Comment Template for: NIST SP 800-63-4 Suite (Initial Public Draft)						
NIST SP 800-63-4 ipd (initial public draft), Digital Identity Guidelines						
Organization: Microsoft						
Name of Submitter/POC: Juliana Cafik						
[REMOVED]						
NIST Guidance	**Publication (Base, 63A, 63B, 63C)**	**Section**	**Page #**	**Line #**	**Comment (Include rationale for comment)**	**Suggested Change**
Control of a digital account: An individual is able to demonstrate control of a digital account (e.g., online bank account) or signed digital assertion (e.g.,verifiable credentials) through the use of authentication or federation protocols.This may be done in person through presentation of the credential to a device or reader, but is more likely to be done during remote identity proofing sessions.	63A	4.4.1	15	684	Can VC's be used as a way to (or sustain) re-use of a previously proofed identity. This would support the notion that an IDP can store a VC at a specific LOA in the user account for a federation scheme - but can it be re-used across multiple IDP's? Current guidance details how a VC can be used as part of the verification step for the Identity proofing to link between claimed identity and real-life existance of the subject, however, it doesn't provide guidance on the possible reuse of a VC issued at a specific AAL as a way to establish AAL at a new IdP without having the user present additional evidence. While there is guidance for converying xAL between parties that allows reusing existing IAL from another source, it is limiting since it requires the RP to maintain the federation dependency for every transaction vs simply just for an initial transaction that would be used to establish the user's IAL.	Recommend additional guidance to include a VC as a form of digital evidence that can be used in the ID proofing process
Collection of Additional Attributes: Validated evidence is the preferred source of identity attributes. If the presented identity evidence does not provide all the attributes the CSP considers core attributes, it MAY collect attributes that are self-asserted by the applicant	63A	5.3.2.2	26	1057	While it is possible to capture IAL's using a federation trust agreement, there is a need for more dynamic method allowing to convey IALs, specifically for identity attributes collected at different IALs as things evolve.	Recommend provding guidance on a consistent way to communicate an attribute in a way that the respective IAL can be captured per attribute
Authenticator and Verifier Requirements	63B	Section 5	14	657	It would be beneficial to have guidance for allowed MFA method for local authentication (sign-in/logon to machine). There are multiple regulations (IRS 1075, PCI-DSS) requiring the use of an authenticator that is separate from the access device. This leads to many question around the suitability of the platform authenticator as part of MFA to the local device.	There is clarity for accepting platform authenitcator for network/remote authentication, recommend adding guidance for local authentication as well.
Authentication using the Public Switched Telephone Network Use of the PSTN for out-of-band verification is restricted as described in this section and in Sec. 5.2.10. If out-of-band verification is to be made using the PSTN, the verifier SHALL verify that the pre-registered telephone number being used is associated with a specific physical device. Changing the pre-registered telephone number is considered to be the binding of a new authenticator and SHALL only occur as described in Sec. 6.1.2	63B	5.1.3.3	23	917	Is GSMA Rich Communication Services (RCS) considered a PSTN-based authenticator? RCS has significant improvements over the previous generation (SMS).	Guidance explicitly mentions GSMA RCS and how it compares to traditional SMS-based methods. Recommend clarification on whether additional OTA channels (such as WhatsApp) qualify. Since they don't have as strong a relationship as SMS and RCS to the subscriber's identity they might not, but would be useful to spell this out.
Use of Biometrics: Biometric comparison can be performed locally on the claimant's device or at a central verifier.	63B	5.2.3	33	1306	Current guidance for use of biometric as part of a multi-factor authentication clearly covers how biometric can be used as part of a multi-factor authenticator where the biometrics is localy checked by the authenticator. However, while NIST guidance seems to allow for the use of a biometric as part of a multi-factor authentication where the biometrics is checked in a central location, it is unclear how this is possible since also states that biometrics are not an acceptable authenticator (and there is no authenticator class capturing such authenticators). This is leading to various biometrics authentication solution providers arguing their solution is meeting NIST guidance.	Recommend clarification on whether a biometric can be part of multi-factor authentication and not be part of a multi-factor authenticator.
Connected Authenticators: Cryptographic authenticators require a direct connection between the authenticator and the endpoint being authenticated.	63B	5.2.12	39	1508	"direct connection" is not defined. The FIDO CTAP 2.2 hybrid transport protocol uses a mix of protocols to support Cross-Device Authentication in a phishing-resistant manner, without what has been traditionally defined as a direct connection (physical cable, Bluetooth pairing, and/or Wi-Fi direct assocation).	Recommend clarification of the meaning of "direct connection" and whether equivalent solutions like CTAP 2.2 hybrid transport could be considered "direct" (or potentially add a statement about "direct equivalence")
Connected Authenticators: Wireless technologies having an effective range of 1 meter or more (e.g., Bluetooth LE) SHALL use an authenticated encrypted connection between the authenticator and endpoint.	63B	5.2.12	39	1523	"use an authenticated encrypted connection". The FIDO CTAP 2.2 hybrid transport protocol uses an encrypted BLE advertisement to provide data from the client to the authenticator to then allow both parties to establish a secure websocket connection	Recommend clarification for the meaning of "connection" in this context so that solutions like CTAP 2.2 with hybrid transport qualify
Connected Authenticators : A pairing process SHALL be used to establish a key for encrypted communication between the authenticator and endpoint.	63B	5.2.12	39	1524	"a pairing process". The FIDO CTAP 2.2 hybrid transport protocol uses an encrypted BLE advertisement. There is no Bluetooth layer pairing / relationship, by design.	Recommend consideration for use cases where a traditional bluetooth "pairing" relationship is not used (such as hybrid which essentially uses an application level relationship)

Binding of an Additional Authenticator at Exisitng AAL: With the exception of memorized secrets, CSPs and verifiers SHOULD encourage subscribers to maintain at least two valid authenticators of each factor that they will be using	63B	6.1.2.1	43	1627	"at least two valid authenticators of each factor that they will be using". With a passkeys, the same credential could exist in two authenticators. Would a single passkey in multiple authenticators meet this requirement?	Recommend clarity for credential vs authenticator in this context
Single-factor cryptographic device authenticators use tamper-resistant hardware to encapsulate one or more secret keys unique to the authenticator that SHALL NOT be exportable (i.e., cannot be removed from the device). The authenticator operates using a secret key to sign a challenge nonce presented through a direct interface between the authenticator and endpoint (e.g., a USB port or secured wireless connection) as specified in Sec. 5.2.12. Alternatively, the authenticator could be a suitably secure processor integrated with the user endpoint itself	63B	5.1.7.1	28	1098	Does HTTP loopback constitute direct connection between the authenticator and the endpoint being authenticated? Assuming the authenticator secrets are stored in TPM/TEE?	Request clarification
Activation Secrets	63B	5.2.11	38-39	1480 - 1507	Authenticators making use of activation secrets SHALL require the secrets to be a least 6 characters in length. The authenticator SHALL contain a blocklist (either specified by specific values or by an algorithm) of at least 10 commonly used activation values and SHALL prevent their use as activation secrets. If the authenticator verifies the activation secret locally verification SHALL be performed within a hardware-based authenticator or in a secure element (e.g., TEE, TPM) that releases the authentication secret only upon presentation of the correct activation secret. In other circumstances (i.e., software-based multi-factor authenticators), the authenticator SHALL use the memorized secret as a key to decrypt its stored authentication secret.	Request for confirmation of intent to force both activation factor and phone unlock for every authentication?