Withdrawn NIST Technical Series Publication

Warning Notice

The attached publication has been withdrawn (archived), and is provided solely for historical purposes. It may have been superseded by another publication (indicated below).

Withdrawn Publication	
Series/Number	NIST Special Publication 800-63Bsup1
Title	Incorporating Syncable Authenticators Into NIST SP 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management
Publication Date(s)	April 2024
Withdrawal Date	August 1, 2025
Withdrawal Note	NIST SP 800-63Bsup1 is withdrawn and superseded in its entirety by NIST SP 800-63B-4.

Superseding Publication(s) *(if applicable)*

The attached publication has been **superseded by** the following publication(s):

Series/Number	NIST SP 800-63B-4
Title	Digital Identity Guidelines: Authentication and Authenticator Management
Author(s)	David Temoshok, et al.
Publication Date(s)	July 2025
URL/DOI	https://doi.org/10.6028/NIST.SP.800-63B-4

Additional Information *(if applicable)*

Contact	Applied Cybersecurity Division (Information Technology Laboratory)
Latest revision of the attached publication	
Related Information	https://csrc.nist.gov/pubs/sp/800/63/b/4/final https://www.nist.gov/identity-access-management/nist-special-publication-800-63-digital-identity-guidelines
Withdrawal Announcement Link	

Date updated: July 24, 2025

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication 800
NIST SP 800-63Bsup1

Incorporating Syncable Authenticators Into NIST SP 800-63B

Digital Identity Guidelines — Authentication and Lifecycle Management

Ryan Galluzzo
Andrew Regenscheid
David Temoshok
Connie LaSalle

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63Bsup1

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication 800
NIST SP 800-63Bsup1

Incorporating Syncable Authenticators Into NIST SP 800-63B

Digital Identity Guidelines — Authentication and Lifecycle Management

Ryan Galluzzo
David Temoshok
Connie LaSalle
Applied Cybersecurity Division
Information Technology Laboratory

Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63Bsup1

April 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies

Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History

Approved by the NIST Editorial Review Board on 2024-04-11

How to Cite this NIST Technical Series Publication

Galluzzo R, Temoshok D, LaSalle C, Regenscheid A (2024) Incorporating Syncable Authenticators Into NIST SP 800-63B: Digital Identity Guidelines — Authentication and Lifecycle Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63Bsup1. https://doi.org/10.6028/NIST.SP.800-63Bsup1

Author ORCID iDs

Ryan Galluzzo: 0000-0003-0304-4239
Andrew Regenscheid: 0000-0002-3930-527X
David Temoshok: 0000-0001-6195-0331
Connie LaSalle: 0000-0001-6031-7550

Contact Information

dig-comments@nist.gov

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information

Additional information about this publication is available at <CSRC link>, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

This supplement to NIST Special Publication 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*, provides agencies with additional guidance on the use of authenticators that may be synced between devices.

Keywords

authentication; authentication assurance; digital authentication; digital credentials; digital identity; electronic authentication; electronic credentials; passkey; syncable authenticator.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Note to Readers

This document is a supplement to NIST Special Publication (SP) 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*. It incorporates the use of duplicated authenticators — known as *syncable authenticators* or passkeys — into the authentication techniques described in that guideline. At the time of publication, NIST is developing revisions of the SP 800-63 publications. When issued as final reports, the SPs will supersede this supplement. Any comments on this document should be submitted during the second public comment period for SP 800-63-4 in mid-2024.

Table of Contents

List of Tables

1. Introduction

The NIST Digital Identity Guidelines [1] provide the process and technical requirements for digital identity, including identity proofing, authentication, and federation. NIST Special Publication (SP) 800-63B (Volume B associated with SP 800-63-3) specifically addresses the requirements for authentication and life cycle management to include specific requirements for each type of acceptable authenticator.[2] Revision 3 is the most recent major revision to the guidelines and was published in June of 2017. While an update to the entire series is ongoing and will culminate in Revision 4, the pace of technology is more rapid than NIST's typical document development and review processes, warranting this supplemental update.

One such authenticator type addressed in SP 800-63B is a multi-factor cryptographic authenticator. Typically, this authentication type protects a cryptographic key in hardware or software that requires activation through a second authentication factor, either a memorized secret or a biometric characteristic. Protecting the private key from unauthorized exposure is fundamental to the security model of a multi-factor cryptographic authenticator. This traditionally includes ensuring that private keys are not exportable or cloneable. However, this paradigm is starting to change. Notably, a new series of authentication protocols and specifications has led to the rapid adoption of syncable authenticators (commonly referred to as "passkeys"), which allow users to synchronize (i.e., duplicate) a private key between different devices.

