October 07, 2024

National Institute of Standards and Technology (NIST)

dig-comments@nist.gov

Re: Comments on Digital Identity Guidelines, NIST SP 800-63-4

The Cloud Service Providers - Advisory Board welcomes the opportunity to comment on the second draft of the fourth revision to the four-volume suite of Special Publication 800-63, Digital Identity Guidelines.

The Cloud Service Providers - Advisory Board (CSP-AB) represents the world's leading cloud companies and supports standards and policies that promote and enable secure cloud adoption in the public and private sectors. Our member companies are global leaders in the drive to provide safe, scalable, and accredited digital government services, with a focus on both the civil servants delivering those services and the end-users receiving them.

We have provided detailed comments below on the questions posed in the feedback request.

Q1. Risk Management and Identity Models

- *Is the "user controlled" wallet model sufficiently described to allow entities to understand its alignment to real-world implementations of wallet-based solutions such as mobile driver's licenses and verifiable credentials?*

A: In our view, yes the NIST guidelines provide a comprehensive description of the user-controlled wallet model, also known as the "three-party model," with the CSP as the issuer, the IdP as the holder, and the RP as the verifier. The guidelines detail the interactions between the user, the relying party (RP), and the credential service provider in a step-by-step manner.

- *Q: Is the updated risk management process sufficiently well-defined to support an effective, repeatable, real-world process for organizations seeking to implement digital identity system solutions to protect online services and systems?*

A: In our view, yes the updated risk management process follows a clear five step process: Define the service, conduct an impact assessment, select initial assurance levels, tailor and document based on detailed risk assessments, and continuously evaluate.

Q2. Identity Proofing and Enrollment

- *Is the updated structure of the requirements around defined types of proofing sufficiently clear? Are the types sufficiently described?*

A: The CSP-AB believes that the updated structure around identity proofing and its types is sufficiently clear, and the types are well described for Remote Unattended, Remote Attended, Onsite Unattended, and Onsite Attended.

The organization of these proofing types helps distinguish between scenarios where supervision, physical presence, or remote proofing tools are in use.

- *Q: Are there additional fraud program requirements that need to be introduced as a common baseline for CSPs and other organizations?*

A: The CSP-AB submits the following six additions for consideration:

1. Unified Fraud Reporting Standards: We recommend the introduction of standardized formats for fraud reporting to create uniform data for tracking fraud attempts. This would improve the ability to recognize trends across multiple providers and help regulators or oversight bodies intervene early.

2. Fraud Prevention Metrics and Benchmarks: We encourage NIST to establish common benchmarks for metrics such as time-to-detection, fraud success rate, and remediation time. CSPs would report these metrics, allowing for performance comparison across the industry.

3. Behavioral Analytics for Continuous Fraud Detection: We recommend requiring CSPs to use advanced fraud detection methods, such as behavioral analytics or AI-driven models, to track and analyze user behaviors over time. For example, anomalies in how a user types or navigates can trigger further scrutiny, even if multi-factor authentication (MFA) has already succeeded.

4. Collaboration and Data Sharing Between CSPs: CSPs should be required to share anonymized fraud detection data with each other, allowing for better cross-provider fraud detection and early warnings. For instance, if a fraudster is detected at one CSP, others can take preemptive measures to block similar attempts.

5. Resilience to MFA Bypass Techniques: We recommend implementing stricter requirements for preventing MFA bypass, including enhanced identity verification steps when recovering access to accounts or resetting authentication mechanisms. This could involve AI-based fraud checks during these recovery processes.

6. Incident Sharing with Security Teams in Real Time: CSPs should implement systems that automatically notify internal security teams about potential fraud incidents in real time, along with tools to freeze or mitigate damage. Integrating automated responses with real-time human review could prevent incidents from escalating.

- *Q: Are the fraud requirements sufficiently described to allow for appropriate balancing of fraud, privacy, and usability trade-offs?*

A: The CSP-AB commend NIST for taking a proactive approach to balancing trade-offs. We offer three suggestions for further improvements:

1. Advanced Analytics Guidance: Our members would welcome additional guidance on how advanced behavioral analytics can be used for fraud detection without collecting intrusive personal data could help organizations implement more privacy-friendly fraud controls.

