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:	*Veza*
Name of Submitter/POC:	*Michael Towers*
Email Address of Submitter/POC:	[redacted]

Comment #	**Publication** (Base, 63A, 63B, 63C)	**Section**	**Page #**	**Line #**	**Comment** (Include rationale for comment)	**Suggested Change**
1	63-Base	2.1	10	630	Consider expanding the definition of "Relying party (RP)" to explicitly include systems that manage permissions and entitlements. This could help bridge the gap between authentication and authorization.	Suggested addition: RPs may also include systems that manage fine-grained permissions and entitlements based on the authenticated identity and associated attributes.
2	63-Base	2.3	12	687	While this section focuses on authentication, it might be beneficial to mention the importance of linking authentication to fine-grained authorization.	Suggested addition: It's crucial to note that robust authentication should be paired with equally robust and granular authorization mechanisms to ensure that authenticated users only access resources they are entitled to.
3	63-Base	2.4	15	791	Consider adding a point about the importance of maintaining visibility into permissions and entitlements across federated systems	Suggested addition: When implementing federation, organizations should maintain comprehensive visibility into permissions and entitlements across all connected systems to ensure consistent and secure access control.
4	63-Base	3.5.2	46	1715	Consider adding metrics related to authorization and entitlement management.	Proposed additions to Table 4: Entitlement Drift Rate: Percentage of entitlements that deviate from expected or policy-defined states over time. Permission Visibility Coverage: Percentage of systems and applications for which comprehensive permission data is available and monitored.
5	63-Base	3.7	50	1792	Emphasize the importance of integrating identity management with entitlement and permission management for a comprehensive security approach.	Proposed addition: Organizations should strive to integrate their identity management systems with robust entitlement and permission management solutions to provide a comprehensive view of 'who has access to what' across all systems and data.
6	63-Base	3.8	50	1817	This section could benefit from mentioning the potential use of AI/ML in analyzing permission patterns and detecting anomalies in access behavior.	Suggested addition: AI and ML can also be leveraged to analyze patterns in permissions and access behaviors, potentially identifying anomalies or risks that may not be apparent through traditional methods.
7	63C	3.6	23	1090	Emphasize the importance of fine-grained attribute disclosure controls.	Propose that the standard includes guidance on how federated attributes should map to specific permissions and entitlements in the RP systems.
8	63C	3.7	24	1107	Highlight the need for clear processes on how federated identities and their attributes should be used to provision and manage permissions in RP systems.	Suggest including guidance on maintaining consistency between federated identity attributes and local permissions.
9	63C	3.11	31	1368	Stress the importance of including authorization-related attributes in federated identity exchanges.	Propose that the standard should provide guidance on securely transmitting and interpreting entitlement-related attributes across federation boundaries.
10	63C	4.6	50	1927	Recommend including considerations for how attribute disclosure decisions impact downstream authorization and entitlement management.	Propose guidelines for RPs on how to securely map received attributes to internal permission structures.
11	63C	4.6.3	53	2050	Emphasize the need for provisioning models to account for complex, fine-grained permission structures.	Suggest including guidance on maintaining the principle of least privilege when provisioning accounts based on federated identities.
12	63C	4.6.4	56	2100	Highlight the importance of real-time or near-real-time synchronization of identity attributes that impact permissions and entitlements.	Propose including best practices for maintaining consistency between federated attributes and local authorization systems.
13	63C	5	69	2494	Recommend including guidance on how subscriber-controlled wallets should interact with authorization systems.	Propose considerations for securely deriving permissions from wallet-based credentials while maintaining user privacy.
14	63C	6	78	2742	Suggest including specific security considerations related to the intersection of federation and fine-grained authorization.	Propose guidelines for securing the entire chain from federated authentication to local permission enforcement.
15	63C	7	81	2773	Recommend including guidelines on balancing the need for detailed attribute sharing for authorization purposes with privacy requirements.	Suggest best practices for minimizing exposure of permission-related information in federated transactions.
16	63C	10	96	3258	Showcase best practices for maintaining security and privacy throughout the process.	Propose including an example that demonstrates how a federated identity transaction flows through to fine-grained permission management in an RP system