When SP 800-63-3 was published in 2017, two key supporting specifications — Fast Identity Online (FIDO) Client to Authenticator Protocol (CTAP) [3] and W3C's Web Authentication [4] (known as FIDO2 when used together) — did not exist, nor did a robust, well-understood ecosystem of implementations. Based on the type of cryptographic authenticators available at the time, the 2017 guidelines restricted the ability of multi-factor cryptographic authenticators to "clone" a key to other devices. However, the ecosystem has accelerated rapidly in the last two years, and most major platform providers now implement scaled, syncable authentication capabilities. These authenticators offer many benefits, including support for phishing resistance,[1] the ability to be bound to specific relying parties, elimination of the need to transmit passwords, simplified authenticator recovery, and the use of a wide variety of device-native biometrics and PINs as a second factor to accompany the stored private key. They also offer convenience that fits an increasingly multi-device and multi-platform world.

As with any new technology, the promise of innovation is accompanied by new threats and challenges that must be explored and understood. As such, this supplement provides an overview of the considerations that federal agencies should weigh, including contemporary threats, as they determine whether and how to implement syncable authenticators.

[1] An authenticator is phishing-resistant if it is a cryptographic authenticator that binds its output to a communication channel (e.g., client-authenticated TLS) or a verifier name (e.g., FIDO2/WebAuthN). Both techniques prevent the authenticator output from being used outside of the intended context. For more on phishing resistance, see SP 800-63B-4 and OMB Memorandum 22-09, *Zero Trust Implementation Strategy*.

2. Purpose

The purpose of this document is to adapt current NIST guidelines to reflect the changing authentication and credential marketplace. This supplement describes how syncable authenticators mitigate threats in a manner consistent with the established Authentication Assurance Levels in SP 800-63-3 and provides federal agencies with an understanding of syncable authenticator capabilities that can be leveraged to achieve SP 800-63-3 Authentication Assurance Level 2 (AAL2). It also provides updates to the use of software cryptographic authenticators discussed in Sec. 5.1.8 of SP 800-63B [2], specifically the ability of said authenticators to support AAL2 authentication requirements even when a key has been duplicated (e.g., “cloned” or “synced”) to another device. Finally, this document provides some considerations for implementation based on two use case types: public-facing applications (i.e., federal information systems that interact with public identities, as described in OMB Memorandum M-19-17) and federal enterprise applications (i.e., federal information systems that primarily interact with federal enterprise identities, as described in OMB Memorandum M-19-17). This document supplements existing guidance found in SP 800-63-3, and it will be superseded by the final version of SP 800-63B-4.

3. Syncable Authenticators Achieve AAL2

NIST's Authenticator Assurance Levels are primarily structured around an authenticator's ability to protect against certain threats to the authentication process. At AAL2, the intent is to provide a high degree of confidence that a user possesses two single-factor authenticators, or a multi-factor authenticator bound to the user's account. Table 1 illustrates the required threat mitigations from SP 800-63-3 [1] and how a properly configured syncable authenticator protects against these threats.

Table 1. Required threat mitigations from SP 800-63-3 (Table 4-1) [1]

Requirement	AAL2	Syncable Authenticators (e.g., Passkeys)
Man in the Middle resistance	Required	**Achieved.** Properly configured syncable authenticators exchange all authentication data by way of authenticated and protected channels.
Verifier-impersonation resistance	Not required	**Achieved.** Properly configured syncable authenticators create a unique public or private key pair whose use is constrained to the domain in which it was created (i.e., the key can only be used with a specific website or relying party). This prevents a falsified web page from being able to capture and re-use an authenticator output.
Verifier-compromise resistance	Not required	**Achieved.** Properly configured syncable authenticators only store public keys on the verifier side. These keys cannot be used to authenticate as the user. Private keys stored by the syncing fabric are only stored in an encrypted form using approved cryptography. Access controls prevent anyone other than the authenticated user from accessing the stored keys.
Replay resistance	Required	**Achieved.** Syncable authenticators prevent replay resistance (i.e., prevention of reuse in future transactions) through the use of a random nonce incorporated into each authentication transaction.
Authentication intent	Recommended	**Achieved.** Syncable authenticators require the user to input an activation secret to initiate the cryptographic authentication protocol. This serves as authentication intent as the event cannot proceed without the user's active participation.

Section 5 discusses additional considerations around the configuration of syncable authenticators.

