What Are NIST AAL Levels? AAL1, AAL2, and AAL3 Without the Standards Headache

Definitions / Last updated 2026-06-11 / https://www.scrambleid.com/learn/what-are-nist-aal-levels

In one sentence: Authenticator Assurance Levels (AAL) are NIST's three-tier framework, defined in SP 800-63B (and updated in the SP 800-63-4), for how confident the relying party can be that the person presenting the authenticator is the same person who originally bound it to the account.

TL;DR (canonical)

- **AAL1:** Some assurance. Single-factor authentication permitted. Suitable for low-risk applications where credential compromise has limited impact.
- **AAL2:** High assurance. Two distinct factors required, with cryptographic mechanisms and several specific resistance properties. The default for most enterprise and consumer scenarios.
- **AAL3:** Very high assurance. Hardware-based cryptographic authenticator with verifier-impersonation resistance and verifier-compromise resistance. Required for the highest-risk applications and for the strongest M-22-09 / FedRAMP postures.
- **AAL is one of three assurance dimensions.** Identity Assurance Level (IAL) covers how confidently the person was proofed at registration. Federation Assurance Level (FAL) covers the strength of federated assertions across trust boundaries.
- **AAL is a property of the ceremony, not the authenticator alone.** The same authenticator can meet different AALs depending on configuration, attestation, and the specific deployment.
- **NIST SP 800-63-4 was finalized in July 2025** and supersedes 800-63-3. Coordinate with your auditor on the transition timeline applicable to your compliance regime.

The NIST 800-63 family in one frame

Volume	What it covers
SP 800-63	Overall framework and risk management
SP 800-63A	Identity proofing and enrollment (IAL)
SP 800-63B	Authentication and lifecycle management (AAL)
SP 800-63C	Federation and assertions (FAL)

NIST SP 800-63-4 was finalized in July 2025 and updates all four volumes. The Revision 4 family is now the current standard; the older 800-63-3 family is superseded but may still apply to specific compliance regimes mid-transition. Verify which revision applies with your auditor.

AAL1: Some assurance

Requirements (paraphrased):

- Single-factor authentication permitted (e.g., a memorized secret).
- Replay resistance, eavesdropping resistance, and other baseline properties.
- No specific verifier-impersonation resistance required.

What qualifies:

- Memorized secrets (passwords) with reasonable strength rules.
- Single-factor cryptographic authenticators (rare in this tier).
- Single-factor OTP devices.

When AAL1 is appropriate:

- Low-risk applications where the cost of credential compromise is bounded.
- Public-facing read-only services where the user is more like an anonymous reader.
- Internal applications behind defense-in-depth that do not store sensitive data.

Practical note: AAL1 is no longer appropriate for any application that touches PII, payments, or privileged operations. Most enterprise and regulated applications start at AAL2 or higher.

AAL2: High assurance

Requirements (paraphrased):

- Two distinct factors of authentication, with at least one factor being cryptographic.
- Replay resistance, eavesdropping resistance, session-hijacking resistance.
- Cryptographic authenticators required for one of the factors.
- Reauthentication required at least once per 12 hours, or after 30 minutes of inactivity (per SP 800-63B).

What qualifies:

- Memorized secret + cryptographic software authenticator (e.g., password + TOTP from an app).
- Memorized secret + cryptographic device authenticator.
- Password + push with number-matching (in many implementations).
- FIDO2/WebAuthn passkeys (single-factor in form, multi-factor in property because they include user verification).

What doesn't qualify (or qualifies only with conditions):

- Two memorized secrets (same factor category) don't qualify.
- Memorized secret + SMS OTP qualifies only conditionally: NIST classifies SMS/PSTN as a RESTRICTED authenticator, which means it can satisfy AAL2 only if the organization assesses the risk, notifies users, and offers an alternative with a migration path.

When AAL2 is appropriate:

- Most enterprise workforce SSO.
- Most consumer financial and healthcare portals.
- The default starting point for new applications.

AAL3: Very high assurance

Requirements (paraphrased):

- Hardware-based cryptographic authenticator (private key in tamper-resistant hardware).
- Verifier-impersonation resistance (the authenticator cannot be tricked into producing a valid response for a fake verifier).
- Verifier-compromise resistance (a compromised verifier cannot subsequently authenticate as the user).
- Authentication intent: the user must take an explicit action that demonstrates intent to authenticate.
- Two distinct factors (the authenticator typically provides "something you have" plus "something you know" or "something you are").

