Comment Template for: NIST SP 800-63-4 Suite (Second Public Draft)

Please submit responses to dig-comments@nist.gov by October 7, 2024.

| Organization: | Google |
|---------------------------------|-----------------------|
| Name of Submitter/POC: | Omid Ghaffari-Tabrizi |
| Email Address of Submitter/POC: | |

| | B. LP | | | • | |
|-----------|--------------------------------------|--|--------|---|------------------|
| Comment # | Publication (Base, 63A, 63B, 63C) | Section | Dage t | Comment Line # (Include rationale for comment) | Suggested Change |
| Comment # | (Base, 03A, 03B, 03C) | Section | Page # | While we appreciate that the main audience of this publication is US government agencies and | Suggested Change |
| | | | | contractors, we expect many other entities will use this as the basis of their own standards. As su | h |
| | | | | we'd recommend calling out aspects of these standards that are more about compliance with oth | |
| | | | | governmental policies and less about xAL per se. Specifically, some of the subscriber notification | |
| | | | | requirements are likely not applicable to most enterprise contexts. Perhaps more use of the "ope | ated |
| | | | | by or on behalf of federal agencies" qualifier could be helpful in such instances (e.g. 63b 4.1.2.1, | |
| 1 | 63-Base | throughout | | 3.4, 63c 3.4.3, 63c 3.6, 63c 3.7.1, 63c 3.9, 63c 3.15, 63c 4.6.7). | |
| | | | | "What specific implementation guidance, reference architectures, metrics, or other supporting | |
| | | | | resources could enable more rapid adoption and implementation of this and future iterations of t | le l |
| | | | | Digital Identity Guidelines?" | |
| | | | | | |
| | | | | The user controllability of the digital identity solutions, especially the pattern with a subscriber | |
| | | | | controlled wallet, is understated throughout the guideline. With a subscriber controlled wallet, the has full control of the digital identity and the exact PII data attributes being presented to RP. This | user |
| | | | | advantage makes a significant difference on the traditional identity solutions and digital identity | |
| 2 | 63-Base | 2. General | | 198 solutions. | |
| | 03-0836 | Z. Gerierai | | "What applied research and measurement efforts would provide the greatest impacts on the idea | iity |
| | | | | market and advancement of these guidelines?" | |
| | | | | · · | |
| | | | | 1. Overall the privacy advantages on the federated digital identity model with subscriber-controll | d |
| | | | | wallet example (Fig. 5.) are not clearly stated within the guideline. Given the CSP-wallet-RP mode | it is a |
| | | | | significant advantage that RP does not need to actively communicate back to the CSP during the | |
| | | | | proofing process thus CSPs would not be able to track the subscribers on their actions on the RP | de. |
| | | | | (The classic phone home problem) | |
| | | | | 2. Zero-knowledge proof would be able to significantly eliminate the risk of applicant being tracket | |
| | | | | under a collusion between multiple RPs via unique identifiers being exchanged during authentica sessions. | ed . |
| | | | | sessions. 3. Zero-knowledge proof would be able to significantly eliminate the risk of applicant being tracket. | |
| | | | | under a collusion between CSP and RP via unique identifiers being exchanged during enrollment | |
| | | | | authenticated sessions. | |
| | | | | 4. Selective disclosure, which is already implemented by ISO 18013-5 mDL, gives user the ability t | |
| | | | | disclose a subset of the digital identity while the RP can still easily verify the authenticity and inte | |
| | | | | the identity. | |
| 3 | 63-Base | 2. General | iii | 203 | |
| | | | | "Federated digital identity model with subscriber-controlled wallet example (Fig. 5.)" | |
| | | | | | |
| | | | | The term "federated" on Fig.5. requires additional clarification to avoid confusion. Although the | |
| | | | | protocol between wallet and RP can be considered as a "federation protocol", there is no federat between a CSP and RP. A reference or name without "federated" would make it much clearer to | |
| 4 | 63-Base | Fig. 5 | 20 | 898 audience. | ie – |
| | 03-0836 | 116. 3 | 20 | Recommend consistent use of "type of factor" e.g. "Multi-factor authentication (MFA) refers to the | s use |
| | | | | of more than one distinct factor." => "Multi-factor authentication (MFA) refers to the use of more | |
| 5 | 63-Base | 2.3.1 | 12 | 702 one type of factor." | |
| | | | | | |
| | | | | | |
| | | | | The standard specifies remote unattended identity proofing vs remote attended identity proofing | |
| | | | | where the difference is essentially if there is an agent online through a secure video session. | |
| | | | | Evidence submitted for personhood and ownership should be categorized as remote attended id | |
| | | | | proofing regardless of when the agent reviews it, as long as liveness and ownership verification a | |
| | | | | passed. Currently, the proofing method is categorized as "unattended" as long as there's no live h | |
| | | | | agents on the video session with the user. All un-attended verification methods are considered as | |
| | | | | assurance level than attended verification, which does not align with currently accepted best pra- | |
| | | | | As long as the verifier collects confident enough evidence from the user to prove their personhoo | |
| | | | | liveness check) and ownership (e.g., selfie matching), it doesn't matter if the human reviewing ag | |
| 6 | 63A | 2.1.3 Identity proofing Types | 8 | 595 interacting with the user online or reviewing the evidence in a separate session. | |
| | | | | Greater clairification is required around Confirmation Code Verification, especially where an indiv | |
| | | | | is able to demonstrate control of a piece of identity evidence through the return of a confirmation | code, |
| | | | | consistent with the requirements specified in Sec. 3.1.8. | |
| | | | | Confirmation code equivalent technology chould also be considered be | tor. |
| _, | 63A | 2.5.1 Identity Verification Methods | 14 | Confirmation code equivalent technology should also be considered here, specifically for multi-fa 784 authentication. E.g., confirm on a different trusted device on file. | |
| / | UJA. | Let out the many vermication internous | 14 | 704 additional addition. E.g., committee of a different drusted device on file. | |

| | | 1 | | |
|----|-----|-------------------------------------|----|--|
| | | | | "Knowledge-based verification (KBV) or knowledge-based authentication SHALL NOT be used for identity verification." |
| | | | | The KBV / KBA shall not be used for identity verification by itself, but KBV/KBA should still be |
| | | | | considered an identity verification method along with other methods and the standard should account for this fact. E.g., PIN code on Japan My Number Card, SSN verification question challenge. |
| 8 | 63A | 2.5.1 Identity Verification Methods | 15 | |
| | | | | "CSPs SHALL implement the following fraud check for all identity proofing processes: 1. Date of Death Check – Confirm with a credible, authoritative, or issuing source that the applicant is |
| | | | | not deceased. Such checks can aid in preventing synthetic identity fraud, the use of stolen identity |
| | | | | information, and exploitation by a close associate or relative." |
| | | | | CSP shall perform a date of death check (liveness check) only if needed. Performing the liveness check |
| | | | | Cor stand pertorn a due to used crieck inverses criecky only in received. For mild interest crieck for all identity verification processes is unrealistic, especially for remote unattended identity |
| 9 | 63A | 3.1.2.1 CSP Fraud Management | 18 | 903 verification. |
| | | | | "6. CSPs SHOULD implement - but are not limited to - the following fraud checks for their identity proofing processes based on their available identity proofing types, selected technologies, evidence, |
| | | | | prooning processes based on their available identity prooning types, selected technologies, evidence, and user base: |
| | | | | SIM Swap Detection – Confirm that the phone number used in an identity proofing process has not |
| | | | | been recently ported to a new user or device. Such checks can provide an indication that a phone or |
| | | | | device was compromised by a targeted attack." |
| | | | | SIM Swap may not be the best and only way to detect a compromised attack. The method suggestion |
| | 63A | 2 1 2 1 CSD Fraud Management | 18 | here should be more generic: Device fraud indicator check, including device wifi, power, movement, 907 rooted, simulator etc. |
| 10 | ACO | 3.1.2.1 CSP Fraud Management | 18 | 30 TOURUS, SIRIURIUS EU. |
| | | | | *11. CSPs SHALL establish a technical or process-based mechanism to communicate suspected and |
| | | | | confirmed fraudulent events to RPs." |
| | | | | This should be modified so that a CSP shall suspend or revoke the identity, if possible, If not possible, |
| | | | | CSP then shall communicate fraudulent events to RPs. Communication is a post-process mitigation after |
| | | | | a fraud event has happened. As the CSP, a better mitigation is to make the identity no longer usable by |
| 11 | 63A | 3.1.2.1 CSP Fraud Management | 19 | suspending or revoking it, so the damage would be fully controlled. Given suspending or revoking by a 943 CSP may not always be feasible, communicating with RP could be a back-up mitigation. |
| | | | | "Government Identifier: A unique identifier which is associated with the applicant in government |
| | | | | records (e.g., SSN, TIN, Driver's License #)" |
| | | | | NIST regulations should account for cases in EUDIW PID credentials where there is no mandated |
| 12 | 63A | 2.2. Core attributes | 9 | 626 regulation to have a unique identifier. |
| | | | | "Physical Address: A physical address to which the applicant can receive communications related to the proofing process;" |
| | | | | proving process, |
| | | | | PO box addresses are not a reliable signal. In those instances where there is no alternative, there |
| 13 | 63A | 2.2. Core attributes | ٩ | should be guidance provided to outline how other signals should be weighted or utilized to make up for 628 this weakness. |
| | | | | |
| | | | | Whether and how frequent reauthentication is necessary should be a function of the strength of the |
| | | | | session credential, and not of the Authentication Assurance Level. |
| | | | | Thinking of possible threats, the following attacks come to mind: |
| | | | | 1) theft of authenticator secrets (through phishing, key extraction, etc.) |
| | | | | 2) theft of session credentials 3) local attackers (someone taking over a signed-in user's device) |
| | | | | a) noted attackers (sourieurie tannig over a signeuriit User's device) |
| | | | | Reauthentication mitigates (2) and (3), but not (1). (3) can be mitigated with screen locks (which the |
| | | | | document should acknowledge). This leaves (2) as the threat that reauthentication can and needs to mitigate. If the session credential is strong (say, a DBSC-bound cookie), there is surely less need for |
| | | | | minugate. In the session Erecential is Strong bay, a Dost-dound cooke), there is surely less need of quick reauthentication than if the session credential is weak (a normal cookie). |
| | | | | |
| 1/ | 63B | 2.{1,2,3}.3 (reauth) | | The current treatment of reauthentication ignores this. The discussion of reauthentication should move 522 [from Section 2 to Section 5, and should take into account session credential strength |
