Antifraud TPAC Breakout - 14 September 2022

- https://www.w3.org/slack-w3ccommunity-invite

Agenda

- Use of DPK for Antifraud.
- Impact of various anonymization efforts on Antifraud.
- Other Discussion

Attendees - add yourself at the bottom

- Steven Valdez (Google)
- Christian Aabye (Visa, EMVCo)
- Mohamed Allibhai (Human Security)
- Vinod Panicker (Amazon Ads)
- Philipp Pfeiffenberger (Google)
- Aloïs Bissuel (Criteo)
- Lionel Basdevant (Criteo)
- Per Bjorke (Google Ad Traffic Quality)
- Erik Taubeneck (Meta)
- Erik Anderson (Microsoft Edge)
- Jeffrey Yasskin (Google Chrome)
- Sameer Tare (Mastercard, EMVCo)
- Mariana Raykova (Google)
- David Benoit (IE, Web Payments Working Group)
- Thiago Diogo (Google)
- Rossen Atanassov (Microsoft)
- Ian Jacobs (W3C)
- Tommy Pauly (Apple)
- Aykut Bulut (Google Chrome)

Queue - add yourself at the bottom

- CLOSED

Minutes

— Steven: Overview of agenda.

Use of DPK for Antifraud

Per Bjorke: Use of DPK for Ad Fraud - no silver bullet for fraud; can DPK be used? Can we solicit ideas for how it could be used?
Tony: How/Why DPK used in passkey. No direct interface to it.
David: Device public key proposed by level 3 from webauthn; could be used for single device credential. Second piece of information/extension that you can accept that is a hint that you are on the same device. In multi-device scenario, hardware-bound keys per device. Example: github.com supports webauthn for authentication. Web vs app may not be the same even on the same hardware. Similar to what sites might do setting a cookie, except it's a known/trusted authenticator.
Sameer: Data only available to relying party who is authenticating. Can it be used by other party?
David: Meant to be per-device, per-credential. Not to correlate credential
Peter: Has it been used for rate limiting?
David: Experiment with FIDO; registration of credential, zero knowledge proof to attest that hardware genuine
Per: non trackable way to see if someone had done 2fa?
David: meant to serve as solution to cloudflare prevention solutions like captcha but still use VPNs. authenticated with cloudflare then used for proof
Per: Trust token and privacy pass are solid communication protocols; what are incentives to share/transact them? How do we create those incentives?
Sameer: Merchant risk indicators go all the way to issuer; merchants can add detail including their own assurance.
Tommy: Privacy pass - if you've done a captcha on my site, I can look at a signature and determine that captcha was done before. Work in IETF has evolved, near complete - more open ecosystem. Websites can challenge and redeem token. Issuer could just be that captcha was done before. Issuer could also be a separate entity (fraud prevention service), to partner with multiple attestation services to collect signal similar to what went into a captcha system. Device would talk to its own hardware attestation and present to issuer, and blindly have it passed back. Cloudflare as intermediary wouldn't be aware of B of A (as an example) as the redeemer. Public v private verifiability: original privacy pass used private verifiability/key. Public verifiability (like blind RSA signature) is more of the trend now. You can also challenge token, go back to issuer; or restrict token scope to origin you work with; you can pre-cache them, but it will only work for example.com - and those redeeming sites can agree on a one-time token spending approach.
Erik: Where is the incentive? Built into browser to attest? Should there be an API for additional attestors?
Per: Concept of multiple types of attestation - device, hardware, OS/platform, browser all useful
David: Incentive is that if you can get an authenticator to verify that the user actually used their passkey/etc, the signal is valuable as compared to just saying the merchant is fraud free

Impact of various anonymization efforts on Antifraud

Sameer: Overview - issuers need to have enough signal/confidence to not introduce additional friction/create risk to merchant transaction. An app-based flow with an embedded SDK helps issuer to get device attestation. Different problem in browser environment because there is no specific identifier
Steven: When I use a card in life, the location is a signal to the bank. Is there a similar concept in IP address for fraud detection?
Sameer: It is, and extremely important. The location and velocity (when it moves, how quickly). In 3DS not only device data, transaction data, transaction history, billing address, etc. If one element is off, it can still be assessed. This study is relevant and explains the drop-off that Microsoft saw when doing more strong customer authentication:
http://www.w3.org/2022/Talks/dean-jordaan-20220912.pdf

Lionel (Criteo): Antifraud very important for ad use cases as well. We rely on a variety of signals (IP address, cookies, user agent string, etc.).

