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:	*American Association of Motor Vehicle Administrators*
Name of Submitter/POC:	*Loffie Jordaan*
Email Address of Submitter/POC:	[REMOVED]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
	63-Base	2. Introduction	3	386	It is explained that the identity proofing process establishes that a subject is a specific physical person. It is our understanding that this process also involves the issuance of an authenticator to a subject. To help readers in this early stage to make the logical connection between this step and the next step (digital authentication of an authenticator), it would be helpful to clarify this.	Explain that the first process (i.e. identity proofing) also includes the issuance of an authenticator (or authenticators) to the subject.
	63-Base	2. Introduction	4	390	Reference is made to the subject that "previously accessed the service". It is not clear what "the service" refers to.	Please clarify what "the service" refers to.
	63-Base		11	630	In the case of mDL (and similar solutions), the Relying Party could be the entity that verifies the claimant's identity. (This will be the case for the 1st edition of ISO/IEC 18013-7 is expected, which is anticipated to specify an over-the-Internet protocol for the exchange of an mdoc and MSO, yet still with the Relying Party being responsible for matching the claimant to the subject described by the authenticated mdoc.) It will be helpful to devise definitions that also accommodate this. Alternatively, if this use case (i.e. where the Relying Party is responsible for matching the claimant to the authenticated mdoc) is considered out of scope (e.g. because from a Relying Party's perspective the function of the mDL device is primarily to confirm that the mDL has not been cloned, rather than helping to verify the claimant), it will be helpful to explicitly state this.	Clarify if the case where a Relying Party matches the claimant to an authenticated mdoc (or similar document) it in scope or not.
	63-Base		11	630	The word "performs" implies direct involvement of the IdP at transaction time. In case of the mDL model (ISO/IEC 18013-7 edition to follow the 1st edition), to support the subject's privacy the solution intentionally will not require IdP involvement at transaction time. It would be helpful for the definition of IdP to more clearly include this case.	Enhance the definition of an IdP such that it does not imply involvement of the IdP at transaction time. For example: "An entity in a federated model that is responsible for both the CSP and Verifier functions. The IdP is responsible for establishing mechanisms to authenticate the subscriber and convey assertions to RPs."
	63-Base			690	As per the definitions on page 11, the IdP is responsible for authenticating the subscriber. Line 690 could be read to say that this is a responsibility of the Verifier.	Clarify the language to resolve the possible inconsistency.
	63-Base			719	While we believe we follow the intent of the requirement for a subscriber to maintain control of an authenticator, it should be noted that a mobile device can be used by different individuals, each with their own mDL on the device. In addition, there may be privacy concerns around requiring a subject to inform a CSP if a mobile device (i.e. authenticator) provided by the subject is not in their control anymore.	Enhance the document to recognize that a mobile device can be used by different individuals, each with their own mDL on the device. Also clarify the CSP's responsibility in respect of enforcing this requirement, especially in case the subject provided the mobile device (i.e. authenticator).
	63-Base			748	Is a claimant referred to as a subscriber once authenticated, or once id-proofed?	Clarify language if needed.
	63-Base			798	It is not clear what the logical difference is between (1) combining a biometric and another authentication factor into a multi-factor authenticator (which is allowed), and (2) considering a biometric and another authentication factor as separate and independent authenticators (which is not allowed). The input and output of both cases appear to be the same.	Clarify what the logical difference is.
	63-Base			889	In the case of device retrieval mDL, the assertions and subscriber attributes are not conveyed "across networked systems". This information is exchanged only between the subscriber and the Relying Party.	Update the federation model to allow for transactions where subscriber attributes are not conveyed across networked systems, but only between the subscriber and the Relying Party.
	63A			420	In Section 4.1, reference is made to "identity proofing and enrolment". This raises the question if "entire identity proofing session" includes enrolment or not. For example, if proofing happens in person but a mDL is subsequently issued remotely, could this qualify for IAL3?	Clarify whether the "entire identity proofing session" includes enrolment or not.
				425	DMVs already face requirements for the issuance of credentials via the REAL ID act and Rules (which are expected to shortly also address mDL issuance). The requirements in Section 4, and the broader requirements in 800-63, address similar issues albeit with different requirements. DMVs are concerned that there may be a vision by NIST to design 800-63 such that it could be possible for e.g. DHS to prescribe 800-63 to DMVs for issuing credentials, including mDLs. Given the difference in requirements, such a situation would place a significant additional burden on DMVs.	It is suggested that 800-63 clarify whether it is designed to be applied (e.g. by DHS) to the issuance of credentials (including mDL) by DMVs, or if the focus/intent excludes the potential application of 800-63 to the issuance of credentials by DMVs.