| 14 | | | - | AAL3 requires FIPS. Additional clarification is required as to whether that is consistent with other areas |
| | can | 2.2.2 (-12 25121 | _ | of the standard or if it should have the federal agencies caveat and/or the "relevant standards" |
| 15 | 63B | 2.3.2 (aal3 verification) | 8 | 606 qualifier. The "reauthentication" row doesn't match the details in 2.2.3 and 2.3.3. There are no "shall" inactivity |
| | | | | requirements at any AAL; only "should". This should be revised to (e.g.) "24 hours overall (required), 1 |
| 16 | 63B | 2.5 (summary table) | 10 | Fig. 1 hour inactivity (recommended)". |
| | | | | The document considers only two types of out-of-band (secondary) devices: those that generate (or |
| | | | | receive from the CSP) a secret that the user then needs to transfer to the primary device, and those |
| | | | | that accept a secret from the user that the user got from the primary device. |
| | | | | Another, third (and rather popular), form of out-of-band device use is for the out-of-band device to |
| | | | | simply let the user confirm the sign-in (e.g. Duo Push (https://duo.com/product/multi-factor- |
| | | | | authentication-mfa/authentication-methods/duo-push) or Google Prompt (Inttus:/support.google.com/accounts/answet/7026/66/hlen), et.c.). This form has equivalent security |
| 17 | 63B | 3.1.3 (Out-of-Band Devices) | 17 | Inttps://support.google.com/accounts/answer/ /uze/zo-rini=nh, etc.j. inis rorm has equivalent 857 properties to the two methods already mentioned in the document and should be documented as well. |
| | | | | |

| | _ | | | | | Water Class Barbara and Calendar Annual Control of the Control of |
|------|------------|-----|---|------|-------|---|
| | | | | | | "verifier SHALL limit consecutive failed authentication attempts using one or more specific |
| | | | | | | authenticators on a single subscriber account to no more than 100" |
| | | | | | | Greater clarification is required around how long this is intended to last (eg, is this "forever") and what |
| 10 | 63B | | 3.2.2 (throttling) | 28 | 1211 | Greater Lamination is required around now only this intended to tast (e.g. in the order) and what resets it (e.g. any successful author just one wing that specific authenticator)? |
| 10 | 5 036 | | s.z.z (tillottillig) | 20 | 1211 | Tesets it (eg., any successituation in pactive using interest processity (eg., any successituation) and the second interest calculation is required to expand on what this means and whether it should just be |
| 10 | 63B | 2 | 3.2.9 (restricted authenticators) | 35 | 1/131 | informative. |
| 15 | 036 | | s.2.9 (restricted autrienticators) | 33 | 1431 | Informative: "For authenticators that are usable at AAL3, verification of activation secrets SHALL be performed in a |
| | | | | | | no administration and an essation at ANLS, verification to activation secrets struct to performed in a hardware-protected environment (e.g., a secure element, TPM, or TEE). At AAL2, if a hardware- |
| | | | | | | protected environment is not used, the authenticator SHALL use the activation secret to derive a key |
| | | | | | | used to decrypt the authentication key." |
| | | | | | | used to bedrypt the authentication key. |
| | | | | | | Greater clarification is required as this could be deemed excessive given that a biometric activation can |
| 20 | 63B | 3 | 3.2.10 (activation secrets) | 35 | 1461 | satisfy AAL3. |
| - 20 | 000 | | SELECTION (GENERAL COS) | - 55 | 1101 | This seems to generally assume "wireless" means RF communication (other than the mention of optical |
| | | | | | | transmission of a secret). Is it sufficiently general or should it explicitly mention the possibility of optical |
| | | | | | | (visible or IR), audio, magnetic, or other potential wireless links? Similarly, would a pairing code on a |
| 21 | 1 63B | 3 | 3.2.11.2 (wireless connections) | 37 | 1506 | magnetic stripe be acceptable under bullet (2)? |
| | | | , | | | "When any new authenticator is bound to a subscriber account, the CSP SHALL ensure that the process |
| | | | | | | requires authentication at either the maximum AAL currently available in the subscriber account or the |
| | | | | | l | maximum AAL at which the new authenticator will be used, whichever is lower. For example, binding |
| | | | | | l | an authenticator that is suitable for use at AAL2 requires authentication at AAL2 unless the subscriber |
| | | | | | l | account currently has only AAL1 authentication capability." |
| | | | | | | |
| | | | | | | Greater clarififcation is required related to the process for upgrading a subscriber from AAL1 to AAL2, |
| | | | | | 1 | as this example seems to contradict the "shall" in the preceding sentence. For example, 4.2.2.2 (below) |
| | | | | | 1 | could be read to mean that a password plus a recovery code can establish a session in which the |
| | | | | | | subscriber can bind an AAL2 authenticator, or read another way, they could "just bind one" if they |
| 22 | 2 63B | 4 | 1.1.2.1 (binding an additional authenticato | 40 | 1600 | currently only have AAL1 capability. |
| | | | , , | | | |
| | | | | | | This section should explicitly discuss phishing-resistant ways of binding an external authenticator. Right |
| | | | | | | now, the methods described in Section 4.1.2.2 are phishable. But phishing-resistant methods exist: for |
| | | | | | | example, today a user can choose to create a passkey on a primary device (say, a laptop), and choose to |
| | | | | | | have the passkey created on their external authenticator (mobile phone). The hybrid CTAP protocol |
| | | | | | | allows for this to happen in a phishing-resistant manner. This approach is already discussed in section |
| | | | | | | 3.2.11.2 in the context of using an external authenticator, and should similarly be discussed here in the |
| 23 | 63B | 4 | 1.1.2.2 (External Authenticator Binding) | 40 | 1616 | context of binding an external authenticator. |
| | | | | | | Clarify whether IAL1 proofing is required to reach AAL2. It looks like password + a code allows |
| 24 | 4 63B | 4 | 1.2.2.2 (recovery at aal2) | 40 | 1616 | establishment of an AAL2, but see question on Sec 4.1.2.1 above. |
| | | | | | | |
| | | | | | | Greater clarification is required around derived sessions and session bindings as it relates to 63B, 5.1, |
| | | | | | | and more specifically as it relates to the relationship between (e.g.) apps or stateful tools acting on |
| | | | | | | behalf of a user and "sessions". For example, Sec 5.1.2 (access tokens) says "The OAuth access token |
| | | | | | | and any associated refresh tokens could be valid long after the authentication session has ended and |
| | | | | | | the subscriber has left the application" and Sec 5.1 (session bindings) says "A session SHOULD inherit |
| | | | | | | the AAL properties of the authentication event that triggered its creation." For example, if a user signs |
| | | | | | 1 | into an email client, can it check for new mail and notify the user about it after the idle timeout? |
| | | | | | | |
| | | | | | | Also, it is not clear why session secrets such as cookies should be deleted when a device reboots or an |
| | | | | | | app restarts, even if the time limit or inactivity limit has not been reached yet. Furthermore, this |
| | | | | | | recommendation could be improved by taking into account the security of the session credential and |
| | | | | | | providing additional clarification. For example, should a DBSC-bound cookie be subject to the same |
| | | | | | 1 | deletion requirements as a normal bearer-token cookie? This section should be brought in line with |
| | | | | | | accepted practices (and soften the language perhaps to a MAY, or completely remove the non- |
| | | _ | d for a star beautiful a | | 40 | retention part), and make sessions credential deletion dependent on the security of the session |
| 25 | 63B | . 5 | 5.1 (session bindings) | 48 | 18/9 | credential. Think our for addressing amounted distinct. However, the earlier amount of them. Creater |
| | | | | | 1 | Thank you for addressing managed devices. However, there is no other mention of them. Greater |
| 20 | 63B | _ | 5.2 (reauth footnote 1) | 51 | 1070 | clarification is required as to how they relate to reauth. For example, it would be nice to allow unlocking of a managed device to satisfy reauth after an idle-timeout. |
| | 63B 63B | | Appendix B4 | 90 | | or a manageo device to satisty reaum arter an ide-timeout. This appends mentions a Table 5, which doesn't seem to exist in the document |
| 21 | 038 | | пррепиіл вч | 90 | 2594 | This appendix menous a robe 5, when obesit a seen to exist in the obtained. |
| | | | | | | Request guidance in relation to "the key material used to authenticate the RP and IdP to each other is |
| | | | | | | Insequest government relations to the Rey inserting used to destinate the relation to the relation to the Rey inserting used to the relation to the relation to the Rey and (dr) in a static fashion using a trusted mechanism". |
| | | | | | 1 | associated with the identifiers for the RP and tup in a static fashion using a discrete mechanism . Change recommended: strike out 'in a static fashion' given that contradicting guidance regarding OIDC key discovery is |
| | | | | | | The language above creates uncertainty about the usage of published SAML XML metadata and OIDC The language above creates uncertainty about the usage of published SAML XML metadata and OIDC The language above creates uncertainty about the usage of published SAML XML metadata and OIDC The language above creates uncertainty about the usage of published SAML XML metadata and OIDC The language above creates uncertainty about the usage of published SAML XML metadata and OIDC The language above creates uncertainty about the usage of published SAML XML metadata and OIDC The language above creates uncertainty about the usage of published SAML XML metadata and OIDC The language above creates uncertainty about the usage of published SAML XML metadata and OIDC The language above creates uncertainty about the usage of published SAML XML metadata and OIDC The language above creates uncertainty about the usage of published SAML XML metadata and OIDC The language above creates uncertainty about the usage of published SAML XML metadata and OIDC The language above creates uncertainty about the usage of published SAML XML metadata and OIDC The language above creates uncertainty about the usage of published SAML XML metadata and OIDC The language above creates uncertainty about the usage of published SAML XML metadata and OIDC The language above creates uncertainty about the usage of published SAML XML metadata and OIDC The language above creates uncertainty about the usage of published SAML XML metadata and OIDC The language above creates uncertainty about the usage of published SAML XML metadata and OIDC The language above creates uncertainty above the usage of published SAML XML metadata and OIDC The language above creates uncertainty above the usage of published SAML XML metadata and OIDC The language above creates uncertainty above the usage of published SAML XML metadata and OIDC The language of the usage of the usage of published SAML XML metadata and OIDC The language of the usage of the usage of the |
| 26 | 8 63C | | 2.4 (FAL3) | 6 | 5/19 | The language above creates uncertainty about the usage of published 3-Mit. Ant. Included and Oric. See discovery. See discovery. See use fashion at runtime, such as through an HTTPS URL, bosted by the IdP." |
