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

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

Organization:	*Siemens AG*
Name of Submitter/POC:	*Jan Herrmann*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63A	in general			Define IAL for non-human-user and device identities: 800-63-3 is until now strongly/solely human user focused. In our IoT, OT but also in IT (e.g. Zero Trust architectures) environments we see many non-human-user and device use cases that require standardization of assurance levels like identity assurance levels for these non-human-user and device identities. In internal governance rules we work on related topics (see column G to get an impression) but we see the strong need for international standardization to allow for harmonized and interoperable definitions.	Define IAL for non-human-user and device identities. Sketch of an initial definition proposal: Every service-user (aka. non-human-user) and device identity respectively shall be created according to the targeted service Identity Assurance Level (sIAL) and device Identity Assurance Level (dIAL). The sIAL or dIAL status of service-user and device identities shall be determinable externally by authorized parties (e.g., via sIAL and dIAL claims in access tokens, via certificate attributes or via an IdP API endpoint). The service Identity Assurance Level (sIAL) as well as the device Identity Assurance Level (dIAL) attribute can have a value of 1, 2 or 3 that express the quality level of the attestation and identity creation process as well as the trustworthiness of service infrastructure and provider used for that attestation/creation process. 1. Details on Service Identity Assurance Level (sIAL) 1.1 The creation of a service user identity with an sIAL assignment of 3 is defined by the following requirements: - A central, trusted Service User IdP having highest security classification (i.e., adequate mitigation for high impact threats) shall be used. - In case of a human user-initiated service user creation process: The human user shall pass the AAL 3 compliant authentication for his IAL 3 human user identity and pass high security level relevant Zero Trust access policy checks (e.g., device compliance as well as human user account and device compromised risk state checks) - In case of a device birth certificate (e.g., an IDevID) based service user-initiated service user creation process: The requesting service user shall use its underlying device birth certificate (or thereof derived service identities), having themself an sIAL/dIAL attribute value of 3, to authenticate according to sAAL 3 or dAAL 3 requirements and then initiate the service user creation/registration process. 1.2 The creation of a service user identity with an sIAL assignment of 2 is defined by the following requirements: - A central, trusted Service User IdP having medium security classification (i.e., adequate mitigation for moderate impact threats) shall be used. - In case of a human user-initiated service user creation process: The human user shall pass at least the AAL 2 compliant [illegible]
2	63B	in general			(three related aspects in this single comment) 1. Include Zero Trust principles 2. add support for step-up authentication in the human user case 3. Define AAL for non-human-user and device identities: 800-63-3 is until now strongly/solely human user focused. In our IoT, OT but also in IT (e.g. Zero Trust architectures) environments we see many non-human-user and device use cases that require standardization of assurance levels like authenticator assurance levels for these non-human-user and device identities. In internal governance rules we work on related topics (see column G to get an impression) but we see the strong need for international standardization to allow for harmonized and interoperable definitions.	additional device authentication to later support device security state related access controls (cf. ZT memorandum M-22-09 or the DoD Zero Trust Reference architecture pillars - cf. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf page 22. Therefore AAL shall in general address the combined user and device authentication requirement. Sketch of an initial definition proposal: 1. For nun-human users + underlying device authentication: Service users (aka non-human users) shall only be able to access functionalities of an asset after passing a combined service user and underlying device authentication. service-user Authenticator Assurance Level (sAAL)=1 and device Authenticator Assurance Level (dAAL)=1: the service user as well as the device authentication shall be using asymmetric cryptography based authentication protocols or symmetric authenticators. Successful authentication requires that the service user and device proves possession and control of the authenticator(s) through a secure authentication protocol. The device shall be authenticated using asymmetric keys. Authentication methods and authenticators shall be selected per user and device group out of the wide range available following a risk-based approach. The selection process of authentication method(s) and authenticator(s) shall be documented, including the conducted authentication methods and authenticators) risk assessment. The authentication factor(s) used, next to their storage type, shall be known or determinable during the authentication process on authentication service side and that information shall be mappable to issued security tokens (e.g., as claim(s) in issued access tokens) or retrievable from outside via other means (e.g., via an authentication service API endpoint serving a user's session context information). sAAL=2 and dAAL=2: same as sAAL and dAAL 1 but: a) asymmetric cryptography based authentication protocols only. b) Secret authentication information that must be stored on user/client side shall be securely persisted using hardware based trust anchors like a hardware trusted platform module (TPM), a secure element or a hardware security module (HSM) - Exemptions: e1: In case of centrally managed, non-backend user devices the secret authentication information of the corresponding users and of these devices themself may alternatively be protected via software based trust anchors
3	63B	in general			put standardized amr claims in relation to AALs. Consider adding new amr value definitions.	e.g. AAL 3 requires an amr like hwk - cf. https://www.ietf.org/rfc/rfc8176.html
4	63-Base			657-658	Line 607-608 state: "The SP 800-63 guidelines use digital identity models that reflect technologies and architectures currently available in the market." If the document wants to target Verifiable Credentials as well then the Figures 1. and Figure 2. might not be fully complete to reflect the Verifiable Credential technology as well. Isn't there a component of Verifiable Data Registry missing which is used by the verifier to authenticate the verifiable credentials because it holds the public information (such as public keys of the issuer, schemas...).	The picture should look like this to also reflect the Verifiable Credentials.