What qualifies:

- FIDO2/WebAuthn with hardware-bound credentials and proper attestation.
- PIV smart cards built to FIPS 201-3.
- CAC cards (DoD).
- Other hardware-based cryptographic authenticators meeting the full set of properties.

What doesn't qualify:

- Software-only TOTP.
- Push notifications.
- SMS.
- Passwords + any of the above.

When AAL3 is appropriate:

- Federal privileged users (M-22-09 alignment).
- FedRAMP High systems and privileged users in FedRAMP Moderate.

- The highest-risk financial transactions.
- DoD CAC environments.
- Enterprise contexts where verifier-impersonation resistance and hardware binding are explicit requirements.

How AAL is determined

The AAL is not just a property of the authenticator. It's a property of:

1. **The authenticator type** (hardware vs software, single vs multi-factor).
2. **The attestation** (does the relying party have proof of which authenticator is in use?).
3. **The configuration** (is user verification enforced? are intent signals required?).
4. **The verifier implementation** (does it implement the resistance properties end to end?).
5. **The session management** (is reauthentication enforced at appropriate intervals?).

Two FIDO2 deployments can land at different AALs depending on attestation and configuration. The vendor and the auditor together determine the AAL of a specific deployment.

AAL vs IAL vs FAL

Dimension	What it covers	Defined in
IAL (Identity Assurance Level)	How confidently the relying party knows who the person actually is	SP 800-63A
AAL (Authenticator Assurance Level)	How confidently the relying party knows the same person is presenting the authenticator at this moment	SP 800-63B
FAL (Federation Assurance Level)	How strongly the federated assertion is bound to the user across trust boundaries	SP 800-63C

Each dimension has three levels. They can vary independently:

- A user can be **IAL2 + AAL3 + FAL2**: identity-proofed at remote-verified level, authenticating with hardware-bound phishing-resistant credential, federated through a holder-of-key assertion.
- Or **IAL1 + AAL2 + FAL1**: self-asserted identity, two-factor authentication, bearer-token federation.

The right combination depends on the risk of the application and the threat model.

Mapping authenticators to AAL

Authenticator	Typical AAL
Password	AAL1

Authenticator	Typical AAL
Password + SMS OTP	AAL2 only as a restricted authenticator (risk assessment, user notice, and a migration path required)
Password + TOTP	AAL2
Password + push (no number-matching)	AAL2 (with caveats; not phishing-resistant)
Password + push with number-matching	AAL2 (improved but not AAL3)
FIDO2/WebAuthn (synced passkey, software-bound)	AAL2 typically; some implementations approach AAL3
FIDO2/WebAuthn (device-bound, hardware-attested)	AAL3 typically achievable
Hardware security key (FIDO2 with attestation)	AAL3 typically achievable
PIV smart card (FIPS 201-3)	AAL3
CAC (DoD)	AAL3
Derived PIV in hardware	AAL3 typically achievable

These are typical assignments; the actual AAL depends on the specific implementation. Validate with NIST documentation and your auditor.

How to choose the right AAL for an application

A practical decision flow:

1. **What's the impact of an authentication compromise?** Low-impact reads, AAL1. PII or transaction-relevant, AAL2. Privileged or high-risk transaction, AAL3.
2. **What regulatory regime applies?** FedRAMP, HIPAA, PCI DSS, NYDFS, CJIS, OMB M-22-09 all imply different baselines.
3. **Do verifier-impersonation and verifier-compromise resistance matter?** If yes (privileged users, federal staff, high-value transactions), AAL3.
4. **Is recovery in scope?** The recovery flow must meet the same AAL as the primary; designing AAL3 primary with AAL1 recovery is self-defeating.
5. **What's the user-experience tolerance?** AAL3 has practical implementation considerations; the answer is rarely "AAL3 everywhere."

A risk-proportionate approach uses AAL3 on privileged and highest-risk paths, AAL2 as the default workforce and customer-facing baseline, and explicit step-up at the actions that warrant higher assurance.

Common misconceptions

"AAL3 means hardware security key only." Platform authenticators with hardware-protected key stores can meet AAL3 properties. AAL3 requires hardware-bound private keys, not specifically a separate USB device.

"FIDO2 is automatically AAL3." FIDO2 can meet AAL3 with the right authenticator, attestation, and configuration. Synced passkeys typically fall short of AAL3 on the verifier-compromise-resistance and hardware-binding properties.