| 20 | , 050 | | | - 0 | 540 | Reguest normative guidance for protocol specific xAL identifiers. For example an RP may signal xAL Request normative guidance for protocol specific xAL identifiers. For example an RP may signal xAL |
| | | | | | | requirements to the IdP. For example OIDC acr. values parameters such as acr. values-valued (al.1 |
| 79 | 9 63C | | 2.5 | 6 | 573 | aal2 fal3). |
| 23 | - 1000 | | 2.3 | - 0 | 5/5 | parameter series for |

| require or method patterns for proteint and each of a security or many for the "designed or works and patterns" or many for the "designed or works and "a security or "a se | | | | | |
|---|----|---|------|---|---|
| socializing if accordinate control considerations or excellence in proceedings in companies of the excellence in the control c | | | | | |
| As in contraction on the production of the first of the production of the first of the production of the first of the firs | | | | | |
| The start Series of American Ser | | | | | |
| In the content of the | | | | | |
| and a "read" or "fall" planted District Action (Part Section 1) in this data may be used fixed for information must be uncertainty for a read or greatly given, filter as examinate or data and or required datas provide management of the provided planted or provided as a provided planted or provided planted or provided planted or provided planted planted or provided planted planted or provided planted pla | | | | | |
| Annual control of the | | | | | |
| section of the property of the | | | | such as "pwd" or "mfa" (reference). | |
| section of the property of the | | | | | |
| Select 12 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 | | | | | |
| NOTE: Comparison of the properties of the pro | | | | | |
| 20 INC 2 Stage / Sta | | | | guidance on if OIDC eKYC-IDA [2] identifiers [3] are sufficient for transmitting IAL verified claims. | |
| 20 INC 2 Stage / Sta | | | | | |
| 30 GC 25 7 7 7 19 18 International control of the c | | | | [1] https://openid.net/specs/openid-connect-4-identity-assurance-1_0-16.html | |
| Figure and contribution of the contribution of | | | | [2] https://openid.net/specs/openid-ida-verified-claims-1_0.html | |
| Service of the servic | 30 | 63C 2.5 7 | 576 | [3] https://bitbucket.org/openid/ekyc-ida/wiki/identifiers | |
| Signature (S. Company) and search from the Cell of the St. Company) and search from the Cell of the St. Company (S. Company) and search from the Cell of the St. Company) and search from the Cell of the St. Company (S. Company) and search from the Cell of the St. Company) and search from the Cell of the St. Company (S. Company) and search from the Cell of the St. Company) and search from the Cell of the St. Company (S. Company) and search from the Cell of the St. Company) and search from the Cell of the St. Company (S. Company) and search from the Cell of the St. Company) and search from the Cell of the St. Company (S. Company) and search from the Cell of the St. Company) and search from the Cell of the St. Company (S. Company) and search from the Cell of the Cell of the St. Company) and search from the Cell of the St. Company (S. Company) and search from the Cell of the St. Company) and search from the Cell of the St. Company (S. Company) and search from the Cell of the St. Company) and search from the Cell of the St. Company (S. Company) and the St. Company (S. Company) a | | | | "Federated identifiers SHALL contain no plaintext personally-identifiable information (PII), such as | |
| 13 ISC 3.1 (Independ widersifiers of 15 a) 20 Interpretate decorate price to both the second to such a same board of 15 a Interpretate and the second to such a same board of 15 a Interpretate and the second second to such a same board of 15 a Interpretate and the second seco | | | | usernames, email addresses, or employee numbers, etc." - Email SAML NameIDs are common in | |
| The tract agreement value on the city of the calcorative and of the calcorative and on the city of the calcorative and the city of the city of the calcorative and the city of the city o | | | | Enterprise SSO. Suggest relaxing this at least in FAL1 and possibly in higher levels when the assertion is | |
| The tract agreement value on the city of the calcorative and of the calcorative and on the city of the calcorative and the city of the city of the calcorative and the city of the city o | 31 | 63C 3.3 (federated identifiers) 14 | 807 | | |
| Second Content of the Content of t | | 3.5 (.553.513.513.513.513.513.513.513.513.513 | | | |
| 32 (E.K. 3.1. 19 Set International Control Con | | | | | |
| First for being provisioned, the PP subscriber account due to a password or other direct condental is associated with a subscriber account at the PP of the substitution of the PP and the State of | 32 | 630 3.4 17 | 894 | | |
| pt to RP? The Section contemplates convairs where a password or other direct credential is associated with a substance account at the RP that was sittably a beloested account. It cleans to proclude the case where an existing pulstorithe account at the RP that was sittably a beloested account. It cleans to proclude the case where an existing pulstorithe account at the RP that was sittably a beloested account. It cleans to proclude the case where an existing pulstorithe account of the RP and a corresponding before cell desiration. We want to the RP and a corresponding before cell desiration. We want to the RP and a corresponding before cell desiration and the substance of the RP and a corresponding before cell desiration. We want to the RP and a corresponding before cell desiration and the substance of the RP and a corresponding before country. The RP stalked resource of the RP and the RP a | 32 | 3.4 1/ | 0.54 | | |
| This section contemplates seeman where a password or other direct credential is associated with a season and an activity and control of the c | | | | | |
| substorces are consumer at the Pit was as stratily a federated account. It seems to preclude the scale and before a control with an infer and accompanied pederated destination and the pit and accompanied pederated destination. We suggest that the being support to control to an infer and accompanied pederated destination and the size accompanied pederated destinations and existing and the size accompanied pederated destinations and existing and the size accompanied pederated destinations and existing and accompanied pederated destinations and existing six accorded an accompanied pederated destination and existing six accorded an accordance accordance and pederated pederat | | | | ot the M . | |
| substorces are consumer at the Pit was as stratily a federated account. It seems to preclude the scale and before a control with an infer and accompanied pederated destination and the pit and accompanied pederated destination. We suggest that the being support to control to an infer and accompanied pederated destination and the size accompanied pederated destinations and existing and the size accompanied pederated destinations and existing and the size accompanied pederated destinations and existing and accompanied pederated destinations and existing six accorded an accompanied pederated destination and existing six accorded an accordance accordance and pederated pederat | 1 | | | This section contemplates scenarios where a password or other direct credential is associated with a | |
| in ensing subschiera excount at the PB (using direct authentication) on be later associated with an in Direct and companies, the proposition of the later associated with an in Direct and companies. 33 (S)C 3.7 28 3107 [Referred destination as companies.] 14 66 F SMALL essure that the sub-ensicator companies in the sub-ensicator companie | 1 | | | | |
| D'or and a corresponding federated defentifier. We suggest that the language be changed to indicate that this abox acceptible is abox acceptible. 33 (SC 3.7 24) 100 Received defentifier. We suggest that the language be changed to indicate that this abox acceptible is abox acceptible. The support of indicate that the submitted control is a support of the PS subcriber account." The use of "indicates" or making or with a specific subscriber at all in a support of the PS subcriber account." The use of "indicates" for making exists a subscriber at all in a support of the PS subcriber account." The use of "indicates" for making exists a subscriber at all in a submitted to when uniqueness improves the PS subcriber account." The use of "indicates" in the provision of a submitted to when uniqueness improves the PS subcriber and the part of the PS subcriber account." A submitted subscriber at all in a submitted to when uniqueness improves the PS subcriber account. The use of "indicates" in the PS subcriber account. The use of "indicates" in the PS subcriber account. The use of "indicates" in the PS subcriber account. The use of "indicates" in the PS subcriber account. The use of "indicates" in the PS subcriber account. The use of "indicates" in the PS subcriber account. The use of "indicates" in the PS subcriber account. The use of "indicates" in the PS subcriber account. The use of "indicates" in the PS subcriber account. The use of "indicates" in the PS subcriber account. The use of "indicates" in the PS subcriber account. The use of "indicates" in the PS subcriber account. The use of "indicates" in the PS subcriber account. The use of "indicates" in the PS subcriber account. The use of "indicates" in the PS subcriber account. The use of "indicates" in the PS subcriber account. The use of "indicates" in the PS subcriber account. The use of "indicates account." The use of "indicates account." In the use of "indicate | 1 | | | | |
| this is also acceptable. this is also acceptable. the same of property in the proposal process and the company of the proposal process and the company of the proposal process and the pro | 1 | | | | |
| We have similar questions where Set. 4.8.3 says. "The provisioned accounts' SHALL be bound to a 13 SEC 3.7 19 SEC | 1 | | | | |
| 33 GE 3.7 24 100 federated identifier at the time of provisioning." **The PS FIALL ensure that the authenticator can be uniquely resolved to the RP subscriber account." **The Vision of Strategy Provision of the Strategy Prov | | | | this is also acceptable. | |
| 33 GE 3.7 24 100 federated identifier at the time of provisioning." **The PS FIALL ensure that the authenticator can be uniquely resolved to the RP subscriber account." **The Vision of Strategy Provision of the Strategy Prov | | | | | |
| "the RP SHALL ensure that the authenticator can be uniquely resolved to the RP subscriber account" The use of "imigratify here pind the requirement of associating is with a specific subscriber and subscriber and the size of the control of the state of | | | | | |
| The use of "uniquely" here (and the requirement of associating it with a specific subscriber at all) is likely to be problematic for machine certs. Grotate clarification is required related to when uniqueness improves the IA. For campile, include it be subficient for the SM and in a for the RP subfit 16, a second control of the subscriber used the same compared for the IAP and in a for the RP subfit 16, a second control of the SM and in a for the RP subfit 16, a second control of the SM and in a for the RP subfit 16, a second control of the SM and in a for the RP subfit 16, a second control of the SM and in a for the RP subfit 16, a second control of the SM and in a for the RP subfit 16, a second control of the SM and in a second control of the | 33 | 63C 3.7 24 | 1107 | federated identifier at the time of provisioning." | |