		4.3.3		542	It is not clear what evidence strength would be assigned to DMV-issued credentials.	Explicitly state the evidence strength assigned to REAL ID and non-REAL ID DMV-issued credentials, for both physical cards and mDLs.
			6	433	As phrased, the statement that identity proofing processes are designed to protect against attacks against CSPs that service a large number of subscribers implies that the proofing processes are not designed to protect against attacks of CSPs that service a small number of subscribers. It should also be noted that the value of data may not always depend only on the number of subscribers; it may also be determined by who the subscribers are.	If the resulting statement remains true, strike "…that affect a large number of enrolled subscribers…".
			10	520	It is not clear if a stock control number would qualify as a "reference number".	Please clarify if a stock control number would qualify as a reference number.
			10	536	It is not clear if the level of identity proofing performed by the issuer of the digital evidence is relevant.	Please clarify if the level of identity proofing performed by the issuer of the digital evidence is relevant.
			10	522	It is not clear if the level of identity proofing performed by the issuer of the document is relevant.	Please clarify if the level of identity proofing performed by the issuer of the document is relevant.
			11	553	Although not common, it should be noted that evidence in some cases has to be delivered to persons other than those to whom it relates, e.g. to parents or caregivers.	Consider amending the description to also cover cases where evidence may have to be delivered to persons other than those to whom the evidence relates.

			11	553	Does delivery by USPS regular mail comply with this requirement?	Consider providing examples of delivery methods that could "reasonably be assumed" to result in correct delivery.
			11	570	Does delivery by USPS regular mail comply with this requirement?	Consider providing examples of delivery methods that could with "high likelihood" result in correct delivery.
				586	It is not clear what is included under "visually identified". Does a selfie compared by a biometric algorithm qualify? A selfie compared to a reference image by a human? A human matching a live video feed against a reference image? An image taken by a kiosk under control of the issuing source that is biometrically matched to a reference image?	Please clarify what is included under "visually identified".
				588	Does delivery by USPS regular mail comply with this requirement?	Consider providing examples of delivery methods that could "ensure" result in correct delivery.
				595	The requirement for superior evidence to include physical security features appears to rule out digital credentials (which per definition do not have a physical component). It will be helpful to clarify if that is indeed the intent.	Clarify if the intent is to disqualify fully digital credentials from serving as superior evidence.
				606	"Confirming" could mean different things to different CSPs. For example, is visual inspection of security features sufficient, or do 2nd level security features have to be checked? Are CSPs required to obtain a list of security features from the original issuers of all documents to be "confirmed"?	Please provide additional guidance on the extent of "confirmation" required.
				631	4.3.4.1, Evidence Validation, is mandatory. 4.3.4.4 implies that additional validation (presumably what is described in 4.3.4.4) may be required. However, 4.3.4.1 does not appear to allow evidence that does not pass the requirements in 4.3.4.1.	Please clarify if evidence that do not pass all the requirements of 4.3.4.1 could still be accepted if it passes the (additional) requirements in 4.3.4.4.
				664	The text indicates that the "CSP operator" has to perform an in-person physical comparison. It is not clear of the comparison has to be performed by a person, or if the CSP operator can perform the comparison using technology (e.g. a supervised kiosk on the CSP operator's premises).	Clarify the extent to which a person must, should or does not have to be involved in the comparison performed by the CSP operator.
				695	DMVs already face requirements for the issuance of credentials via the REAL ID act and Rules (which are expected to shortly also address mDL issuance). The requirements in Section 5, and the broader requirements in 800-63, address similar issues albeit with different requirements. DMVs are concerned that there may be a vision by NIST to design 800-63 such that it could be possible for e.g. DHS to prescribe 800-63 to DMVs for issuing credentials, including mDLs. Given the difference in requirements, such a situation would place a significant additional burden on DMVs.	It is suggested that 800-63 clarify whether it is designed to be applied (e.g. by DHS) to the issuance of credentials (including mDL) by DMVs, or if the focus/intent excludes the potential application of 800-63 to the issuance of credentials by DMVs.
				466	The sentence before Figure 1 indicates that the diagram covers both identity proofing and enrollment. However, the title of the diagram only refers to identity proofing. In addition, the diagram itself does not appear to cover the enrollment step.	Clarify if Figure 1 includes enroment, and if so, indicate which step(s) in the process comprise enrollment.
