NIST Adds Passkey Considerations to Digital ID Guidelines

April 24, 2024

The National Institute of Standards and Technology has announced a new supplement to the NIST SP 800-63B Digital Identity Guidelines, which provides interim guidance for incorporating "syncable authenticators" such as passkeys into digital identity management systems. This supplement is designed to update the guidelines without waiting for a full revision, allowing for quicker adaptation to new technologies.

Syncable authenticators, which enable a private key to be cloned and used across different devices, offer benefits like phishing resistance, easier recovery, and support for biometrics, enhancing user and agency flexibility. NIST's new supplement specifically addresses their use at Authentication Assurance Level 2 (AAL2) and responds to the evolving standards and widespread adoption of these technologies.

Authentication Assurance Level 2 is one of the three levels defined in the NIST Digital Identity Guidelines that specify the assurance in the identity of the user in a digital authentication process. AAL2 provides a moderate level of assurance and is designed to protect against a broader range of potential threats than AAL1, including more sophisticated fraud risks. It typically requires that users provide at least two different factors of authentication, such as something they know (a password or PIN) and something they have (a security token or mobile device authenticator).

Although there are inherent risks with key cloning, the new supplement outlines requirements to mitigate such issues. These include:

- **Secure Storage**: Ensuring that both the original and cloned keys are stored securely using encryption, so that they are protected even if the storage medium is compromised.
- **Secure Transmission**: When keys need to be transmitted between devices or systems, this should be done using secure, encrypted communication channels to prevent interception by unauthorized parties.
- **Access Controls**: Implementing strict access controls and monitoring mechanisms to detect and respond to unauthorized attempts to access or use the cloned keys.
- **Authentication Protocols**: Using robust authentication protocols that can ensure the integrity and authenticity of the key during the cloning process and thereafter.
- **Audit and Compliance**: Regular audits and compliance checks to ensure that all security measures are in place and functioning as expected.
- **User Education**: Educating users about the safe handling of authentication keys, the risks associated with key cloning, and the steps they can take to protect themselves.

The NIST has decided not to wait for the complete revision of the guidelines (Revision 4) to include this update, citing the immediate need for agencies to deploy these modern, secure authentication methods as part of a broader Federal Zero Trust strategy. Feedback from earlier public comments has been incorporated into this supplement, and further comments will be considered during the upcoming public comment period for Revision 4.

Source: NIST

–

(Originally published on Mobile ID World)

Related News

ID Talk: Passkeys, Standards, and Selfie Certification with FIDO's Andrew Shikiar

Visa Brings Passkeys to Online Payments in Major FIDO Victory

Biometric Privacy Lawsuits Don't Only Happen in Illinois – Identity News Digest

Google Makes Passkeys Default Login Option for Personal Accounts

Hackers Take the Stage – Identity News Digest

NIST, Tech Giants Commit to White House Cybersecurity Effort

Filed Under: News

Tagged With: AAL2, authentication assurance level, Biometric, biometrics, cybersecurity, digital identity guidelines, key cloning, NIST, passkeys, phishing resistance, syncable authenticators, zero trust strategy

Neurotechnology, founded in 1990 in Vilnius, Lithuania, leverages neural networks for biometric identification, computer vision, robotics, and AI. Surviving the "neural networks winter," the company thrived post-2012 with advancements in deep learning. Neurotechnology employs over 100 people, with 15% holding Ph.D.s and half engaged in R&D. The company has developed projects in object recognition and various other applications, capitalizing on deep neural network innovations. https://neurotechnology.com/

HID

HID powers the trusted identities of the world's people, places and things. Our trusted identity solutions give people convenient and secure access to physical and digital places and connect things that can be identified, verified and tracked digitally. Millions of people use HID products to navigate their everyday lives, and billions of things are connected through HID technology. https://www.hidglobal.com/

Prove

As the world moves to a mobile-first economy, businesses need to modernize how they acquire, engage with, and enable consumers. Prove's phone-centric identity tokenization and passive cryptographic authentication solutions reduce friction, enhance security and privacy across all digital channels, and accelerate revenues while reducing operating expenses and fraud losses. Over 1,000 enterprise customers use Prove's platform to process 20 billion customer requests

annually across industries including banking, lending, healthcare, gaming, crypto, e-commerce, marketplaces, and payments.
https://www.prove.com/

RECENT POSTS

- Mall of America Introduces Facial Recognition Security System
- AI Update: ChatGPT’s Lips are Sealed
- Identity News Digest – June 27, 2024
- Facial Recognition Factors Big Into Hyundai’s ‘Robot Total Solution’
- ID R&D Gets US Patent for Tech to Fight Voice Deepfake Threat

BIOMETRIC ASSOCIATIONS

ibia

fido alliance member