Vinod (Amazon): The IVT detection use case subsumes many of the other fraud methods. If we see illegitimate publishers taking a piece of ad $, this impacts how much money flows to honest/authenticated publishers.
Steven: Individual events, or aggregated events?
Vinod: 2 ways of doing it: some are real-time, do we let this traffic through (prebid); once the event takes place (if it was allowed), we can observe and report post-bid (based on an impression/page JS load). The latter enables more sophisticated detection methods and the ability to better scrub metrics overall. Also aggregated at Seller-ID level to take enforcement action. So if a seller has anomalous traffic, they can be demonetized.
Lionel: Similar mechanism, based on set of actions. One fraudulent click is not an issue. Real-time prevention helps quickly detect fraudulent pattern, directly stop accepting traffic from specific IP addresses; as well as post-bid/post-click detection and data cleansing.
Steven: Is there much in aggregate data on sellers?
Sameer: Issuer fraud model is aware of both merchant and individual level issues. Also merchant category codes. All this takes place server side
Vinod: A trend in ad industry is move to SSAI (server side ad insertion) - a server stitching ad in with content and delivering to client. Common in streaming tv, online video. Better user experience, less ad blocking, causes again obfuscation (we don't get client IP or client details; server in between can alter data in transit)
Ian: Question in the 3DS context is: Have I seen this card with this device in the past? Could the digital public key serve the same purpose? Also, trust token is "I trust some token issuer, so I'm going to ask to have a token … there's a distinction between the issuer and the redemption." You authenticate from a bank and the bank trusts this browser. Same party issues token and evaluates later, without decoupling.
Mariana: Can we weigh privacy concerns against adding additional data to the actual trust token? When issuer needs a token, even when it's given, they don't know they gave it to me - it's unlinkable.

Sameer: This is ok because it's still your bank and there's another consent mechanism (your credentials, etc).
Mariana: Does this defeat the purpose if it is linkable?
Peter: Primarily to prevent account takeover? Are there low friction ways of keeping a session alive on a single device? Technical challenge because session doesn't begin until payment request from issuer
Tommy: Maybe this doesn't require a new API, could fit into privacy pass spec. Seems reasonable to have an attestor system that is aware of payment methods and verifying specific account is following
Vinod: a list of primitives from an antifraud POV would be helpful here.

Joint Antifraud/WebPayments/WebAuth CG Meeting (TPAC) - 13 September 2022

Agenda

- 13:00-14:30 Antifraud
  - Use cases and proposals
  - Anonymous Credentials Overview (trust tokens, etc.)
  - Device/Client Attestation Overview
  - Hearing more from payments on threats (e.g., 3ds)
- 14:30-15:00 WebAuthn topics
  - Passkeys
  - Hybrid (formerly caBLE)
- 15:00-15:30 Coffee
- 15:30-16:00 SPC
  - Demo
  - Status of getting to CR and implementation
  - SPC/WebAuthn liaison issues
- 16:00-16:10 Breakout suggestions
  - Anti-Fraud Followup Breakout on Wednesday 15:00-16:00
- 16:10-17:00 White board session.

Attendees - add yourself at the bottom

- Ian Jacobs (W3C)
- Per Bjorke (Google Ad Traffic Quality)
- Sofía Celi (Brave)
- Sameer Tare (Mastercard)
- Nick Telford-Reed (IE, Web Payments Working Group)

