Identity Wallets and the Web

Notes

Level Set / History

[Rick]

- Presentation for PING yesterday: https://docs.google.com/presentation/d/1Z7blMTME1tAQAdO-Wr42oVNN3CRIbklASjbJdB1JYOc/edit?resourcekey=0-ockU2NbemVbLEeF94-peNA#slide=id.g1e7061371dc_1_5
- Mdoc: standardized by ISO, used by TSA in the US at airports (-5)
- 18013-7 talks about using them on the web
- W3C Verifiable Credentials: three party system, issuer/holder/verifier. Similar to federated identity but upgrade from a privacy perspective since you don't have to phone home to issuer
- Example: US immigration is deploying VCs: vaccine cards, permanent resident cards, job apps, verifying age, buying age restricted products, etc
- Microsoft Authenticator implements VCs
- eIDAS 2.0 in Europe passed into law in 2023 and goes into effect in 2025. Designed to comply with GDPR and requires that RPs accept digital IDs from EU digital wallet apps. Sign in with a wallet credential.
- A bit late to this party in the browser world
- Bunch of upsides:
    - Seems better than federated identity (better privacy)
    - Improve privacy over status quo (anonymous age verification)
    - Similar to passkeys (reducing fraud and identity theft)
    - Gives users more control
- Risks:
    - Some systems rely on trusting issuers
    - Privacy: if you're at risk, hard to be anonymous online, how do they participate?
    - Opportunity for bugs and coercion
    - Use of devices in full control of users (Linux, rooted Android, etc)
    - Normalization of signing in for gov ID, what does that mean for critique of government?
    - Healthy to think about concerns about big tech
- Key questions:
    - Should we have an API?

- How do we get people to use it?
- What do folks want to see in it?

Use Cases

[Torsten] what will this group cover? Dependent on how the issuer and the wallet, and the verifier and the wallet talk to each other. Most important open issue is wallet discovery and invocation. The rest, in my opinion, is already solved.
[Tim] Yes lots of that started years ago, including in FIDO. But we haven't even started trying to figure out the discovery and invocation problem. WICG is built for incubation, conducive for doing this sort of work. Goal is to dive into.

[Rick] Torsten you said other stuff may already be solved, that may be true, except for education of the community.

[Torsten] Existing work needs to be considered, iron out the scope. There is work in OpenID Foundation on OpenID for Verifiable Credentials and IETF SD-JWT, for example.

[Ben VanderSloot] there's a lot of concerns around privacy, equity, censorship, with specifically ISO 18013-7. -5 is one thing (in person), to make it web accessible easily is a drastic step, and is scary. There's things that can be done to mitigate harms. Examples: releasing info that is blinded instead of sharing the whole ID string, proving you're an age without sharing an age. There's a lot to consider and a lot of risk involved and that is why Mozilla is interested in this space.

[Rick] That risk involves even just -7?

[Ben VanderSloot] other concerns around the method of selective disclosure. Message heard that this is happening quickly no matter what. -7 isn't approved and signed off on. Just because on a current trajectory doesn't mean we can't change.

[Michiel de Jong (Solid Project)] Use case is logging in with any ID, including a self-asserted, or personal domain name.

[Tess] That's about signing i
, this is about identity - separate. N

[Gerhard] Financial services industry.

Proof of address is used in some countries. Some claims in a credential haven't been defined in things like the VC spec (e.g. what is an address or country).

Cornerstone identity or high trust identity: cross-domain identity usage. Government mandates about a legal person, with consent, replace things like ID scanning selfie.

[David Benoit] larger payments or cross-border payments that require KYC, currently complex state of the world

[Sameer Tare] financial as well. Payment auth would require integrating with a digital identity wallet such as a national identity scheme for KYC. Currently left up to many of these parties.

[Oliver Terbu] works on ISO mdoc WG. authentication use cases are a thing. was brought up by govs and iso wg. protocol should allow guaranteeing certain confidence levels and confidence in the presenter and not requiring presentation of biometrics in all situations.

Presenting online in a secure way. Doesn't always require presenting biometrics. Authentication

[Nick Steele] considering how password/passkey now wallets could act as VC holders. Second class citizens in the browser. Difficult to pass credentials securely via web extension. User may not want to use platform of gov controlled wallet. Account recovery for passkeys, being able to provide a way to recover accounts without giving users a secret key that they need ro write down or print out. Being able to strongly tie an account to a gov identity may not always be a bad thing.

[Nick Doty] Access of government benefits sometimes requires a gov credential. Current methods may be very intrusive and moving to a new method may not be easy. Persistent user identifiers? governments have expressed strong interest in blocking access to content based on these credentials.

[Gerard] travel in airports and has regulatory approval in many places

Potential Concerns

[Ben] proliferation of real name policies. Could this be used to set a name on someone’s profile? Has impact on equity for some groups.

The 3 party model doesn’t change the compulsion factor between parties. The people who are most compelled to use these are likely the most disadvantaged.

Aadhar is an example of this in India. News stories about rice rations based on an Aadhar check. Deep issues here.

[Garhard] Various schools of thought on how parties interact with each other. DidComm is proposed by some. Microsoft talks about OpenID4VC/OpenID4VP may be better. These interlinking protocols are important.

[Nina] hearing governments are starting to do this, so we need to this. Just because governments are doing this doesn't mean the community should necessarily encourage it. Example, adding friction to usage.

[Giuseppe De Marco]
I'd like to ask which role and scope the web browser would or should have within the wallet ecosystem.

Considering the EIDAS Regulation (and the roles defined within its ARF), would the web browsers be a wallet application instance and then be enabled within each Member State under their wallet solution providers or form a wallet solution to be accredited directly with the european community accreditation platforms.