| The use of "uniquely" here (and the requirement of associating it with a specific subscriber at all) is likely to be problematic for machine certs. Grotate clarification is required related to when uniqueness improves the IA. For campile, include it be subficient for the SM and in a for the RP subfit 16, a second control of the subscriber used the same compared for the IAP and in a for the RP subfit 16, a second control of the SM and in a for the RP subfit 16, a second control of the SM and in a for the RP subfit 16, a second control of the SM and in a for the RP subfit 16, a second control of the SM and in a for the RP subfit 16, a second control of the SM and in a for the RP subfit 16, a second control of the SM and in a second control of the | 1 | | | | |
| likely to be problematic for machine certs. Creating children to set sufficient at least is some cases for the RP to be confident than the subscriber used the same computer for the life auch is a for the RP auch? E.g., a 15 (Sct of More employee uses a shared criminal in a scant of certifier.) 35 (SC 3.15 (bound authenticators) 37 (15 (Sct of More employee) and subscriber used the same computer for the life auch is a for the RP auch? E.g., a 15 (Sct of More employee) and subscriber used the same handware key for two accounts is likely to be satisfactory, at least at come FALS. Setting a setting a setting a setting and subscriber used the same handware key for two accounts is likely to be satisfactory, at least at come FALS. Setting a setting a setting a setting a setting and subscriber to setting and subscriber to setting a setting and subscriber to setting and subscriber to setting and look above this susce. The trust agreement many require an infer can ensure a subscriber uses a specific bound authenticator in some and subscriber to set and the setting and subscriber to setting and look based insurance. The trust agreement many require an infer can ensure a subscriber used in least setting a look based insurance. The trust agreement many require an life P can ensure a subscriber used in least setting a look based insurance. The trust agreement many require an life P can ensure a subscriber used in least setting a look based insurance. If this proposal is accepted normality or informative quidance for implementers is appreciated as the diff and of the manage bound authenticators are restricted to a specific based of reversaries and existing a standardized dains for holder of key assertion is stand for the subscriber is superior and look as the subscriber used in least standard and least set of the subscriber and authenticator and authenticator at a stent of bound authenticator and authenticator at a stent of bound authenticator in a stent of bound authenticator in a stent of bound authenticator in a st | | | | "the RP SHALL ensure that the authenticator can be uniquely resolved to the RP subscriber account" | |
| likely to be problematic for machine certs. Creating children to set sufficient at least is some cases for the RP to be confident than the subscriber used the same computer for the life auch is a for the RP auch? E.g., a 15 (Sct of More employee uses a shared criminal in a scant of certifier.) 35 (SC 3.15 (bound authenticators) 37 (15 (Sct of More employee) and subscriber used the same computer for the life auch is a for the RP auch? E.g., a 15 (Sct of More employee) and subscriber used the same handware key for two accounts is likely to be satisfactory, at least at come FALS. Setting a setting a setting a setting and subscriber used the same handware key for two accounts is likely to be satisfactory, at least at come FALS. Setting a setting a setting a setting a setting and subscriber to setting and subscriber to setting a setting and subscriber to setting and subscriber to setting and look above this susce. The trust agreement many require an infer can ensure a subscriber uses a specific bound authenticator in some and subscriber to set and the setting and subscriber to setting and look based insurance. The trust agreement many require an infer can ensure a subscriber used in least setting a look based insurance. The trust agreement many require an life P can ensure a subscriber used in least setting a look based insurance. The trust agreement many require an life P can ensure a subscriber used in least setting a look based insurance. If this proposal is accepted normality or informative quidance for implementers is appreciated as the diff and of the manage bound authenticators are restricted to a specific based of reversaries and existing a standardized dains for holder of key assertion is stand for the subscriber is superior and look as the subscriber used in least standard and least set of the subscriber and authenticator and authenticator at a stent of bound authenticator and authenticator at a stent of bound authenticator in a stent of bound authenticator in a stent of bound authenticator in a st | | | | | |
| mproves the FAL For example, shouldn't the sufficient at least as some cases for the RP to be' confident that the subscriber used this amake on the BP at the BP and T Eg., a 1 170 (Sectory floor employee uses a shared terminal as secured facility. A bown admitted and admitted | | | | | |
| onlident that the subscriber used the same compare for the file year has for the RP auth? E.g., a 3.14 (Hool) 37 1570 (Earch of complayer used a shared arminal in a secured a failty. A bound authenticators SHALL be unique per subscriber at the RP". A show, greater districtions in required as to which a shared to make a shared arminal in a secured failty. A show, greater districtions in required as to which a shared to the RP as | | | | likely to be problematic for machine certs. Greater clarification is required related to when uniqueness | |
| 34 ISC 3.1.5 (bound authenticators) 37 1570 factory floor employee uses a shared terminal in a secured facility. *A bound authenticators at the second authenticator of the statistic of the bund authenticator is the bund authenticator is the bund authenticator | | | | improves the FAL. For example, shouldn't it be sufficient at least in some cases for the RP to be | |
| "A bound authenticator SHALL be unique per subscriber at the 8P". As above, greater clarification is required as to why this is a "SHALL" since it seems overly strict; using 1550 libe same hardware key for two accounts is likely to be satisfactory, at least at some FALs. features in FIDO/WebAuth that have been implemented in browsers [1] that enable individual attention of enterprise corrolled subscriber consent behavior [2]). Des such as Microsoft fature 10 support authenticator attestation [3] and vendors such as Yubios outport enterprise attestation [4] and vendors such as Yubios outport enterprise attestation [5] and vendors such as Yubios outport enterprise attestation [6] and vendors such as Yubios outport enterprise attestation [7] and vendors such as Yubios outport enterprise attestation [7] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestation [8] and vendors such as Yubios outport enterprise attestati | | | | confident that the subscriber used the same computer for the IdP auth as for the RP auth? E.g., a | |
| As above, greater clarification is required as to why this is a "SHALL" since it seems overly strict; using 1952 the same hardware key for two accounts is likely to be satisfactory, at least at some FALS. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some FALS. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some FALS. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some FALS. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some FALS. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some FALS. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some FALS. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some FALS. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some FALS. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some falls. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some falls. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some falls. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some falls. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some falls. Seems of the same hardware key for two accounts is likely to the satisfactory, at least at some falls. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some falls. Seems of the same hardware key for two accounts is likely to the satisfactory, at least at some falls. Seems of the same hardware key for two accounts is likely to the satisfactory, at least at some falls. Seems of the same hardware key for two accounts is labely and accounts the same and same falls | 34 | 63C 3.14 (HoK) 37 | 1570 | | |
| As above, greater clarification is required as to why this is a "SHALL" since it seems overly strict; using 1952 the same hardware key for two accounts is likely to be satisfactory, at least at some FALS. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some FALS. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some FALS. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some FALS. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some FALS. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some FALS. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some FALS. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some FALS. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some FALS. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some falls. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some falls. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some falls. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some falls. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some falls. Seems of the same hardware key for two accounts is likely to the satisfactory, at least at some falls. Seems of the same hardware key for two accounts is likely to be satisfactory, at least at some falls. Seems of the same hardware key for two accounts is likely to the satisfactory, at least at some falls. Seems of the same hardware key for two accounts is likely to the satisfactory, at least at some falls. Seems of the same hardware key for two accounts is labely and accounts the same and same falls | | | | "A bound authenticator SHALL be unique per subscriber at the RP". | |
| 35 SC 3.15 (bound authenticators) 38 1992 the same hardware key for two accounts is likely to be astificatory, at least at some FALS. 15 status in FIDO2004-bouthen that have implemented in browners [13] that enable individual statistation of enterprise encolled authenticators (with enterprise controlled subscriber consent behavior [21], left, so that some controlled subscriber content behavior [21], left, so that some controlled subscriber content behavior [21], left, so that some controlled subscriber content and the source of the controlled subscriber controlled subscriber content and the source of the controlled subscriber controlled subs | | | | , , | |
| 35 SC 3.15 (bound authenticators) 38 1992 the same hardware key for two accounts is likely to be astificatory, at least at some FALS. 15 status in FIDO2004-bouthen that have implemented in browners [13] that enable individual statistation of enterprise encolled authenticators (with enterprise controlled subscriber consent behavior [21], left, so that some controlled subscriber content behavior [21], left, so that some controlled subscriber content behavior [21], left, so that some controlled subscriber content and the source of the controlled subscriber controlled subscriber content and the source of the controlled subscriber controlled subs | | | | As above, greater clarification is required as to why this is a "SHALL" since it seems overly strict; using | |