To meet AAL2 requirements, the syncable authenticator **SHALL** make use of a local authentication event to unlock the locally stored key or **SHALL** be used with another authenticator (e.g., a user-selected password) if no local authentication mechanism is available. In the FIDO2 Web Authentication (WebAuthn) context, this will be indicated by the value of the User Verification flag available in the authenticator data of the W3C Web Authentication specifications. See Sec. 5 for more details on FIDO2 WebAuthn Authenticator data flags.

4. Updates on the Allowance of Cloning Authentication Keys

SP 800-63B, Section 5.1.8.1, Multi-Factor Cryptographic Software Authenticators, restricts the ability of an authenticator to "clone" a cryptographic authentication key from one device to another. Specifically, it states:

> Multi-factor cryptographic software authenticators SHOULD discourage and SHALL NOT facilitate the cloning of the secret key onto multiple devices.

Syncable authenticators explicitly facilitate key cloning to provide the user with access to previously enrolled authenticators across devices and different platform providers. This is an experience that can be both secure and convenient if done correctly — a reality acknowledged by NIST's removal of this restriction from the initial public draft (ipd) of SP 800-63B-4.

Effective at the time of the publication of this document, the above statement in section 5.1.8.1 is superseded by this supplement and syncable authenticators that are deployed under the requirements set forth in this supplement **SHALL** be considered sufficient to protect against threats contemplated under AAL2.

General requirements for all uses of syncable authenticators:

- All keys **SHALL** be generated using approved cryptography.
- Private keys that are cloned or exported from a device **SHALL** only be stored in an encrypted form.
- All authentication transactions **SHALL** perform private-key operations on the local device using cryptographic keys that were generated on-device or recovered from the sync fabric (e.g., in cloud storage).
- Private keys stored in cloud-based accounts **SHALL** be protected by access control mechanisms such that only the authenticated user can access their private keys in the sync fabric.
- User access to private keys in the sync fabric **SHALL** be protected by AAL2 equivalent MFA to preserve the integrity of the authentication protocols using the synced keys.
- These general requirements and any other agency-specific requirements for the use of syncable authenticators **SHALL** be documented and communicated, including on public-facing websites and digital service policies, where applicable.

Additional requirements for federal enterprise[2] use of syncable authenticators:

- Federal enterprise private keys (i.e., federal keys) **SHALL** be stored in sync fabrics that have achieved FISMA Moderate protections or comparable.

[2] For the purposes of these requirements, federal enterprise systems and keys include what would be considered in-scope for PIV guidance, such as government contractors, government employees, and mission partners. It does not include government-to-consumer or public-facing use cases.

- Devices (e.g., mobile phones, laptops, tablets) that generate, store, and sync authenticators containing federal enterprise private keys **SHALL** be protected by mobile device management software or other device configuration controls that prevent the syncing or sharing of keys to unauthorized devices or sync fabrics.
- Access to the sync fabric **SHALL** be controlled by agency-managed accounts (e.g., a central identity and access management solution or platform-based managed account) to maintain enterprise control over the life cycle of the private key.
- Authenticators that generate private keys **SHOULD** support attestation features that can be used to verify the capabilities and source of the authenticator (e.g., enterprise attestation).

These controls specifically support syncing and should be considered additive to the existing multi-factor software cryptographic authenticator requirements and AAL2 requirements, including FIPS 140 validation.

5. Implementation Considerations and Requirements

Syncable authenticators are built upon W3C's WebAuthn specification, which provides a common data structure, a challenge-response cryptographic protocol, and an API for leveraging public-key credentials. The specification is flexible and adaptive, meaning that not all deployments of WebAuthn credentials will meet the requirements of federal agencies for implementation.

The specification has a series of "flags" that the relying party (RP) application can request from the authenticator to provide additional context for the authentication event and determine whether it meets the RP's access policies. This section describes certain flags in the WebAuthn specification that federal agencies acting as RPs should understand and interrogate when building their syncable authenticator implementations to align with NIST AAL2 threat mitigations.