Differently, would the web browser implement interfaces and bindings to let the user control their wallet instance, issued by member states wallet solutions and installed on their personal devices, to improve integrations and UX following some kind of standards.

How do you want to propose web browsers within the ecosystem?
- wallet solutions;
- wallet instances under pre-existing wallet solution;
- external wallet instances controllers and interfaces through a standard API that binds the personal devices.

The impacts may be found in the technical requirements related to the security of the storage and access to the digital credentials and not at least to the trust model, that forces the wallet solutions to be accredited and be fully compliant according to the regulation and its trust framework.

[Rick] Chrome definitely wants only the 3rd - help connect websites to accredited wallets. We do not want to be a wallet ourselves in any form.

Next steps

[Tim] We want to start meeting ASAP, probably the week after next. We recognize we'll have to be flexible with time. Want to know who wants to be part of a recurring meeting. OK to do under WICG?

[Tess] Sounds good to me. Sometimes makes sense to spin up a CG. But this is also why WICG is there. Hit the ground running.

[Tim] For FedID CG
Any objections with starting to meeting weekly 2 weeks from now? We could send out a doodle to see who is interested / timezones.

Our repo:
Issue tracking setting up a meeting.

[Nick] What specifically is the scope of the meetings? API discussions vs talking about the risks, or whether the work should be moved forward.
[Rick] We are starting work in Chromium, and aim to do a origin trial to learn. We need a forum for that discussion.

[Kristina] Is WICG the best place for this? The work has been contributed in WICG has only been from two browser vendors. Need expertise from other groups. Worried about starting

[Rick] Different proposals?

[Brent Zundel] There is a community group at W3C called Credentials Community group. Google is already a member. Chairs have already said they would accept it as a work item.

[Sam] Want to go where the discussions are happening. Not sure if CCG has strong representation from ISO mDoc group.

[Tess] Apple is already in the WICG. Could join CCG but it could take months.

[Brent] WICG could work. Need to work with CCG and invite

[Sam] WICG is not a final destination

[Rick] May be good to have some separation. We're looking at discovery and invocation.

[Kristina] Concern is not WICG not involving expertise in multiple other groups (IETF, OpenID, ISO, etc)

[Tim] One of the goals of this is to get people involved. We need help

[Brent] List of folks to talk to: CCG, OIDF, DIF, ISO, IETF

[Michiel de Jong] Secure Payment Confirmation from Web Payments Working Group as inspiration (besides of course FedCM and Passkeys)

Queue

- <queue closed]

Add your name

- Tim Cappalli (Microsoft Identity, session chair) [tim.cappalli@microsoft.com]
- Sam Goto (Google Chrome, session chair)
- Michael Ficarra (F5)
- Wenjing Chu (Futurewei and OpenWallet Foundation)
- Theresa O'Connor <hober@apple.com> (Apple, TAG)
- Rick Byers (Google Chrome)
- Lee Campbell (Google/Android)
- Helen Qin (Google/Android)
- Nick Doty (CDT)
- Oliver Terbu (Spruce), o.terbu@gmail.com
- Przemek Praszczalek (Mastercard)
- Benjamin VanderSloot (Mozilla) bvandersloot@mozilla.com
- Manu Sporny (Digital Bazaar)
- Achim Schlosser (European netID Foundation)
- Koichi Moriyama (NTT DOCOMO)
- Jean Luc DI Manno (Fime)
- Laurens Debackere (Government of Flanders - Digitaal Vlaanderen)
- Ryan Kalla (Google Chrome)
- Sameer Tare (Mastercard) **sameer.tare@mastercard.com**
- Sebastian Crane - seabass@fsfe.org
- Gabe Cohen (Block/TBD) - gabe@tbd.email
- Tony England (VISA) tengland@visa.com
- Benjamin Young (Digital Bazaar) - byoung@digitalbazaar.com
- Yen-Lin Huang (ministry of digital affairs, Taiwan)
- Mike Fisk (Meta)
- Brian Campbell (Ping Identity) - bcampbell@pingidentity.com
- Torsten Lodderstedt (Tuconic, OWF, OIDF)
- Kaustubha Govind (Google Chrome)
- Alex Rudenko (Google Chrome)
- Wonsuk Lee(ETRI)
- Jean-Yves Rossi (Canton)
- Nicolas Pena Moreno (Google Chrome)
- Yi Gu (Google Chrome)
- Christian Biesinger (Google Chrome)
- Imran Ahmed (Modirum)
- Matthew Miller (Cisco)
- Gerhard Oosthuizen (Entersekt) [goosthuizen@entersekt.com]
- Kristina Yasuda (Microsoft, VC WG chair, ISO, OIDF)
- Sami Tikkala (Visa)
- Melissa Sebastian (Modirum)
- Brent Zundel (Gen)
- Giuseppe De Marco (Dept. Digital Innovation - Italian Government)

- Marcos Cáceres (Apple)
- Martijn Haring (Apple)
- Hicham Lozi (Apple)
- David Benoit (IE)
- Geun-Hyung Kim(Gooroomee, Dong-eui University)
- Olivier Maas (Worldline)
- Nina Satragno (Google Chrome)
- Torsten Lodderstedt ()
- David Zeuthen (Google, Android, ISO)
- Michiel de Jong (Solid Project)
- Laurens Debackere (Solid Project)
- Nick Steele (1Password)[nick.steele@1password.com]
- Dirk Balfanz (Google) [balfanz@google.com]
- Dan Brickley (Google, Schema.org) danbri@google.com