- Jean Luc Di Manno (Fime)
- Michael Ficarra (F5)
- Nicolas Pena Moreno (Google)
- Magda Sypula (Apple)
- Steven Valdez (Google)
- Praveena Subrahmanyam(Airbnb)
- Gerhard Oosthuizen (Entersekt), only for first 2 hours
- Shane Weeden (IBM)
- Tony Nadalin
- Mike Jones (Microsoft)
- Aykut Bulut (Google Chrome)
- Zachary Tan (Google)
- John Pascoe (Apple)
- David Benoit (IE, Web Payments Working Group)
- Mandar Gaonkar(PayPal)
- Nina Satragno (Google)
- Ben Kelly (google)
- Rick Byers (Google Chrome)
- Marie Jordan (Visa)
- Sami Tikkala (Visa)
- Nakjo Shishkov (Netcetera)
- Jeffrey Yasskin (Google Chrome)
- Derek Hanson (Yubico)
- Luke Walker (Yubico)
- Xu Lin (UIC)
- Vinod Panicker (Amazon Ads)
- Kristina Yasuda (Microsoft)
- David Turner (FIDO Alliance)
- Brian Lefler (Google Chrome)
- Christian Aabye (Visa)
- Carey Ferro (Discover)
- Doug Fisher (Visa)
- David Turner (Google Ad Traffic Quality)
- Stephen McGruer (Google Chrome)
- Guillermo Movia (Article 19)
- Tommy Pauly (Apple)
- Sue Koomen (American Express)
- Fahad Saleem (Mastercard)
- Michael Horne (American Express)
- Jorge Vargas (Discover)
- Emil Lundberg (Yubico)

Action Items/Open Questions

- Explore device/client bindings as a potential capability.
- App Attestation exposed to the web (as an equivalent of origins).
- Breakout suggestion: Use of DPK+Passkey for Antifraud.

Minutes

Intro

(Steven introduces use cases)

Steven: Scope of anti-fraud CG work is primarily web-exposed threats, not including server-server/purely mobile fraud. We consider purely carve-out based solutions to be out of the scope of the CG, though those that require technical components could potentially be in-scope.

Steven: Goes over the list of use cases in https://github.com/antifraudcg/use-cases.

Steven: Given those use cases, we're looking for common capabilities shared across use cases. Some examples are IP, Geolocation, Device Attestation, etc.

???: Have you considered binding between a human and their device as a potential capability.

???: What's the scope of device attestation?

Steven: From real device, to potentially the thing running on the device/OS/etc.

Vinod: App attestation as an additional capability, exposing that information similar to how web origin is exposed.

Anonymous Credentials

(Sofia presents slides)

Sofia: Goal is to attest a past honest action so that future access is granted without a challenge. Tokens must not be forgeable, with no link between context where minted and where used.

Status:

- Privacy pass at IETF
- Trust tokens currently in WICG at W3C
- Implementations: Chrome and Apple as examples
- Apple Private Access Tokens

Sofia: In privacy pass discussions on IETF there are more recent discussions about adding metadata to prevent fraud, e.g., for token expiration, to prevent token hoarding, for token exchange for single-origin cookies.

[Some discussion of architecture, and roles played in that architecture, such as client, attester, and issuer].

See privacy pass documents at IETF: https://datatracker.ietf.org/wg/privacypass/documents/

Sofia: Issuers have to think about a lot to avoid privacy violations (e.g., related to key management and rotation, addition of metadata, etc.).

Sofia: We want to hear here whether this novel technology is usable for the use cases of interest here. The new architecture may introduce some issues; we still need a proper analysis of security and privacy considerations.

Praveena: Can you say more about the trusted devices use case?

Sofia: It’s not implemented currently, but it’s a potential use case cited by the IETF documentation. More work needed to know for sure whether tokens could be used for that use case.

Steven: See also the discussion upcoming on device attestation.

Tony: How do you determine whether to trust an issuer?

Sofia: The issuer will have a public key. ….

Tony: Clarification - how do you determine “who is an issuer” and “who is not”?

Sofia: That’s something that the ecosystem will need to figure out. Right now there are only a few companies, but that creates a problem of centralization. This is an ongoing discussion in the IETF.

Tony: Risk is collusion and tracking between issuers. Feels like a major problem.

SameerT: Do you see an identity provider fulfilling both issuer and attester role?

Sofia: Correct, they don’t have to be distinct entities.

SameerT: So assumes qualification criteria?

Sofia: Yes.

Per: Big challenge - how to create an ecosystem of issuers.

Sofia: From a technical perspective it’s not that difficult; what’s difficult is to manage different policies and the complexity of the ecosystem.

Steven: One thing to think about is that there might be multiple ecosystems. E.g., one thing on the web might be used for ad fraud (e.g., trust tokens), another thing might be used for payment fraud issues. So use cases may lead to specific technologies rather than one large solution for all use cases.

Sofia: Even the different type of considerations depends on what your system is trying to do. We’d probably have documents for each system.

Vinod: One of the use cases I see for these is device/app attestation. The question is how you make this work in a high throughput environment (such as advertisement).