Table 2. WebAuthn Level 3 flags

Flag	Description	Requirements & Recommendations
User Present (UP)	Indicates a "presence" test to confirm that the user has interacted with the authenticator (e.g., tapping hardware token inserted into a USB port)	Federal agencies **SHALL** confirm that the User Present flag has been set. Supports **Authentication Intent**.
User Verified (UV)	Indicates that the user has been locally authenticated by the authenticator using one of the available "user verification" methods	Federal agencies **SHALL** indicate that UV is preferred, and all assertions **SHALL** be inspected to confirm the value of the UV flag. This indicates whether the authenticator can be treated as a **multi-factor cryptographic authenticator**. If the user is not verified, agencies may still treat the authenticator as a **single-factor cryptographic authenticator** by adding an RP-specific memorized secret to the authentication event. A further extension to the WebAuthn Level 3 specification provides additional data on verification methods if agencies seek to gain context on the local authentication event [4]
Backup Eligibility	Indicates whether the authenticator *can* be synced to a different device (i.e., whether the key can be stored elsewhere). It's important to note just because an authenticator CAN be synced does not mean that it HAS been synced.	Federal agencies **MAY** use this flag if they intend to establish policies that restrict the use of **syncable authenticators**. This flag is necessary to distinguish between authenticators that are device-bound or those that may be cloned to more than one device.
Backup State	Indicates whether an authenticator *has* been synced to a different device	Federal agencies **MAY** use this flag if they intend to establish restrictions on authenticators that **have been synced** to other devices. For public-facing applications, agencies **SHOULD NOT** change the acceptance based on this flag due to user experience concerns. For enterprise decisions, this flag **MAY** be used to support the restriction of syncable authenticators for specific applications.

In addition to the flags indicated in Table 2, agencies may wish to gain greater information on the origins and capabilities of the syncable authenticators that they choose to implement and accept. Within the context of FIDO2 WebAuthn, some authenticators support attestation features that can be used to determine the capabilities and manufacturer of a specific authenticator. For enterprise use cases, agencies **SHOULD** implement attestation capabilities based on the functionality offered by their platform providers. Preferably, this would take the form of an enterprise attestation where the RP requests uniquely identifying information about the authenticator.

Attestations **SHOULD NOT** be used for broad public-facing applications. Such a requirement (i.e., one that blocks some public users' syncable authenticators if they do not support attestation) may divert users to less secure authentication options that are vulnerable to phishing, such as Short Message Service (SMS) one-time password (OTP).

Even if the RP requests flag and attestation data, the authenticator may not return all of the requested information, or it may return information that is inconsistent with the expected response mandated for access to a resource. Therefore, it is critically important that agencies evaluate the use cases for which they are using syncable authenticators and determine the appropriate access policy decisions they intend to make based on the returned information.

6. Syncable Authenticator Threats and Challenges

Syncable authenticators present some distinct threats and challenges that agencies should evaluate before implementation or deployment. Table 3 outlines these risks and suggested mitigations.

Table 3. Syncable authenticator threats, challenges, and mitigations

Threats and Challenges	Description	Syncable Authenticator Mitigations
Unauthorized key use or loss of control	Some syncable authenticator deployments support the sharing of private keys to devices that belong to other users who can then misuse the key.	- Enforce enterprise device management features or managed profiles that prevent the sharing of synced keys. - Notify users of key-sharing events through all available notification channels. - Provide mechanisms for users to view keys, key status, and whether/where keys have been shared. - Educate users about the risk of unauthorized key use through existing awareness and training mechanisms.
Sync fabric compromise	To support key syncing, most implementations clone keys to a "sync fabric," which is a cloud-based service connected to multiple devices associated with an account.	- Store only encrypted key material. - Implement syncing fabric access controls that prevent anyone other than the authenticated user from accessing the private key. - Evaluate cloud services for baseline security features (e.g., FISMA Moderate protections or comparable). - Leverage hardware security modules to protect encrypted keys.
Unauthorized access to sync fabric and recovery	Synced keys are accessible via cloud-based account recovery processes. These processes represent a potential weakness to the authenticators.	- Implement authentication recovery processes that are consistent with SP 800-63B. - Restrict recovery capabilities for federal enterprise keys through device management or managed account capabilities. - Bind multiple authenticators at AAL2 and above to support recovery. - Require AAL2 authentication to add any new authenticators for user access to the sync fabric. - Use only as a derived authenticator in federal enterprise scenarios [6] - Notify the user of any recovery activities. - Leverage a user-controlled secret (i.e., something not known to the sync fabric provider) to encrypt and recover keys.

Threats and Challenges	Description	Syncable Authenticator Mitigations
Revocation	Since syncable authenticators use RP-specific keys, the ability to centrally revoke access based on those keys is challenging. For example, with traditional PKI, CRLs can be used centrally to revoke access. A similar process is not available for syncable authenticators (or any FIDO WebAuthn-based credentials).	- Implement a central Identity Management (IDM) account for users to manage authenticators and remove said authenticators from the "home agency" account if compromised or expired. - Leverage SSO and federation to limit the number of RP-specific keys that will need to be revoked in an incident. - Establish policies and tools to periodically request that users review keys for validity and currency.