| features in FIDO2/WebAuthth that have been implemented in browsers (1) that enable individual attestation of enterprise enrolled authenticators (with enterprise controlled subscriber consent behavior (2)), left's such as Microsoft Entra 10 support authenticator attestation (3) and vendors such as Yubico support enterprise attestation (4) in addition to batch attestation. This proposal provides a middle ground between subscriber managed bound authenticator issuance and the subscriber subscriber such as specific bound authenticator is for the RP with the first in the PR is present in both the did and authenticator allowists. Where enterprise attestation is not possible, both attestation still serves to reduce the likelihood that an unknown bound authenticator is subscribed as the lidP and RP must agree on a method of conveying standardized claims for hideor of the subscriber account at the RP as bound authenticators are restricted to a specific batch of vendor authenticators. If this proposal is accepted normative or informative guidance for implementers is appreciated as the lidP and RP must agree on a method of conveying standardized claims for hideor of the subscriber account at the RP as bound authenticators are restricted to a specific batch of vendor authenticators. If this proposal is accepted normative or informative guidance for implementers is appreciated as the lidP and RP must agree on a method of conveying standardized claims for hideor in the subscriber account at the RP as bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (13.6.1), and bound authenticator informative examples (10.7). [1] https://www.chronium.org/security-keys/ [2] https://chromeenterprise google-plocles/#Security-keys/ [2] https://chromeenterprise google-plocles/#Security-keys/ [2] https://chromeenterprise google-plocles/#Security-keys/ [2] https://chromeenterprise google-plocles/#Security-keys/ [2] https://chromeenterpr | 35 | 63C 3.15 (bound authenticators) 38 | 1592 | | |
| attestation of enterprise an Arichard Enterprise controlled subscriber consent behavior (2) Lidds such an Microal Fatter 10 support enterprise attestation (3) and vendors such as Yubico support enterprise attestation (3) in addition to batch attestation. This proposal provides a middle ground between subscriber managed bound authenticator issuance. The trust agreement may require an IdP can present in the IdP and authenticator allowists. Where enterprise attestation is not possible, batch attestation still serves to reduce the likelihood that an unknown bound authenticator account at the RP as bound authenticators are restricted to a specific batch of vendor authenticators. If this proposal is accepted normative or informative guidance for implementers is appreciated as the IdP and RP must agree on a method of conveying attestation certificate information and existing standardized claims for holder of key assertions such as the IoO Cort (5) and Sc (5) claims may be misinterpreted by a RP as a holder of key assertion instead of conveyance of bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (13.6.1), and bound authenticator informative examples (10.7). The trust agreement may require an IdP MAY identify the bound authenticator or a batch of bound authenticator is sushed to be considered alongside feedback about trust agreements (3.4), RP requirements (13.6.1), and bound authenticator informative examples (10.7). The trust agreement may require an IdP MAY identify the bound authenticator or a batch of bound authenticator is sush of RPS of the proposal authenticator is sush of RPS of the proposal authenticator is sush of RPS of the PS of the Alterstation of PS of the SP of the Alterstation of the SP of the Alterstation certificate the Uniform in addition to the bound authenticator certificate the Uniform in addition to the bound authenticator or a batch in fow. The trust agreement may require an IdP MA | 33 | 5.25 (554.15 454.161.161.151) 55 | 1332 | | |
| behavior [2]). IdPs such suffices of text to 18 support authenticator attestation [8] and vendors such as Vabios support enterprise attestation [8] in addition to back attestation. This proposal provides a middle ground between subscriber managed bound authenticator issuance and kiook based issuance. The trust agreement may require an idP and sure and issuance and kiook based issuance. The trust agreement may require an idP and sure the idP and subscriber uses a specific bound authenticator slowlist. Where enterprise attestation is not public buth attestation is susued for the subscriber account at the RP as bound authenticators are restricted to a specific batch of vendor authenticators. If this proposal is accepted normative or informative guidance for implementers is appreciated as the loff and RP must agree on a method of conveying attestation certificate information and existing standardized claims for holder yeas-sertions used as the OIDC or [15] and as Sci [6] claims may be misinterpreted by a RP as a holder of key assertion instead of conveyance of bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements [3.4], RP requirements [13.5.1], and bound authenticator informative examples [10.7). (1) https://www.chromium.org/security-key/s [1] https://www.chromium.org/security-key/s [2] https://chromeenterprise.google/policies//Securitykey/PermitAttestation [3] https://chromeenterprise.google/policies//Securitykey/PermitAttestation [4] https://chromeenterprise.google/policies//Securitykey/PermitAttestation [5] https://chromeenterprise.google/policies//Securitykey/PermitAttestation [6] https://chromeenterprise.google/policies//Securitykey/PermitAttestation/concept-fido2-handware-vendor [6] https://chromeenterprise.google/policies//Securitykey/PermitAttestation/concept-fido2-handware-vendor [6] https://chromeenterprise.google/policies//Securitykey/PermitAttestation/concept-fido2-handware-vendor [6] https://chromeenterprise.google/po | | | | | |
| vulcio support enterprise attestation [4] in addition to batch attestation. This proposal provides a middle ground between subtre managed bound authenticator is suscerned when the PR is present in both the IdP and authenticator allowist. Where enterprise attestation is not possible, batch attestation still serve to reduce the filledhood that an unknown bound authenticator is issued for the subscriber account at the RP as bound authenticators are restricted to a specific batch of vendor authenticators. If this proposal is accepted normative or informative guidance for implementers is appreciated as the IdP and RP must agree on a method of conveying attestation certificate information and existing standardized claims for holder of key assertion instead of conveyance of bound authenticator attestation certificate. Note: this proposal is accepted normative or informative guidance for implementers is appreciated as the IdP and RP must agree on a method of conveying attestation certificate information and existing standardized claims for holder of key assertion instead of conveyance of bound authenticator attestation certificate. Note: this proposal is accepted normative or informative guidance for implementers is appreciated as the IdP and RP must agree on a method of conveying attestation certificate. Note: this proposal is accepted normative or informative guidance for implementers is appreciated as the IdP and RP must agree on a method of conveying attestation certificate. Note: this proposal is accepted by a RP as a holder of key assertion instead of conveyance of bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (3.6.1), RP requirements (3.6.1), RP requirements (3.6.1), AR proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (3.6.1), RP requirements (3.6.1), AR proposal is intended to be considered alongside feedback about trust agreements (3.4), RP | | | | | |
| middle ground between subscriber managed bound authenticator issuance and kiosk based issuance. The trust agreement may require an IdP can ensure the IdP at the RP when the RP is present in both the IdP and authenticator allowlist. Where enterprise attestation is not possible, both attestation sill serves to reduce the likelihood that an unknown bound authenticator issuance and unknown bound authenticators are restricted to a specific batch of vendor authenticators. If this proposal is accepted normative or informative guidance for implementers is appreciated as the IdP and RP must agree on a method of conveying attestation certificate information and existing standardized claims for holder of key assertions such as the OIDC crif [5] and x5c [6] claims may be misinterpreted by a RP as a holder of key assertions such as the OIDC crif [5] and x5c [6] claims may be misinterpreted by a RP as a holder of key assertion instead of conveyance of bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements [3.4], RP requirements [13.6.1], and bound authenticator informative examples (10.7). If trust agreement may require an IdP MAY identify the bound authenticator or a batch of bound authenticator is suance using an enterprise or batch attestation all the IdP as a part of RP bound authenticator is suance using an enterprise or batch attestation all the IdP as a part of RP bound authenticator to the RP if the Pis not present in the IdP's enterprise. If I https://levan.chronium.org/security-keys/ 1] https://levan.chronium.org/security-keys/ 2] https://levan.chronium.org/security-keys/ 3 https://levan.chronium.org/security-keys/ 3 https://developers.yulo.co.orm/WebAuthn/Concepts/Enterprise_Attestation alternation and verify the attestation certificate through in it addition to the Dound authenticator credentials from the bound authenticator and verify the attestation certificate throughmin in addition to the Dound authenticator and ver | 1 | | | | |
| The trust agreement may require an IdP can ensure a subscriber uses a specific bound authenticator known to the IdP at the RP when the RP is present in both the IdP and authenticator allowlist. Where enterprise attestation is not possible, batch attestation still serves to reduce the likelihood that an unknown bound authenticator is issued for the subscriber account at the RP as bound authenticators are restricted to a specific batch of vendor authenticators. If this proposal is accepted normative or informative guidance for implementers is appreciated as the idP and RP must agree on a method of conveying attestation certificate information and existing standardized claims for holder of key assertion is such as the OIDC off [5] and x5c [6] claims may be misinterpreted by a RP as a holder of key assertion instead of conveyance of bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements [3.4], RP requirements [13.6.1], and bound authenticator informative examples [10.7]. The trust agreement may require an IdP MAY identify the bound authenticator or a batch of bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements [3.4], RP requirements [13.6.1], and bound authenticator informative examples [10.7]. If https://www.chromium.org/security-key/ [2] https://schromeentreprise, google/policies/#SecurityKeyPermilAttestation [3] https://schromeentreprise, google/policies/#SecurityKeyPermilAttestation [3] https://developers.ycies/tablestation/concepts/fiedo2-hardware-vendor [4] https://developers.ycies/tablestation/concepts/fiedo2-hardware-vendor [4] https://developers.ycies/tablestation/concepts/fiedo2-hardware-vendor [4] https://developers.ycies/tablestation/concepts/fiedo2-hardware-vendor [4] https://developers.ycies/tablestation/concepts/fiedo2-hardware-vendor [4] https://developers.ycies/tablestation/concepts/fiedo2-hardware-vendor [4] https://developers.yci | 1 | | | | |