Sofia: I haven’t heard much on that, but it's definitely an open problem.

Device/Client Attestation Overview

Philipp: Why device attestation?
Patterns that emerge: capabilities can come from the device: is the device that is expected?
Rate-limiting: how many accounts has this device created for me?
This creates confidence on the device and element visibility
Is it resilient?: Trust over time

Still have to solve for older devices. Custom kernels, etc. Additionally some of these may be slow, and for many use cases you don’t have the time.

Still, there is hope. Sending attestation signs with a nonce, signed with the attestation server.
Can the same be done for the web?
Can Privacy Pass like protocols be used?: Open problems: Multi-attester support, standard for attester capabilities, feedback for broken attestation.

What attestation capabilities are needed?
How can attesters identify broken attesters?
User agency vs community rules
Which protocols and what kind of implications of multiple attesters support?
Lessons from auth and payments regarding standardization and accreditation?

Jeffrey: How will a new user agent gain acceptance?
PP: It shouldn’t matter in terms of the device’s identity.

Jeffrey: I heard that some questions are about trusting the browser; how would a new browser be trusted?
PP: As long as one can verify the identity claimed by the software, it should work. There are interesting topics about checks and how to ensure those checks are equitable.

Tony: Consent is a big issue (e.g., to release an attestation from a device). Another issue – the privacy of the attestation; how can you blind the attestation?
PP: We've not settled on amount of entropy. In terms of consent, good question. Ideally this reduces friction for the user. As we explore use cases we can see where there are or aren't other avenues for less invasive ways to do something.
Tony: If you have to consent every time, will people use it? We ran into this with WebAuthn.
Tommy_Pauly: Regarding a new browser/attestation source: in privacy pass, one of the benefits of splitting attester and issuer is that a web site only needs to trust their issuer. It's designed to make it easier for new attesters to enter the ecosystem. This should facilitate new entrants.

PP: How does the issuer reason about the confidence it should have in the attester over time?
Tommy: Need to continue to understand that more and how it plays out. To begin with, having shared understanding of what is being attested (and doing auditing) is a good baseline. There are ways on different platforms already that servers already trust.
Sameer: I can some application of this in Web Payments context. One way to do fraud prevention is data collection about a device. The attestion shows integrity of device, but not that the user and device are bound together.
PP: The device binding of tokens seems parallel to attestation. It sounds like it's a re-identification problem.
Sameer: If the user can attest their device to a service, and send an identifier, if it can be reused for re-identification, you don't need to do anything different. Suppose I'm doing a card-not-present payment on the Web, if the device were already attested, the experience could be frictionless.
PP: I want to talk about how that relates to unlinkability. There might be some other levels of consent required for additional linking.
Sameer: If I as a customer consent to the data collection, could the issuer issue a token with metadata to payments. Let's do a deep-dive later on.
PP: +1
Tony: There are cases where the attestation wants to be tracked. E.g., an enterprise might want to track devices (and avoid BYOD to work). Have you thought about "enterprise attestations"?
PP: Not yet. I would think of that as an extension.
Tony: There are different requirements in enterprise and open Web use cases.

Followup Meetings

Steven: Thursday afternoon more on payments and Antifraud. (2pm Thursday)

Erhard: I work with Entersekt. We provide antifraud solutions usually around payments. I'll be talking about payment fraud patterns as well as evaluating some of the Antifraud CG Proposals to see how they relate to those patterns.

More Antifraud CG discussing will resume Thursday morning.

WebAuthn topics

Tony: We are working on Web Authentication Level 3. Some of the big topics:

- Passkeys
- Device public keys

Tony: We are working on our FPWD (after charter approval delays). Expect the FPWD in about a month.

[Passkeys]

Tim_Cappalli: Big goal, as a reminder, is how to bring keys to users with multiple devices. Some challenges today:

- Roaming authenticators are required to bootstrap the platform.
- Roaming authenticators impose an additional cost.
- Consumers are not interested in buying these security keys.
- Device loss is an issue with roaming authenticators
- Some branding issues: do users understand "login with WebAuthn?"

[We see a passkey demonstration, cross device]

Tim: These capabilities help address the bootstrapping issue.

Tim:

- For "easy to use as a password", we have Conditional UI
- For "easy to understand", we have Conditional UI and Cross-Device authentication via CTAP 2.2
- To leverage existing investments, CTAP 2.2
- For durability across device loss, we have made a big change to allow credentials to be synced. We've added some backup bits and device public key.