2. Risk-Based Approach Guidance: We encourage NIST to provide more detailed examples of risk-based authentication and fraud prevention strategies could help organizations better understand how to scale their fraud prevention efforts according to the risk profile of their services.

3. Performance Metrics: We encourage NIST to provide clearer guidance on what metrics to use when evaluating the trade-offs between fraud prevention, privacy, and usability, as this could help organizations fine-tune their systems. For example, Fraud Detection Rate may cause frequent false positives if not tuned well, costing the business and users time and labor to resolve. Similarly, overly aggressive data collection for fraud detection could expose user data during security incidents.

- *Q: Are the added identity evidence validation and authenticity requirements and performance metrics realistic and achievable with existing technology capabilities?*

A: Biometric authentication, document verification, and continuous identity monitoring systems have matured significantly and can meet the performance metrics outlined in the draft. However, the implementation complexity and associated costs may vary depending on the organization's current technology infrastructure and resource availability. For organizations that are less technologically advanced, cloud-based identity services and phased implementations may help bridge the gap.

Q3. Authentication and Authenticator Management

- *Are the syncable authenticator requirements sufficiently defined to allow for reasonable risk-based acceptance of syncable authenticators for public and enterprise-facing uses?*

A: In our view, the guidelines provide a solid foundation for securing syncable authenticators, particularly by emphasizing secure syncing mechanisms with encryption; Multi-factor authentication for syncing; and Risk-based flexibility, allowing organizations to scale requirements based on the security needs of their environment.

- *Q: Are there additional recommended controls that should be applied? Are there specific implementation recommendations or considerations that should be captured?*

A: The CSP-AB offers the following additional recommendations:

1. Requiring conditional access policies would allow for heightened security. For example, conditional access allows organizations to dynamically adjust authentication requirements based on context, such as user location, device compliance, or behavior patterns.
2. Device Trust - synching authenticators on devices that are untrusted could compromise the security chain. Devices should provide attestation, or syncing should be blocked. Likewise, Endpoint Security Monitoring would be useful for enterprise authenticator devices to continuously monitor device security and disable authenticator syncs on devices that exhibit suspicious behavior.
3. Session Binding/Token Expiration - reduces the impact of long term credential exposure if a device is compromised.
4. User Behavior Analysis - Deploy user behavior analytics (UBA) and risk-based MFA to dynamically adjust authentication requirements based on user behavior. For example, unusual login times, unusual device use, or rapid geographic movement can trigger additional MFA steps or block access until further verification.
5. Stronger Data Encryption Mechanisms - When syncing authenticators (such as passwords or OTP generators) via the cloud, implement advanced encryption standards (e.g., Post Quantum Encryption) with secure key management. For high-assurance environments, end-to-end encryption can ensure that only the user and authorized systems can decrypt the authenticator data.

- *Q: Are wallet-based authentication mechanisms and "attribute bundles" sufficiently described as authenticators? Are there additional requirements that need to be added or clarified?*

A: The CSP-AB offers the following additional recommendations:

1. Wallet Revocation and Recovery: The CSP-AB encourages NIST to add more detailed guidance on how to securely handle wallet loss or revocation, including requirements for attribute bundle invalidation and recovery mechanisms.
2. Attribute Verification: Our members would welcome the addition of specific timelines or triggers for re-verifying attribute bundles.
3. Data Encryption Mechanisms: We encourage NIST to provide more clarity on acceptable algorithms for ensuring cryptographic protection (such as post quantum).
4. Real Time Security Alerts: Contemplate incorporating guidance on real-time security detection, including the ability to issue alerts if wallet-based authentications exhibit anomalous behavior (e.g., multiple failed activation attempts or suspicious geographic locations).

Q4. Federation and Assertions

- *Is the concept of user-controlled wallets and attribute bundles sufficiently and clearly described to support real-world implementations? Are there additional requirements or considerations that should be added to improve the security, usability, and privacy of these technologies?*

A: The CSP-AB offers the following considerations:

1. User Controlled Wallets: Although the core functionality is covered, we believe further clarification on lifecycle management (e.g., updating, revoking, and recovering wallets) could be beneficial, particularly when a user loses access to their wallet or changes devices.
2. Consider providing more detailed interoperability guidelines to ensure that wallet-based authentication mechanisms are platform-agnostic and work seamlessly across devices and services. This includes ensuring that cryptographic standards and identity assertion formats are uniformly implemented.
3. Consider mandating that wallets provide fine-grained control over which attributes are shared with an RP, allowing users to approve or deny the sharing of specific information during each authentication request.
4. Consider requiring wallets to integrate phishing-resistant protocols such as FIDO2/WebAuthn to ensure that only legitimate, user-initiated requests are processed. This could involve user-confirmation steps (e.g., physical button press or biometric scan) to prevent malware from automatically approving requests.
5. Attribute Bundles: Our members would welcome more detailed guidance on how RPs should validate the authenticity and freshness of the attribute bundles. Additionally, providing examples of derived attribute values could help organizations better understand how to limit unnecessary data exposure.
6. Consider introducing a requirement for expiration timestamps in attribute bundles or enforce periodic re-verification of certain critical attributes (e.g., address or employment status). This would ensure that RPs are working with up-to-date information without requiring direct interaction with CSPs for every transaction.

Q5. General

- *What specific implementation guidance, reference architectures, metrics, or other supporting resources could enable more rapid adoption and implementation of this and future iterations of the Digital Identity Guidelines?*

A: Playbooks can be highly effective tools: A playbook could detail the processes and technology needed to implement MFA or syncable authenticators, including system configurations, deployment best practices, and troubleshooting tips.

Mapping Industry Standards and Technologies: Mapping NIST's identity assurance levels (IAL, AAL, FAL) to industry standards (e.g., FIDO2, OAuth 2.0, SAML, OpenID Connect) and widely used technologies would be highly beneficial. Similarly, a reference guide that shows how FIDO2/WebAuthn-based MFA can meet AAL2/AAL3 requirements or how OpenID Connect can support identity federation under the guidelines.

Toolkits and Software Libraries can support implementation:

- Open-source toolkits, APIs, and software libraries that developers can directly integrate into their applications to implement the NIST guidelines.
- Providing ready-made code and libraries would significantly lower the barrier to adoption, especially for smaller organizations or those with limited development resources.
- A library for implementing user-controlled wallets or attribute bundles, offering built-in encryption, authentication protocols, and user interfaces aligned with NIST standards.

- *Q: What applied research and measurement efforts would provide the greatest impacts on the identity market and advancement of these guidelines?*

A: The CSP-AB offers the following considerations:

Frictionless Authentication

Many users abandon services due to cumbersome identity proofing and authentication processes. Research aimed at reducing friction while maintaining high security is critical. A more seamless user experience would encourage broader adoption, especially in consumer-facing services. It would also make high-assurance identity systems more accessible in emerging markets or sectors where technology infrastructure is limited.

Accessibility in Identity Systems

Research on designing identity solutions that accommodate users with visual, auditory, or cognitive impairments, focusing on ensuring equitable access. This research would enable more inclusive identity systems, opening the market to underserved populations and complying with accessibility standards such as ADA and WCAG.

Research on Zero-Knowledge Proofs

ZKPs allow users to prove possession of certain attributes (e.g., age, citizenship) without revealing unnecessary personal data. This can significantly enhance privacy in identity verification processes. Widespread adoption of privacy-preserving methods like ZKPs could greatly enhance user trust and mitigate concerns about data overexposure, especially in highly regulated sectors where privacy is paramount.

Data Minimization and Selective Disclosure Mechanisms

Users often disclose more information than necessary during authentication processes, creating privacy risks. More robust data minimization practices would increase user confidence in sharing personal information, thus driving adoption of digital identity systems in sensitive sectors like healthcare and finance.

Blockchain and Decentralized Identity Research

Decentralized identity solutions offer users control over their data and enable secure, self-sovereign identities. However, blockchain-based identity systems are still nascent and require further development to ensure scalability, security, and interoperability. This research could accelerate the adoption of decentralized identity solutions.

Advanced Cryptographic Techniques for Authentication

Current cryptographic techniques need to evolve to handle new challenges, including quantum computing threats. Research on quantum-resistant encryption for identity management systems, as well as advanced cryptographic techniques such as multi-party computation (MPC) and homomorphic encryption for secure identity proofing and attribute verification.

Thank you for consideration of our comments, we would be happy to discuss any of these points further at your convenience.

Sincerely,

Laura Navaratnam

Executive Director

The Cloud Service Providers - Advisory Board

[redacted].

http://csp-ab.com