| known to the IdP at the RP when the RP is present in both the IdP and authenticator allowlist. Where enterprise attestation is not possible, batch attestation still serves to reduce the likelihood that an unknown bound authenticator is issued for the subscriber account at the RP as bound authenticators are restricted to a specific batch of vendor authenticators. If this proposal is accepted normative or informative guidance for implementers is appreciated as the IdP and RP must agree on a method of conveying attestation certificate information and existing standardized claims for holder of key assertion such as the OIDC or [5] and \$5.0 [6] claims may be misinterpreted by a RP as a holder of key assertion instead of conveyance of bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (13.6), and bound authenticator informative examples [10.7). The trust agreement may require an IdP MAY identify the bound authenticator or a batch of bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (13.6), and bound authenticator informative examples [10.7). If trust agreement may require an IdP MAY identify the bound authenticator or a batch of bound authenticator is susce using an enterprise or batch attestation certificate. The IdP MUST NOT identify a specific bound authenticator issuance using an enterprise or batch attestation certificate. The IdP MUST NOT identify a specific bound authenticator issuance using an enterprise or batch attestation allowlists or if disallowed by the trust agreement instead MUST present the bound authenticator attestation allowlists or if disallowed by the trust agreement instead MUST present the bound authenticator and verify the trust agreement instead MUST present the bound authenticator and verify the trust agreement in a did in the present in the IdP's enterprise attestation ce | 1 | | | | |
| enterprise attestation is not possible, batch attestation still serves to reduce the likelihood that an unknown bound authenticator is issued for the subscriber account at the RP as bound authenticators are restricted to a specific batch of vendor authenticators. If this proposal is accepted normative or informative guidance for implementers is appreciated as the IdP and RP must agree on a method of conveying attestation certificate information and existing standardized claims for holder of key assertions such as the OIDC cnf [5] and x5c [6] claims may be misinterpreted by a RP as a holder of key assertion instead of conveyance of bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (13.6.1), and bound authenticator informative examples (10.7). Note: this proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (13.6.1), and bound authenticator informative examples (10.7). [1] https://www.chromium.org/security-keys/ [2] https://chromeenterprise google/policies/#security-keyPermitAttestation [3] https://learn.org.fc.org.fc.org.ec.prise.pf.doz-hardware-vendor [4] https://developers.yubico.com/WebAuthn/Concepts/Enterprise_Attestation/ [4] https://developers.yubico.com/WebAuthn/Concepts/Enterprise_Attestation/ [5] https://developers.yubico.com/WebAuthn/Concepts/Ente | 1 | | | | |
| unknown bound authenticator is issued for the subscriber account at the RP as bound authenticators are restricted to a specific batch of vendor authenticators. If this proposal is accepted normative or informative guidance for implementers is appreciated as the IdP and RP must agree on a method of conveying attestation certificate information and existing standardized claims for holder of key assertion such as the OIDC cnf [5] and x5c [6] claims may be misinterpreted by a RP as a holder of key assertion instead of conveyance of bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (13.6.1), and bound authenticator informative examples (10.7). The trust agreement may require an IdP MAY identify the bound authenticator or a batch of bound authenticator is usance using an enterprise or batch attestation certificate. He IdP MUST NOTI dentify a specific bound authenticator to the RP if the RP is not present in the IdP's enterprise attestation allowists or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation allowists or if disallowed by the IdP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the attestation certificate thumbprint in addition to the bound authenticator credential public key such that the RP bound authenticator power and verify the attestation object using the attestation certificate thumbprint in addition to the bound authenticator credential public key such that the RP bound authenticator provided by the IdP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the attestation certificate thumbprint in addition to the bound authenticator certificate thumbprint in addition to the bound authenticator certificate thumbprint in addition to the bound authenticator redential public key such that the RP bound authenticator may be id | 1 | | | | |
| are restricted to a specific batch of vendor authenticators. If this proposal is accepted normative or informative guidance for implementers is appreciated as the IdP and RP must agree on a method of conveying attestation certificate information and existing standardized claims for holder of key assertions such as the OIDC cnf [5] and x5c [6] claims may be misinterpreted by a RP as a holder of key assertion instead of conveyance of bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (13.6.1), and bound authenticator informative examples (10.7). [1] https://www.chromium.org/security-keys/ [2] https://chromeenterprise_google/policies/#SecurityKeyPermitAttestation [3] https://chromeenterprise_google/policies/#SecurityKeyPermitAttestation [4] https://developers.yubico.com/WebAuthn/Concept-fido2-hardware-vendor and verificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verificate. When indicated provided by the IdP. The RP must store the attestation certificate. When indicated provided by the IdP. The RP must store the attestation certificate or attestation certificate thumbprint in addition to the bound authenticator credential public key such that the RP bound authenticator may be identified using IdP provided data in future FAL3 authentication flows. | 1 | | | enterprise attestation is not possible, batch attestation still serves to reduce the likelihood that an | |
| If this proposal is accepted normative or informative guidance for implementers is appreciated as the IdP and RP must agree on a method of conveying attestation certificate information and existing standardized claims for holder of key assertions such as the OIDC orf. [5] and x5c [6] claims may be misinterpreted by a RP as a holder of key assertion instead of conveyance of bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (13.6.1), and bound authenticator informative examples (10.7). The trust agreement may require an IdP MAY identify the bound authenticator or a batch of bound authenticator used by a subscriber to authenticate with the IdP as a part of RP bound authenticator or tent Pf ide RP is not present in the IdP in the RP is not present in the IdP in the RP is not present in the IdP in the RP is not present in the IdP in the RP is not present in the IdP in the RP is not not attestation certificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the steatation certificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the steatation certificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the steatation certificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the steatation certificate. When indicated by the IdP the RP is not present in the IdP | 1 | | | | |
| If this proposal is accepted normative or informative guidance for implementers is appreciated as the IdP and RP must agree on a method of conveying attestation certificate information and existing standardized claims for holder of key assertions such as the OIDC orf. [5] and x5c [6] claims may be misinterpreted by a RP as a holder of key assertion instead of conveyance of bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (13.6.1), and bound authenticator informative examples (10.7). The trust agreement may require an IdP MAY identify the bound authenticator or a batch of bound authenticator used by a subscriber to authenticate with the IdP as a part of RP bound authenticator or tent Pf ide RP is not present in the IdP in the RP is not present in the IdP in the RP is not present in the IdP in the RP is not present in the IdP in the RP is not present in the IdP in the RP is not not attestation certificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the steatation certificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the steatation certificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the steatation certificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the steatation certificate. When indicated by the IdP the RP is not present in the IdP | | | | are restricted to a specific batch of vendor authenticators. | |
| IdP and RP must agree on a method of conveying attestation certificate information and existing standardized claims for holder of key assertions such as the OIDC off [5] and x5c [6] claims may be misinterpreted by a RP as a holder of key assertion instead of conveyance of bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (13.6.1), and bound authenticator informative examples (10.7). Interview a previous and provided and authenticator or a batch of bound authenticator used by a subscriber to authenticate with the IdP as a part of RP bound authenticator issuance using an enterprise or batch attestation certificate. The IdP MUST NOT identify a subscriber to authenticate with the IdP as a part of RP bound authenticator is the SP if the RP is not present in the IdP is enterprise. The IdP MUST NOT identify and the IdP is the RP is not present the bound authenticator batch attestation allowlist or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation allowlist or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation allowlist or if disallowed by the IdP the RP SHALL attest generated credentials from the bound authenticator and verificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verificate. When indicate provided by the IdP. The RP must store the attestation certificate. When indicate provided by the IdP. The RP must store the attestation and verificate. When indicate provided by the IdP. The RP must store the attestation and verificate. When indicate provided by the IdP. The RP must store the attestation and verificate. When indicate the provided by the IdP. The RP must store the attestation and verificate. When indicate the provided by the IdP. The RP must store the attestation and verificate. When indicate on object is given the The PS SHALL attest | | | | | |