[Details on these changes]

Tim: Device Public Key (DPK) is NOT a credential, it is a device-specific public key. So if the RP sees a new DPK it may choose to do additional authentication. The DPK needs to be requested by the RP. It can be generated at any time (whether on creation or at any time subsequently). It is the authenticator's responsibility to generate the DPK. So there are three classes of credential:

- Single-device
- Multi-device
- Multi-device with DPK.

Tim: The RP can reject multi-device credentials; it's better than passwords and we hope people will use them.
Sameer: Is DPK a possibility today?
Tim: There's no shipping authenticator with it yet. Microsoft will have it when we make syncable credentials available.
Adam: Look soon on Android.
John_Bradley: There's a subtlety – attestations are important. Attestations are optional with DPK. You can always ask for an attestation; you may not always get one.
Tim: It is optional today; will remain so.
Sameer: Will re-enrollment be required once DPK arrives?
John_Bradley: No. If I have an iphone, it will automatically be synced to my laptop. The RP doesn't know which one I'm using. It will ask for an attestation; it will get it on creation. If you share your credential with someone close (e.g., via AirDrop) you'll get a new DPK for that device.
Tim: No single-device credential will automatically transition to a multi-device credential.
@@: Can you tell if a credential is multi-device if unattested?
John_Bradley: If you take a credential without attestation you don't know what you're getting. If you have security requirements, you should check attestations.
Per: Can we discuss this feature for anti-fraud (e.g., in breakout tomorrow)
Tim: To summarize - a user account may have multiple types of credentials, and for a given multi-device credential there may be multiple DKPs.
Gerhard: Excited to see this rolling out. One of the challenges we face as implementers is to establish a great UX. We don't know if there's a credential on a device; we don't know when to enroll the user. How do we detect that, yes, I should show these credentials at the system to see if it sticks? If the credential is not available, there's a clunky "sorry" message.
Tim: We think Conditional UI will help with the transition. When everyone has a passkey in the future, we expect there will just be a "sign in with passkey" button on sites. But in a transition period, we want to help the user out to know that they have a credential. So when I entered a username field, I am shown available credentials (to choose from). There is a WebAuthn call to detect platform authenticator presence. If you get back "true" you should start using passkeys.
Gerhard: What about roaming authenticators that may not have been synced? (even worse with SPC).
Shane: I've been experimenting with Conditional UI; it's goal is to address the privacy issue (by not leaking info about enrolled credential).
Gerhard: If it's universally available, that's great. But the second scenario where the bank might have user name entry on a primary page…is there anything we can do where there's a username hint?
Tim: If you do discovery on a redirect and discover has a passkey, you can on the last screen show a "signin with passkey" button. The WebAuthn adoption CG is a place where discussions like this are happening.
Shane: Even if you go to a page with username, you could show a password field that, when focused, shows the credential UI.
Gerhard: What percentage of browsers will have autofill UI in the next 3 months?

Adam: Answer: Chrome, Edge, Safari within a few months.
Tim: Passkeys are not a new protocol; it's an attempt to give a friendly name to an enhanced signin experience. In terms of support, iOS 16 dropped yesterday (with full support), @@scribe missed other information@@
@@: Within approximately 3-4 months, Android will support.
Nina: You can query the availability of the autofill API in the browser.
Steven: Let's move most discussion of this tomorrow.
PP: It looks like the attestation here uses revocable device certificates.
John_Bradley: The attestations support existing and future formats. Imagine we are in a post Quantum world; we want RPs to be able to say "Yes, I support that new format." You can send a list of what you support, and the authenticator will return what it has that matches. Previously authenticators supported a single format; there is now more flexibility.
Tim: You can delete either from RP or authenticator.
StephenMcGruer: In payments, verification is often not side-effect free. The decision is more difficult; there is no idempotent fallback.

[Slide on newly allocated backup bits]

- Backup eligibility. These credentials in some cases could be share with third parties. For friendly fraud use cases, you may wish to use DPK or some other fingerprinting approach.
- Backup state

Tim: there will be authenticators that support both single and multi-device credentials. Some credentials are eligible for backups, others are actually backed.

Ian: where does the assertion go after mobile authentication?