7. Sharing

Cybersecurity guidelines have historically cautioned against sharing authenticators between users, expecting that different users would maintain their own unique authenticators. Despite this guidance, authenticator and password sharing occurs within some user groups and applications to allow individuals to share access to a digital account.

As indicated in Table 3, some syncable authenticator implementations have embraced this user behavior and have established methods for sharing authentication keys between different users. Further, some implementations actively encourage the sharing of syncable authenticators as a convenient and more secure alternative to password-sharing for common services.

For enterprise use cases, concerns over sharing keys can be effectively mitigated using device management techniques that limit the ability for keys to be moved off approved devices or sync fabrics. However, similar mitigations are not currently available for public-facing use cases, leaving relying parties dependent on the sharing models adopted by syncable authenticator providers. Owners of public-facing applications should be aware of risks associated with shared authenticators. When interacting with the public, agencies have limited visibility into which specific authenticators are being employed by their users and should assume that all syncable authenticators may be subject to sharing. While many sharing models have substantial controls that minimize risks (e.g., requiring close proximity between devices to allow sharing), other implementations are less restrictive.

The risk of sharing posed by this new class of authenticators is not unique. In fact, it applies to all AAL2 authenticator types, some of which are weaker than syncable authenticators. Any authenticator at AAL2 can be shared by a user who is determined to share it. Users can actively share passwords, OTPs, out-of-band authenticators, and even push authentication events or allow a designee (whether formal or not) to authenticate on behalf of an end user.

Agencies determine which authenticators they will accept for their applications based on the specific risks, threats, and usability considerations they face. Syncable authenticators may be offered as a new option for applications seeking to implement up to AAL2, and, like any authenticator, the trade-offs of this technology should be well balanced based on their expected outcomes for security, privacy, equity, and usability.

8. Conclusion

Syncable authenticators represent a substantive technological shift in the authentication landscape, particularly in the use of multi-factor cryptographic authenticators. Their proliferation will result in an inevitable evaluation of the trade-offs associated with allowing cryptographic keys to be replicated and stored in cloud infrastructure. While this presents distinct risks (e.g., loss of enterprise control over authentication keys), it also provides a pathway to convenient, phishing-resistant authenticators that eliminate a primary threat vector for the public and enterprises. Syncable authenticators will not be appropriate for all use cases. However, when deployed in a manner that is consistent with the guidelines contained in this supplement, they can achieve alignment with AAL2 risk mitigations and promote the adoption of phishing-resistant authentication more broadly.

This document is a companion to the existing Digital Identity Guidelines [1], which provide agencies with information that will allow them to make informed risk-based decisions and — where appropriate — integrate the latest in industry innovation.

References

[1] Grassi PA, Garcia ME, Fenton JL (2017) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63-3, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63-3

[2] Grassi PA, Newton EM, Perlner RA, Regenscheid AR, Fenton JL, Burr WE, Richer JP, Lefkovitz NB, Danker JM, Choong Y-Y, Greene KK, Theofanos MF (2017) Digital Identity Guidelines: Authentication and Lifecycle Management. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63B, Includes updates as of March 02, 2020. https://doi.org/10.6028/NIST.SP.800-63B

[3] Fast Identity Online Alliance (2023) Client to Authenticator Protocol 2.2. https://fidoalliance.org/specs/fido-v2.2-rd-20230321/fido-client-to-authenticator-protocol-v2.2-rd-20230321.html

[4] World Wide Web Consortium (2021) Web Authentication: An API for Accessing Public Key Credentials Level 3. https://www.w3.org/TR/webauthn-3/

[5] Word Wide Web Consortium (2021) Web Authentication: An API for Accessing Public Key Credentials Level 3. Section 10.2 Authenticator Extensions. https://www.w3.org/TR/webauthn-3/#sctn-defined-authenticator-extensions

[6] Ferraiolo H, Regenscheid AR, Fenton J (2023) Guidelines for Derived Personal Identity Verification (PIV) Credentials. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-157r1 ipd (initial public draft). https://doi.org/10.6028/NIST.SP.800-157r1.ipd

Appendix A. Glossary

New terms introduced in this supplement are included below. All other terms used are consistent with the Glossary in SP 800-63-3, which is available at https://doi.org/10.6028/NIST.SP.800-63-3.

syncable authenticators
Software or hardware cryptographic authenticators that allow authentication keys to be cloned and exported to other storage in order to sync those keys to other authenticators (i.e., devices).

sync fabric
Any on-premises, cloud-based, or hybrid service used to store, transmit, or manage authentication keys generated by syncable authenticators that are not local to the user's device.