| IdP and RP must agree on a method of conveying attestation certificate information and existing standardized claims for holder of key assertions such as the OIDC off [5] and x5c [6] claims may be misinterpreted by a RP as a holder of key assertion instead of conveyance of bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (13.6.1), and bound authenticator informative examples (10.7). Interview a previous and provided and authenticator or a batch of bound authenticator used by a subscriber to authenticate with the IdP as a part of RP bound authenticator issuance using an enterprise or batch attestation certificate. The IdP MUST NOT identify a subscriber to authenticate with the IdP as a part of RP bound authenticator is the SP if the RP is not present in the IdP is enterprise. The IdP MUST NOT identify and the IdP is the RP is not present the bound authenticator batch attestation allowlist or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation allowlist or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation allowlist or if disallowed by the IdP the RP SHALL attest generated credentials from the bound authenticator and verificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verificate. When indicate provided by the IdP. The RP must store the attestation certificate. When indicate provided by the IdP. The RP must store the attestation and verificate. When indicate provided by the IdP. The RP must store the attestation and verificate. When indicate provided by the IdP. The RP must store the attestation and verificate. When indicate the provided by the IdP. The RP must store the attestation and verificate. When indicate the provided by the IdP. The RP must store the attestation and verificate. When indicate on object is given the The PS SHALL attest | | | | | |
| IdP and RP must agree on a method of conveying attestation certificate information and existing standardized claims for holder of key assertions such as the OIDC off [5] and x5c [6] claims may be misinterpreted by a RP as a holder of key assertion instead of conveyance of bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (13.6.1), and bound authenticator informative examples (10.7). Interview a previous and provided and authenticator or a batch of bound authenticator used by a subscriber to authenticate with the IdP as a part of RP bound authenticator issuance using an enterprise or batch attestation certificate. The IdP MUST NOT identify a subscriber to authenticate with the IdP as a part of RP bound authenticator is the SP if the RP is not present in the IdP is enterprise. The IdP MUST NOT identify and the IdP is the RP is not present the bound authenticator batch attestation allowlist or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation allowlist or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation allowlist or if disallowed by the IdP the RP SHALL attest generated credentials from the bound authenticator and verificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verificate. When indicate provided by the IdP. The RP must store the attestation certificate. When indicate provided by the IdP. The RP must store the attestation and verificate. When indicate provided by the IdP. The RP must store the attestation and verificate. When indicate provided by the IdP. The RP must store the attestation and verificate. When indicate the provided by the IdP. The RP must store the attestation and verificate. When indicate the provided by the IdP. The RP must store the attestation and verificate. When indicate on object is given the The PS SHALL attest | 1 | | | If this proposal is accepted normative or informative guidance for implementers is appreciated as the | |
| standardized claims for holder of key assertion such as the OIDC cnf [5] and x5c [6] claims may be misinterpreted by a RP as a holder of key assertion instead of conveyance of bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (13.6.1), and bound authenticator informative examples (10.7). [1] https://www.chromium.org/security-keys/ [2] https://chromeenterprise.google/policies/#SecurityKeyPermitAttestation [3] https://chromeenterprise.google/policies/#SecurityKeyPermitAttestation [4] https://chromeenterprise.google/policies/#SecurityKeyPermitAttestation [4] https://developers.yubico.com/WebAuthn/Concept-fido2-hardware-vendor and verify the attestation object using the attestation certificate by the ldP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the attestation certificate provided by the ldP. The RP must store the attestation certificate or attestation to certificate or attestation certificate or at | 1 | | | | |
| misinterpreted by a RP as a holder of key assertion instead of conveyance of bound authenticator attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (13.6.1), and bound authenticator informative examples (10.7). The trust agreement may require an IdP MAY identify the bound authenticator or a batch of bound authenticators used by a subscriber to authenticate with the IdP as a part of RP bound authenticator is using an enterprise or batch attestation certificate. The IdP MUST NOT identify a specific bound authenticator to the RP if the RP is not present in the IdP's enterprise. It has the IdP's enterprise. It has the IdP's enterprise. It is a treated in a lowering the attestation allowits or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation certificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the attestation certificate provided by the IdP. The RP must store the attestation certificate or attestation certificate or attestation to the bound authenticator received by the IdP. The RP must store the attestation certificate or attestation to the bound authenticator received by the IdP. The RP must store the attestation certificate or attestation certificate thumbprint in addition to the bound authenticator credential public key such that the RP bound authenticator may be identified using IdP provided data in future FAL3 authentication flows. | | | | | |
| attestation certificate. Note: this proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (13.6.1), and bound authenticator informative examples (10.7). The trust agreement may require an IdP MAY identify the bound authenticator or a batch of bound authenticator used by a subscriber to authenticate with the IdP as a part of RP bound authenticator to the RP fite RP is not present in the IdP's enterprise attestation attestation attestation allowlist or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation allowlist or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation allowlist or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation allowlist or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation allowlist or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation allowlist or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation allowlist or if disallowed by the trust agreement may require an IdP MAY identify the bound authenticator or a batch of bound authenticator used by a subscriber to authenticate with the IdP as a part of RP bound authenticator or the batch attestation allowlist or if disallowed by the trust agreement may require an IdP MAY identify and the part of RP bound authenticator or a batch of bound authenticator is attestation allowlist or if disallowed by the trust agreement may require an IdP MAY identify the bound authenticator or a batch of boun | 1 | | | | |
| Note: this proposal is intended to be considered alongside feedback about trust agreements (3.4), RP requirements (13.6.1), and bound authenticator informative examples (10.7). The trust agreement may require an IdP MAY identify the bound authenticator or a batch of bound authenticator used by a subscriber to authenticate with the IdP as a part of RP bound authenticator to the RP if the RP is not present in the IdP's enterprise attestation allowing or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation allowing or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation certificate. The IdP MUST NOT identify a specific bound authenticator to the RP if the RP is not present in the IdP's enterprise attestation allowing or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation certificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the attestation certificate provided by the IdP. The RP must store the attestation certificate provided by the IdP. The RP must store the attestation certificate provided by the IdP. The RP must store the attestation certificate provided by the IdP. The RP must store the attestation certificate provided by the IdP. The RP must store the attestation certificate provided by the IdP. The RP must store the attestation certificate provided by the IdP. The RP must store the attestation certificate provided by the IdP. The RP must store the attestation certificate provided by the IdP. The RP must store the attestation certificate provided by the IdP. The RP must store the attestation certificate provided by the IdP. The RP must store the attestation certificate provided by the IdP. The RP must store the attestation certificate provided by the IdP. The RP must store the attestation certificate provided by the IdP. The RP must store the attestation certif | 1 | | | | |
| requirements (13.6.1), and bound authenticator informative examples (10.7). subscriber to authenticate with the IdP as a part of RP bound authenticator issuance using an enterprise or batch attestation certificate. The IdP MUST NOT identify a specific bound authenticator to the RP if the RP is not present in the IdP's enterprise attestation allowists or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation certificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verificate using the attestation certificate provided by the IdP. The RP must store the attestation certificate or attestation to extend the IdP the RP standard or and verificate provided by the IdP. The RP must store the attestation certificate or attestation certificate or attestation certificate or attestation to extificate or attestation to the bound authenticator credential public key such that the RP bound authenticator may be identified using IdP provided data in future FAL3 authentication flows. | | | | | |
| requirements (13.6.1), and bound authenticator informative examples (10.7). subscriber to authenticate with the IdP as a part of RP bound authenticator issuance using an enterprise or batch attestation certificate. The IdP MUST NOT identify a specific bound authenticator to the RP if the RP is not present in the IdP's enterprise attestation allowists or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation certificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verificate using the attestation certificate provided by the IdP. The RP must store the attestation certificate or attestation to extend the IdP the RP standard or and verificate provided by the IdP. The RP must store the attestation certificate or attestation certificate or attestation certificate or attestation to extificate or attestation to the bound authenticator credential public key such that the RP bound authenticator may be identified using IdP provided data in future FAL3 authentication flows. | 1 | | | Note: this proposal is intended to be considered alongside feedback about trust agreements (2.4). BB | The trust agreement may require an IdP MAY identify the hound authoriticator or a batch of bound authoriticator used by a |
| certificate. The IdP MUST NOT identify a specific bound authenticator to the RP if the RP is not present in the IdP's enterprise attestation allowists or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation certificate. When indicated by the difference of the provided provided the ABS Hall Latest generated credentials from the bound authenticator and verify the attestation certificate under the provided by the IdP. The RP must store the attestation of and verify the attestation object using the attestation certificate provided by the IdP. The RP must store the attestation of certificate under the provided by the IdP. The RP must store the attestation of and verify the attestation certificate thumbprint in addition to the bound authenticator credential public key such that the RP bound authenticator may be identified using IdP provided data in future FAL3 authentication flows. | 1 | | | | |