[We see an animation to answer this question]

Tim: Authenticator tunnel service is run by authenticator. How the authenticator talks to tunnel service is an implementation detail. BLE is just used for proximity test.

Nick: Is BLE replayable?

Adam Langley: Any attacker has to be physically proximate.

Nick: What about NFC?

Adam Langley: I would love for NFC or Ultraband on every device. But BLE is everywhere today.

Tim: We expect to have a passkey icon soon.

IJ: How to know when to offer registration?

Adam:

- If user used password and API is available, consider offering enrollment experience.
- If multi-device credential was used, can prompt the user to get credential on a new device.

@@: We are also experimenting with an interstitial to give people an option to enroll a passkey, only when passkeys are available. Would be nice to have a standard UI (rather than Okta doing this).

Tim: Another idea is to have a “create an account” button that just creates passkeys.

[More discussion on this at breakout tomorrow.]

SPC

Ian: Welcome back to the session on SPC. I’m Ian Jacobs, W3C staff. Today there will be a little bit of sharing of what SPC looks like for people who haven’t seen it yet. Purpose of this is to talk about our relation with WebAuthN and questions we have.

Ian: [demo] This is a checkout experience where the user is paying with credit card. When they go to pay, typically there is a verification step. With some sort of challenge by the issuing bank (such as an SMS code). Flow offers the user a way to enroll to a faster method of verification. Prompted and creating an assertion for the credential and the payment instrument.

Ian: For 3DSecure 2.3, buying again with the same credit card/service provider, the payment provider can use the 3DS to see if there’s any FIDO/SPC credentials associated with the payment instrument. If there is, user is prompted to authenticate with the credentials, which are over the transaction details. Big reason is for requirements to have crypto proof of user consent. Relying party can then verify.

Ian: One of the stories of SPC is payment use cases might diverge a bit from WebAuth level 2. For SPC, you might want to enroll in an iframe without redirect to bank site. (supports cross-origin registration). Another piece of SPC is that other parties than just the relying party can validate the credential, allowing the merchant to control the payment experience, while the issuing bank is the one validating the assertion. Another change is the UX and using client data to sign the transaction data.

Ian: Payments folks have new use cases, and more data they want to display. How can we narrow the distinction between SPC and WebAuthN, by moving some of the differences into WebAuthN.

[Slide Deck]

Stephen McGruer: Create in a cross-origin iframe isn't just an SPC requirement, and useful for other parts of web payments. The third-party authentication has to be opted-in by the relying party.

Ian: Links in the deck for the various demos. Status of SPC: Stripe pilot that showed 8% increase in conversions. Version of SPC shipping in Chromium for MacOS and Windows Hello. Stephen announced support coming in Android. Mentioned in EMVCo 3-D Secure 2.3 Working group moving to advance the spec to candidate recommendation.

Ian: Ability to use credential cross-origin led to proposal to CTAP folks to pick up the cross-origin bit.

Tony: Stephen has filed PRs…

Stephen: PR has been landed in CTAP.

Ian: What's the meaning of availability of the spec.

???: Working on a publish schedule, trying to sync what's going on with WebAuth.

Ian: TL;DR Coming soon, but not available public yet.

Adam: Has landed in the editor's spec, can we get support in Windows Hello?

Ian: Landed in CTAP, coming soon publicly. WebAuthN will need some changes to say that bit is allowed at creation time.

Stephen: Might be a pass-through to FIDO so might not need WebAuthN changes. Hopefully all WebAuthN extensions get moved from SPC to WebAuthN.

Adam: Is valid to specify outside of WebAuthN if purely authentication extension, though should go into a registry.

Ian: Where does the registry live?

Adam: IANA?

Ian: Action, Stephen to follow up on registering the extension.

Adam: Do you want the extension plumbed to the web layer?

Stephen: Yes, SPC defines a WebAuthN extension. Today is in SPC, eventually move to WebAuthN. Questions about why its outside of the spec.

Stephen: It is a vanilla webauthn create with this extension.

Ian: What's the next steps for authenticators to support this? Is there another bit of changes to query whether the bit/data is set.

Stephen: Part of the credential listing API in CTAP. Equivalent functionality in platform authenticators.

Shane: Question about differentiating between SPC and authentication credentials. If they can be queried by third-party, doesn't that break the non-phishable pattern? What prevents SPC from being used as an authentication to a website.

