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

Please submit responses to dig-comments@nist.gov by March 24 April 14, 2023

Organization:	*ADUCID*
Name of Submitter/POC:	*Libor Neumann*
Email Address of Submitter/POC:	[REMOVED]

	Publication				**Comment**	
Comment #	**(Base, 63A, 63B, 63C)**	**Section**	**Page #**	**Line #**	**(Include rationale for comment)**	**Suggested Change**
1					Compatibility between Digital Identity Guidelines (Update) and Zero Trust Architecture NIST SP 800-63-3 last update 2017 NIST SP 800-207 published 2020 Common topics – identity + authentication. No compatibility seen. Open questions: • What is the relationship between CSP, RP, Verifier and IdP on the one hand and Policy Decision Point, Policy Engine, Policy Administrator and Policy Enforcement Point on the other? • ZTA is identity based, Digital Identity Guidelines is account/authenticator based. • ZTA requires centralized management of users and their access rights, Digital Identity Guidelines allows RP to be a different organization than CSP, Verifier or IdP. • Digital Identity Guidelines allow SSO, ZTA prohibits repeated use of authentication "However, authentication and authorization to one resource will not automatically grant access to a different resource." • The application of ZTA principles in the architecture used by the Digital Identity Guidelines is also a challenge. E.g.	Solve compatibility with ZTA in full range.
2	63B				No requirement for long-term sustainability Unsolved problems that will manifest themselves during long-term use • Refreshment of crypto material. There is no limitation of the time of use of cryptomaterial/cryptographic keys, procedures for updating cryptomaterial/keys without the need for physical exchange of authenticators. Described organizationally without technological support 6.Authenticator Lifecycle Management, 6.1.4. Renewal, 6.3. Expiration • Cryptographic agility. There is no solution for changing cryptography during operation (without the need for physical exchange of authenticators and repeated proofing). This is important for both planned and unplanned events when cryptographic algorithm and/or authentication protocol change is necessary. • Technological support of the complete life cycle of authenticators. There is a lack of technological support for replacing	Solve unsolved issues of long-term sustainability.
3	63B				The randomness of generated keys, authentication challenges and other authentication elements significantly affects the security of authentication. I have not found a way to control and verify the quality of the randomness. Seems it it only open to classic physical random generators (true random). Not open to alternatives, possibly more modern methods , e.g. distributed entropy enrichment - use of external randomness generators or external seed	Include random number generation quality control.
4	63B				Positives: Proper separation from authentication passwords. Issues: Outdated technical solution of the second factor in many places of the text (biometrics p. 33-34, SW authenticators + verifiers – p. 29-30). These requirements explicitly chain authentication factors facilitating brute force attack on encrypted keys. The requirement specifications block the use of more secure modern methods. Chaining factors is also in contradiction to Zero Trust Architecture principles. Especially with SW authenticators. I suggest to make an improvement by separation of real-world factors from authentication strength. So far only partial. E.g. 4.2.1. PermittedAuthenticatorTypes Separate verification of authenticator usage by an authorized person from online authentication strength. This can achieved by eliminating factor chaining, or at least allow full two-factor authentication (with data channel binding) instead of relying on the authenticator's local security. This would be consistent with ZTA principles: authenticate everything (according to ZTA). The server side can be secured significantly better than the client side. The user (and their equipment) is the weakest point of cyber security. Authentication keys are not a protected asset. RP owns a protected asset/resource. The keys/cryptomaterial are intended to distinguish the user from the attacker. In a MITM attack (see data channel binding), authentication on the network is only one-factor. The attacker does not have to deal with the second factor.	Separate verification of authenticator usage by an authorized person from authentication strength. Eliminate factor chaining, or at least allow full two-factor authentication - don't rely on the authenticator's local security. Authenticate everything (according to ZTA). Enable full two-factor authentication including key misuse protection with modern methods following ZTA principles
5	63B				Data channel binding methods Positive: The requirement reacts to an important existing weakness. Suggestions for improvement: Another example solution: – signature of the exported key material - RFC 5705 - Keying Material Exporters for Transport Layer Security (TLS) - signature of the server certificate used by the TLS client (verification of ownership of the private key is part of the TLS negotiation). Data channel binding can also be used for assertion protection as an alternative to Bound Authenticator (FAL3). This can	Enable use of other data channel binding solutions/add examples. Enable use of 2 channel bindings.

6	63B				Limits the use of modern methods of protection against misuse of copied keys and detection of attackers Time and computing power cannot be used as a security measure, e.g. dynamic detection of the use of a copied key. At the same time, sufficient computing power is available in the hands of users (smart phones, tablets,...) and there are significant barriers to the use of specialized HW •User acceptance •Lack of user care. •Limit of processing power, controls, power supply. •The impossibility of fixing with security patches in HW.	Enable the use of modern methods of protection against the misuse of copied keys and the detection of attackers instead of relying on the impossibility of copying or revealing keys.
7	63B				Slide 41 - Security compromises of FIDO passkeys. In addition to the risks of copy protection attacks (unknown security), there is a consequence of long-term use of the same private key (potentially repeated copying of a very old key (e.g. several decades) to future device, e.g. future smart phone). Possible new attack vector - misuse of keys in decommissioned devices (“second hand shop attack”). Security of key transfer is unknown, cannot be verified - not standardized/described.	
8	63B				Slide 41 - Security of Verifiable Credentials. Be very careful. Do high quality security analysis, especially identification (e.g. reliable globally unique identifier generation) and authentication security.	
9	63B				Slide 41 - Phishing resistance - correct and progressive solution - see comment# 5	
10	63B				Slide 41 - Security vulnerabilities of common session management methods - there is no solution to the issue of the lifetime of cookies used by IdP. What is the point of reauthenticating a session when cookies are used instead of user	
11	63C				Slide 52 - Bound Authenticators - has a security benefit only in some implementations. When using e.g. push notification, Bound authentication is unnecessary. It is not bound to the assertion transfer. Does not prevent MITM attack. It could be	