				866	An enrollment code can be used to re-establish an applicant's binding to an enrollment record. If enrollment is considered part of verification (see separate comment on Figure 1 and how enroment applies), is it correct that usage of an enrollment code in this manner is limited to IAL1 (as per line 1086)? If enrollment is something that follows verification, it is not clear how and at what IAL levels the code can be used. Of particular interest is the case where a subject has already gone through a proofing process in the past, the subject was enrolled in the CSP's system, but the CSP did not issue an authenticator and the CSP now wants to issue an authenticator to the subject.	Clarify the use of an enrollment code. Of particular interest is the case where a subject has already gone through a proofing process in the past, the subject was enrolled in the CSP's system, but the CSP did not issue an authenticator and the CSP now wants to issue an authenticator to the subject.
				869	It is not clear what "validated" means. For example, does the existence of a postal address as per the USPS qualify as "validated"? Does a phone number that rings when called qualify as a validated number? If not, what steps would validate an address and a phone number?	Please clarify how an address and a phone number can be "validated".
				889	As phrased it is not clear if the sending of proofing notifications is a requirement.	Clarify if the sending of proofing notifications is a requirement.
				1222	It is not clear that "integrated scanners and sensors" means. For example, does a camera or fingerprint reader on a device supplied by a subject comply with this requirement?	Clarify what "integrated scanners and sensors" mean.
	63B			360	The text explains the assurances that successful authentication provide for services in which return visits are applicable. What assurances do successful authentication provide for services in which return visits are not applicable (i.e. for one-time services)?	Clarify if successful authentication provide assurances for one-time services, and if so, what those assurances are.
				378	If the vision of the 800-63 series of documents is to potentially support the use of decentralized state-issued credentials (such as mDL) as authenticators, the requirement that federal participants in authentication protocols be authenticated to subscribers means that state issuers would have to keep track of all federal relying parties. This could put an undue burden on state issuers (e.g. to validate the relying party, which fulfil the verifier role in this case, to the appropriate FIPS140 level - see e.g. line 469).	If the vision of the 800-63 series of documents is to potentially support the use of decentralized state-issued credentials (such as mDL) as authenticators, consider exempting such authenticators from the authentication requirement.
				387	It is not clear which subscriber account is "the subscriber account".	Assuming our understanding is correct, it may be helpful to clarify that this is about the "...authenticator bound to the subscriber account of the claimant".
				537	If the vision of the 800-63 series of documents is to potentially support the use of decentralized state-issued credentials (such as mDL) as authenticators, it should be noted that the relying party takes on the role of a verifier, and that a determination on whether the biometric sensor (of the authenticator, i.e. the mobile device) meets requirements is made by the issuing state (i.e. the CSP).	If the vision of the 800-63 series of documents is to potentially support the use of decentralized state-issued credentials (such as mDL) as authenticators, consider enhancements to the text to explain the role of the CSP to determine if the biometric sensor meets the requirements.
				555	If the vision of the 800-63 series of documents is to potentially support the use of decentralized state-issued credentials (such as mDL) as authenticators, this requirement (security controls from 800-53) may overlap REAL ID requirements, and place an undue burden on issuing states.	If the vision of the 800-63 series of documents is to potentially support the use of decentralized state-issued credentials (such as mDL) as authenticators, consider allowing state issuers to comply with REAL ID requirements in lieu of this requirement (i.e. security controls from 800-53).
				1214	Where the secret is the same for the authenticator and for unlocking the device (e.g. a biometric), it is suggested that consideration be given to allowing a single presentation of the secret provided the device unlocking and authenticator use steps are sufficiently close together in time. It is not clear what additional benefit two separate operations, sufficiently close together in time, will bring. The upside of a single operation is an improved user experience.	Consider allowing a single presentation of the secret, provided the device unlocking and authenticator use steps are sufficiently close together in time.
				1218	It is not clear what "zeroized" means.	Consider defining "zeroized".

				1229	If the vision of the 800-63 series of documents is to potentially support the use of decentralized state-issued credentials (such as mDL) as authenticators, it should be noted that that there are privacy considerations around a state issuer "pushing" updates to a device (as opposed to a subject requesting an update). The fallback mechanism is to limit the validity period of the authenticator (i.e. mDL), which allows the subject to retain choice, and the issuer to take invalid authenticators (i.e. mDLs) out of circulation much faster than is the case with physical credentials. This approach would fit within the requirement stated on line 1229 if "immediately" can be interpreted to include the natural expiration of a relatively short-lived authenticator.	Clarify if "immediately" can be interpreted to include the natural expiration of a relatively short-lived authenticator.
