  - How federation works
  - User activity tracking on the web
  - Scope of this project
- Solution Framework
  - Directed identifiers
  - High-level approaches for an identity API
- Moving Forward
  - Challenges
  - Community engagement
The Problem
Federation is Safer Than Usernames/Passwords

Create an account with

Sign-in with A
Sign-in with B

or

your@email.com
******

Two factor authentication, password-less single sign-on

phishing, credential stuffing, password reuse
Reliance on General-purpose Web Primitives

Browser
RP
IDP

Create an account with

Sign-in with A
Sign-in with B

or

your@email.com
******
Sign Up

forgot password

other low level primitives:
- Iframes
- Cookies
- Redirects
- Pop-ups
- URL Parameters

https://example.com

Create an account with

Sign-in with A
Sign-in with B

or

Pop up blocked
example.com wants to open a new window to a.com, but we blocked.

allow
Navigational/Bounce Tracking and Link Decoration

User 123 viewed engagement rings
User 123 viewed engagement shoes
The Classification Problem

https://example.com

Create an account with
Sign-in with A
Sign-in with B
or
your@email.com
******

https://idp.com

Welcome Sam!
Are you trying to create an account with example.com?

Referrer: https://example.com

Sam Goto
samuelgoto@gmail.com

navigation callback
?idToken=123

Sign Up

forgot password

Yes
RP Consequences of Web Identity

Welcome Sam!
Are you trying to create an account with example.com?

Sign-in with A
https://example1.com

Sign-in with B

Sign-in with A
https://example2.com

Sign-in with B

global identifiers

Sam Goto
samuelgoto@gmail.com

Samuel Goto
samuelgoto@gmail.com

Yes
Welcome Sam!

Here are the sites you’ve logged in this week:

- example.com
- a.com
- b.com
- embarrassing.com
- ugh.com
- blargh.com

Yes
Scope and Limitations
Currently out of scope

- IDP Impersonation
- Cross-device sign-in state
- The “NASCAR flag” problem
Enterprise Use Cases

Use your corporate profile to sign into expenses.com and create an account with the information below:

NAME
Sam Goto

EMAIL
samuelgoto@corporate.com

Sign in with
https://corporate.com

Report your expenses!

Sign-in with your company

Sign Up

forgot password

Welcome!

https://example.com

Sign in with
https://corporate.com

continue
cancel
WebID Proposals for Sign-In / Sign-Up
Important caveat

This project is in very early stages and everything below is still considered exploratory.
Complex Trade-offs

- Usability
- Ease of Deployment
- Developer Control
- Privacy Properties
- Use Case Coverage
Welcome Sam!

Are you trying to create an account with example.com?

Verifiably Directed Identifiers

SHA256(IDP_ID + RP + NONCE)
Alternatives under consideration

- Approaches for designing a new API fall into three general buckets:
  - The Permission-oriented Variation
  - The Mediation-oriented Variation
  - The Delegation-oriented Variation
#1 The Permission-oriented Variation

Would you like to sign-in to example.com with accounts.idp.com?

No  Yes

Sign in with
https://accounts.idp.com

Use your accounts.idp.com profile to sign into example.com and create an account with the information below:

NAME  Sam Goto
EMAIL  Share my email
samuelgoto@gmail.com
Forward to:
  samuelgoto@gmail.com

By signing-in to example.com with your email address, you can be tracked across sites.

EMAIL  samuelgoto@gmail.com

allow  cancel
Use your accounts.idp.com profile to sign into example.com and create an account with the information below:

- NAME: Sam Goto
- EMAIL: Share my email samuelgoto@gmail.com

Forward to samuelgoto@gmail.com

Sign Up

cancel continue
IDP Tracking

- Neither the permission-based nor mediation-based approach limits the ability of the IDP to know where the user has signed in using the IDP credentials.
- Delegation-based approach redefines the role of an IDP to address that.
User Agent

Email Proxy (proxy.com)

[2a] What accounts does this user have?

[2b] Sign-in user is alice@email.com.

Email Provider (email.com)

Relying Party (rp.com)

[1] Want to Sign-in with IDP.com?

Identity Provider (idp.com)

[4a] Does RP have an account for SHA256(alice@email.com, R, rp.com)?

[4b] No..

[5] Forward abc@proxy.com to alice@email.com and hand me back a certificate?

[6] Can I sign IdTokens for {id:abc, email:abc@proxy.com}?

[6a] Check no one else has claimed id:abc

[6b] Verify email address (if included in claim)

[6c] Here is a nonce and a certificate.

[7] I am abc@proxy.com and SHA256(alice@email.com, RP, nonce). Prove this to me later with SIGNED(SHA256(alice@email, abc@proxy, RP, nonce), private key)

[8] Welcome abc@proxy.com!

[9] Welcome abc@proxy.com!

#3 The Delegation-oriented Variation

global email directed email keypair certificate nonce recovery token
If the user grants access, the id token is passed back to the application:

```json
{
  "alg": "HS256",
  "typ": "JWT"
}
{
  "iss": "https://accounts.a.com",
  "sub": "110169484474386276334",
  "aud": "https://example.com",
  "name": "Sam",
  "given_name": "Sam",
  "family_name": "G.",
  "email": "242423asf390@email.example",
  "email_verified": "true",
}
```

HMACSHA256(base64UrlEncode(header) + "." + base64UrlEncode(payload), SECRET)
Welcome! Sync your external calendar with us!

Would you like to connect your accounts.idp.com calendar with example.com?

No
Yes

Authorize example.com to read your calendar?

continue cancel

By authorizing example.com to access your calendar, you can be tracked across sites.

cancel allow

Aside: Authorization

Sync your calendar!
Looking Forward
Challenges

- Ecosystem design
  - Can RPs do their job well enough with directed identifiers? Customer support classic example.

- Technical questions
  - To what extent can we programmatically enforce directed identifiers?
  - How valuable are technical enforcement measures over policy requirements for IDP behaviour?
  - What about server-to-server communication that is in common use today?

- Accommodating other use cases
  - Should enterprise policies play a role in setting a different privacy bar for enterprise SSO? How would we handle “bring your own device” scenarios?
Engagement

- Many stakeholders:
  - RPs
  - IDPs
  - Browsers
  - Other identity ecosystem participants

- Feedback is welcome on [https://github.com/WICG/WebID](https://github.com/WICG/WebID)
This deck is shared publicly.