| [1] https://www.chromium.org/security-keys/ attestation allowlist or if disallowed by the trust agreement and instead MUST present the bound authenticator batch attestation certificate. When indicated by the ldP the RP SHALL attest generated credentials from the bound authenticator and series of the state attention colect using the attestation certificate. When indicated by the ldP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the attestation conclusted provided by the ldP. The RP must store the attestation allowlist or if disallowed by the ldP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the attestation certificate provided by the ldP. The RP must store the attestation allowlist or if disallowed by the ldP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the attestation certificate. When indicated by the ldP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the provided by the ldP. The RP must store the attestation certificate. When indicated by the ldP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the provided by the ldP. The RP must store the attestation certificate. When indicated by the ldP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation certificate. When indicated by the ldP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation certificate. When indicated by the ldP the RP SHALL attest generated credentials from the bound authenticator and verificate. When indicated by the ldP the RP SHALL attest generated received and verificate. When indicated by the ldP the RP SHALL attest generated received and verificate. When indicated by the ldP the attestation certificate. When indicated by the ldP the RP SHA | | | | requirements (±5.0.±), and bound authenticator informative examples (±0.7). | |
| [2] https://chromeenterprise.google/policies/#SecurityKeyPermitAttestation attestation certificate. When indicated by the IdP the RP SHALL attest generated credentials from the bound authenticator and verify the attestation object using the attestation certificate provided by the IdP. The RP must store the attestation and verify the attestation object using the attestation certificate provided by the IdP. The RP must store the attestation and verify the attestation object using the attestation certificate provided by the IdP. The RP must store the attestation certificate or attestation certificate or attestation certificate and verify the attestation certificate or advertify the attestation certificate. When indicated by the IdP The RP must store the attestation certificate. When indicated by the IdP The RP must store the attestation certificate. When indicated by the IdP The RP must store the attestation certificate. When indicated by the IdP The RP must store the attestation certificate. When indicated by the IdP The RP must store the attestation certificate. When indicated by the IdP The RP must store the attestation certificate. When indicated by the IdP The RP must store the attestation certificate. When indicated by the IdP The RP must store the attestation certificate. When indicated by the IdP The RP must store the attestation certificate. When indicated by the IdP The RP must store the attestation c | | | | [4] between 1/1 constant and the second second second second | |
| [3] https://learn.microsoft.com/en-us/entra/identity/authentication/concept-fido2-hardware-vendor [4] https://developers.yubico.com/WebAuthn/Concepts-fido2-hardware-vendor [4] https://developers.yubico.com/WebAuthn/Concepts-finetprise_Attestation/ certificate or attestation certificate thumbprint in addition to the bound authenticator credential public key such that the RP bound authenticator may be identified using IdP provided data in future FAL3 authentication flows. Request protocol specific normative guidance for identifiers used in IdP indication of bound | | | | | |
| [4] https://developers.yubico.com/WebAuthn/Concepts/Enterprise_Attestation/ certificate or attestation certificate thumbprint in addition to the bound authenticator credential public key such that the RP bound authenticator may be identified using IdP provided data in future FAL3 authentication flows. Request protocol specific normative guidance for identifiers used in IdP indication of bound authenticator may be identified using IdP provided data in future FAL3 authentication flows. | | | | | |
| 36 63C 3.15.1 39 1619 [5] https://datatracker.ietf.org/doc/html/rfc7800 bound authenticator may be identified using IdP provided data in future FAL3 authentication flows. Request protocol specific normative guidance for identifiers used in IdP indication of bound | | | | | |
| Request protocol specific normative guidance for identifiers used in IdP indication of bound | | | | | |
| | 36 | 63C 3.15.1 39 | 1619 | | bound authenticator may be identified using IdP provided data in future FAL3 authentication flows. |
| 37 63C 3.15.2 40 1646 authenticator use. | | | | | |
| | 37 | 63C 3.15.2 40 | 1646 | authenticator use. | |

| | | | | Propose additional RP required behavior for bound authenticator use in FAL3 authentication based on | |
|--------|---|-----|-------|--|---|
| | | | | IdP assertion contents which restrict what bound authenticators may be used by a subscriber to | |
| | | | | authenticate to the RP. This feedback is paired with IdP constrained bound authenticator issuance | |
| | | | | feedback for section 13.5.1. When supported by the bound authenticator (enterprise attestation | |
| | | | | enabled) and RP (present in the IdP and authenticator enterprise attestation allowlist) these additional | |
| | | | | requirements enable an IdP to require authentication using the same bound authenticator at the IdP | 5. The trust agreement may require an IdP to include a bound authenticator attestation certificate or certificate thumbprint in |
| | | | | and RP. | the assertion presented to the RP. When required by the trust agreement the RP MUST limit the acceptable bound |
| | | | | | authenticators for the subscriber account using the provided attestation certificate or certificate thumbprint by comparing |
| | | | | If these proposed additions are accepted, we suggest the means of communicating attestation | the IdP supplied value with attestation certificates or certificate thumbprints stored by the RP during subscriber bound |
| | | | | certificates between the IdP and RP follow normative or informative guidance requested as a part of | authenticator issuance. The RP SHALL reject authentication attempts using subscriber bound authenticators which do not |
| | | | | bound authenticator issuance feedback in section 13.5.1. Additional normative or informative guidance | match the IdP supplied attestation certificate or certificate thumbprint value. The RP MAY initiate bound authenticator |
| | | | | for implementers is requested for the means by which IdPs may disallow subscriber registered bound | issuance using the IdP provided enterprise attestation data after rejecting authentication with an unknown bound |
| 38 63C | 3.16.1 | 42 | 1000 | authenticator use. | authenticator. |
| 39 63C | 3.10.1 | 46 | | "a priori" should always be two words | authenticator. |
| 39 b3C | 4.5.1 | 46 | 1//9 | "All assertion SHALL contain sufficient [IAL, AAL, and intended FAL]" and "At FAL3, the assertion SHALL | |
| | | | | | |
| | | | | include or An indicator that verification of a bound authenticator is required to process this | |
| | | | | assertion." | |
| | | | | | |
| | | | | Greater clarification is required as to the intent as this is challenging unless there's an explicit proposal | |
| | | | | for both OIDC and SAML in terms of how to do this. Consider allowing "the terms of the trust | |
| | | | | agreement" to declare this as per Sec. 2.5, especially for lower FAL levels, since this requirement would | |
| | | | | render any existing implementation that fails to explicitly indicate non-assertion of IAL, AAL, or intended | All assertions contain sufficient unless the trust agreement specifies an obligation for the RP and IDP to always meet the |
| 40 63C | 4.9 (assertion contents) | 62 | 2348 | FAL noncompliant for even FAL1. | required xAL for specified subscribers or for otherwise clearly identifiable assertion workflows. |
| | | | | "A cryptographic nonce". | |
| | | | | | |
| | | | | Clarification is required as to whether the SAML request "ID" can satisfy this requirement if | |
| 41 63C | 4.10 (authn requests) | 65 | 2400 | implemented to carry sufficient randomness (e.g. as in Sec. 3.12.1). | |
| | (| | | (-8 | |
| | | | | "an IdP that uses HTTP redirects for front channel presentation of assertions that contain PII SHALL | |
| | | | | encrypt the assertion as discussed in Sec 3.12.3." | |
| | | | | encrypt the assertion as discussed in Sec 3.12.3. | |
| | | | | Greater clarification is required around the intent as this seems excessive for FAL1 since front-channel | |
| 42 63C | 4.11 (front-channel) | 68 | 2401 | SAML is very common in industry. See also comment about federated identifiers in Sec 3.3 | For SAML at FAL1, RPs and IDPs are deemed to meet this requirement if they only expose HTTPS-protected endpoints. |
| 42 03C | 4.11 (Hone-channer) | 00 | 2451 | Under "The following terms SHALL be disclosed to the subscriber during the runtime decision:" is does | For Salvic at FALL, KPS and IDPS are deemed to meet this requirement if they only expose HTTPS-protected enupoints. |
| | | | | | |
| | | | | not say that additional information implicitly shared (like the credential issuer or any reused salted-hash | |
| | | | | values) should be disclosed to the user. Several of us are worried that users may be deceived by the | |
| | | | | consent screens for salted-hash selective disclosure schemes into believing that the interaction is more | |
| | | | | private than it really is (especially in the context of proof-of-adulthood). Perhaps this is covered | |
| | | | | elsewhere in the document, but it seems like a potential omission here to mention disclosure of the | |
| | | | | subscriber attributes but not the implicit attributes. | |
| | | | | | |
| | | | | Also note that there are multiple sections named "trust agreements" (eg, 3.4 and 4.3) which could | |
| 43 63C | 5.3 Trust agreements | 71 | 2557 | cause problems for a #trust-agreements anchor. | |
| 44 63C | 5.5 | 73 | 2604 | typo: "attribute bundle >>>singing<<< public key" | |
| | | | | Request informative examples of trust agreements for FAL1, FAL2, and FAL3 including xAL | |
| 45 63C | 10 | 96 | 3258 | requirements. | |
| 46 63C | 10 | | | Request informative examples of RP specified xAL requirements for OIDC and SAML. | |
| | 10 | | 2230 | Expand informative examples of bound authenticator use to include IdP specified bound authenticator | |
| 47 63C | 10.7 | 101 | 3423 | use via enterprise attestation. | |
| 050 | 10.7 | 101 | 5-125 | "the RP can use [the token binding headers] to associate the contents of the assertion with the | |
| | | | | subscriber's bound authenticator." | |
| | | | | Subscriber's bound authenticator. | |
| | | | | Control of the contro | |
| | | | | Greater clarification is required as to whether is this considered a "bound authenticator". It could be | |
| | | | | read that this term was only used in this revision for RP-managed things and that's why "or HoK" is used | " |
| | | | | pervasively (e.g. Sec. 3.16). Perhaps this should say " with the subscriber's authenticator" (omitting | <u>'</u> |
| 48 63C | 10.8 (fal3 with referred token binding) | 102 | 3448 | "bound")? | |
| | | | | | |