				1764	If the vision of the 800-63 series of documents is to potentially support the use of decentralized state-issued credentials (such as mDL) as authenticators, it should be noted that that there are privacy considerations around a state issuer "pushing" updates to a device (as opposed to a subject requesting an update). The fallback mechanism is to limit the validity period of the authenticator (i.e. mDL), which allows the subject to retain choice, and the issuer to take invalid authenticators (i.e. mDLs) out of circulation much faster than is the case with physical credentials. This approach would fit within the requirement stated on line 1763 if "as promptly as practical" can be interpreted to include the natural expiration of a relatively short-lived authenticator.	Clarify if "as promptly as practical" can be interpreted to include the natural expiration of a relatively short-lived authenticator.
				1783	If the vision of the 800-63 series of documents is to potentially support the use of decentralized state-issued credentials (such as mDL) as authenticators, it should be noted that physical authenticators comprise a subject provided mobile device, and requiring destruction of the device is not viable.	If the vision of the 800-63 series of documents is to potentially support the use of decentralized state-issued credentials (such as mDL) as authenticators, consider relaxing the requirement requiring destruction of the device carrying a state-issued decentralized credentials (such as mDL).
	63C			353	If the vision of the 800-63 series of documents is to potentially support the acceptance of decentralized state-issued credentials (such as mDL) by the federal government for purposes other than identity proofing and enrollment, it should be noted that the IdP is not necessarily the entity that authenticates the subscriber. This function could be performed by the relying party, e.g. by comparing an authenticated portrait image of the subscriber to the claimant.	If the vision of the 800-63 series of documents is to potentially support the acceptance of decentralized state-issued credentials (such as mDL) by the federal government for purposes other than identity proofing and enrollment, consider amending the text to also allow a relying party to authenticate the subscriber.
				432	If the vision of the 800-63 series of documents is to potentially support the acceptance of decentralized state-issued credentials (such as mDL) by the federal government for purposes other than identity proofing and enrollment, it should be noted that the use of these credentials are at the sole discretion of the subject. The state issuer does not, and has no desire to, limit the subject regarding with whom the credential can be shared. Consequently, the state issuer is not in a position to target any information to a specific relying party.	If the vision of the 800-63 series of documents is to potentially support the acceptance of decentralized state-issued credentials (such as mDL) by the federal government for purposes other than identity proofing and enrollment, consider amending the text to allow targeting (and verification of such targeting by a relying party) to occur without involvement of the CSP.
				440	If the vision of the 800-63 series of documents is to potentially support the acceptance of decentralized state-issued credentials (such as mDL) by the federal government for purposes other than identity proofing and enrollment, the requirement on line 440 would require state issuers to conclude an agreement with each federal relying party. This would place an additional burden on issuing states.	If the vision of the 800-63 series of documents is to potentially support the acceptance of decentralized state-issued credentials (such as mDL) by the federal government for purposes other than identity proofing and enrollment, consider allowing federal relying parties to accept such credentials without an agreement with the state issuer.
				441	It is not clear if this requirement is limited to cases where a subscriber wants to log in to a relying party, or whether it also covers cases where a relying party wants to confirm identity without requiring the subscriber to log in.	Clarify if this requirement is limited to cases where a subscriber wants to log in to a relying party, or whether it also covers cases where a relying party wants to confirm identity without requiring the subscriber to log in.
				448	It is not clear why a bound authenticator will be presented to the relying party even though the IdP is responsible for authentication (line 353).	Clarify why a bound authenticator should be presented to the relying party even though the IdP is responsible for authentication (line 353).
				590	If the vision of the 800-63 series of documents is to potentially support the acceptance of decentralized state-issued credentials (such as mDL) by the federal government for purposes other than identity proofing and enrollment, it should be noted that the mDL solution includes a device retrieval option (including for over-the-Internet use). This option by design does not include any communication with the IdP at transaction time. Figure 1 does not appear to support this approach.	If the vision of the 800-63 series of documents is to potentially support the acceptance of decentralized state-issued credentials (such as mDL) by the federal government for purposes other than identity proofing and enrollment, consider enhancing Figure 1 to allow a device retrieval option where there is no communication between the IdP and the relying party at transaction time.
	63C			784	If the vision of the 800-63 series of documents is to potentially support the acceptance of decentralized state-issued credentials (such as mDL) by the federal government for purposes other than identity proofing and enrollment, it should be noted that the default method of public key distribution is either by the state issuer via their public website, or via the AAMVA Digital Trust Service public website. Requiring a separate secure protocol for the exchange of this material will impose an additional burden on state issuers.	If the vision of the 800-63 series of documents is to potentially support the acceptance of decentralized state-issued credentials (such as mDL) by the federal government for purposes other than identity proofing and enrollment, consider allowing federal relying parties to obtain state issuer public keys from the state's website, or from the AAMVA Digital Trust Service website.