Stephen: Protection is that the RP needs to opt-in to the new credentials type. If you are aware of the type, you might have both the new credential type and the authentication credential.

Shane: If the RP doesn't know about the extension, how would they be aware that the SPC and authentication credential have different threat models.

Christian: What's the threat model?

Shane: I'm concerned about RPs winding up with third-party exercisable credentials without understanding the issues. Something on the UA modifies the create call to include the bit, the RP then responds with an attestation that includes the SPC extension without understanding it. Either the RP needs to understand the extension and ignore it or has a credential with the bit set.

Stephen: Good point, this could happen, however the only way to use a credential in a cross-origin way is doing a SPC flow, causing a big payment screen to show. If the user isn't the malicious then that would be a red flag. Also the type isn't credential.get vs payment.get.

Shane: I presume its been considered and there are controls.

???: WebAuthN doesn't know anything about the cross-origin bit, its only via the SPC flow. The client data includes the RP ID and identity of the proxy. There's additional information in the client data that says how it was exercised cross-origin.

Stephen: The important thing is that webauthn should be checking the type to ensure that you aren't using a non credential. But the only way for the wrong type to show up is a malicious client implementation to use SPC as auth.

Ian: Cross-origin create, get was allowed in level 2 but not cross-origin create(). This is one of the points of divergence. Stephen has created a PR to add cross-origin create() be considered for Level 3. Now an open issue (1656).

???: No action on these pull requests so far. If the only blocker is sending them officially, but not sure how the WebAuthN WG works for it.

???: Parameter was in the spec but removed, delta would just be to put it back in the spec.

John: We don't want cross-origin create, we think UX is confusing and privacy issues are concerning.

???: Objection noted and will be discussed in the WebAuthN working group. Next step is getting PR filed and then discussion in the WG.

Make sure it matches the change, separate from the rest of Stephen's.

Ian: Can we dig into the objection slightly. I heard two pieces, confusing the user and tracking concern.

Stephen: This is all in the issue comment, we acknowledge the tracking concern. There's an existing concern that because of get, that you can trigger it from an iframe and colluding main page (permission policy). User tricked they're doing a get on the main page, and full identity on the user. Create makes that worse since user doesn't need to go to evil top-level origin. Reasonable threat, though if the top-level isn't colluding the permission policy protects it. For non-colluding, user activation requirement to trigger create could mitigate this. My stance is user activation for create is sufficient. There is a job for the WebAuthN UI to make it clearer to the user. Currently hard to tell as a user.

Ian: Another piece of UX, that you have to go through the SPC.

Not for create credential.

Stephen: Big scary warning if UAs want. More reasonable world is better/more clear UX.

Ian: Document about the bigger picture of SPC evolution.

Stephen: Most of the content is the rest of the slide. Document contains details on how to get this into WebAuthN.

Ian: Welcome read on the doc, as movements arise, talk again. Last slide is that there are other use cases, might want to register a credential associated with a card for a future/recurring payment. Could we have signature over the additional data (or less data for pre-auth).

(IANA registry for WebAuthN extensions can be found here: https://www.iana.org/assignments/webauthn/webauthn.xhtml#webauthn-extension-ids)

Quick update from yesterday, could be introduced, but wary about generic string types, but okay if there's a compelling reason as long as malicious RPs can't confuse the users. If the requirements are a little more detailed, maybe we can talk about a generic dictionary type thing. It'll kind of depend on what we want to do. Discussion yesterday is to come back with requirements and present it to the group.

Wouldn't be supported on older authenticators (ie Windows 10). Pushback from security and privacy.

The biggest issue is having broad enough authenticator support to make it worthwhile to the RP and having the user understand what they're agreeing to.

What you can put in there needs to be considered, and probably shouldn't be wide open.

Another question is whether it belongs in WebAuthN. This is a pretty generic thing to do.

Ian: WebPayments will see what scope, and if its more of an SPC thing or WebAuthN thing.

People will have all sorts of expectations once you start doing generic signing. How it will be verified later by a third party, how does the third party know its the right public key.

Ian: Third bullet on the slide, addressed earlier.

Breakout suggestions

Steven: We reserved an hour session tomorrow (3-4pm). Ideas for continued discussion?

- Brainstorm if Passkey/DPK can be used for anti-abuse use cases
- Talk about impact of anonymization efforts on anti-fraud.

Other