"AAL2 is always enough." AAL2 is appropriate for many applications but not all. Federal privileged access, the highest-value financial transactions, and DoD environments require AAL3.

"AAL is set once at registration." AAL is a property of every authentication ceremony. A user registered to an AAL3 authenticator can still authenticate at lower assurance via a fallback flow; the lower assurance is what applies for that session.

"AAL covers identity proofing." No, IAL covers proofing. AAL is independent.

Key Takeaway

Authenticator Assurance Levels (AAL1, AAL2, AAL3) are NIST's three-tier framework for the strength of an authentication ceremony, defined in NIST SP 800-63B and updated in SP 800-63-4. AAL1 is single-factor; AAL2 is two-factor with cryptographic mechanisms; AAL3 requires hardware-bound cryptographic authenticators with verifier-impersonation resistance and verifier-compromise resistance. FIDO2/WebAuthn with hardware-bound credentials, PIV, and CAC can meet AAL3. SMS, push notifications, and TOTP do not. AAL is independent of IAL (Identity Assurance Level, about proofing) and FAL (Federation Assurance Level, about federated assertions). The actual AAL of a deployment depends on authenticator type, attestation, configuration, and verifier implementation; coordinate with your auditor for formal AAL determination.

FAQ

What are NIST AAL levels?

Authenticator Assurance Levels (AAL) are NIST's framework for the strength of an authentication ceremony. AAL1 provides some assurance the user is who they claim to be (single-factor permitted). AAL2 provides high assurance, requiring two distinct factors with cryptographic mechanisms and resistance to several attack types. AAL3 provides very high assurance, requiring hardware-bound cryptographic authenticators and verifier-impersonation resistance. AAL is defined in NIST SP 800-63B (final, 2017 with revisions) and updated in NIST SP 800-63-4.

What's the difference between AAL2 and AAL3?

AAL2 requires two distinct authentication factors and several specific resistance properties (replay, eavesdropping, session hijacking) but allows software-based authenticators and does not require verifier-impersonation resistance. AAL3 requires hardware-based cryptographic authenticators (the private key in tamper-resistant hardware), verifier-impersonation resistance, and verifier-compromise resistance. FIDO2/WebAuthn with hardware-bound keys, PIV, and CAC can satisfy AAL3. Push notifications, TOTP, and SMS cannot.

What's the difference between AAL and IAL?

AAL (Authenticator Assurance Level) is about the strength of the authentication ceremony at the moment of access. IAL (Identity Assurance Level) is about how confidently the relying party knows who the person actually is at registration. IAL is established at proofing time; AAL is exercised at every authentication. They are independent: a user can be registered at IAL2 but authenticate at AAL1, or the reverse. FAL (Federation Assurance Level) is a third dimension covering the strength of the federated assertion when authentication crosses trust boundaries. See What Is Identity Proofing?.

Does AAL3 require a hardware security key?

AAL3 requires the private key to be held in a hardware-protected key store, but that doesn't have to be a separate USB device. Platform authenticators using hardware-protected key stores (Secure Enclave on Apple, TPM on Windows, Android Keystore) can meet AAL3 requirements depending on the specific authenticator and configuration. Hardware security keys (YubiKey, etc.) are one path to AAL3; not the only path. The actual AAL determination depends on the specific authenticator implementation, attestation, and binding.

What does verifier-impersonation resistance mean?

Verifier-impersonation resistance is a property of the authentication ceremony where an attacker who stands up a fake verifier (a phishing site impersonating the real relying party) cannot trick the authenticator into producing a valid authentication response. FIDO2/WebAuthn achieves this by binding the signed assertion to the relying-party origin; the authenticator only signs valid challenges for the real origin. Verifier-impersonation resistance is a defining AAL3 property.

Is NIST SP 800-63-4 in force?

Yes. NIST SP 800-63-4 was finalized in July 2025 and supersedes NIST SP 800-63-3. The Revision 4 family (800-63A-4 for identity proofing, 800-63B-4 for authentication and lifecycle management, 800-63C-4 for federation) updates AAL definitions, sharpens phishing resistance and verifier-impersonation requirements, and revises identity proofing guidance. Federal agencies and contractors should align with Revision 4 going forward; coordinate with your auditor on the specific transition timeline that applies to your compliance regime.

References (public)

- NIST SP 800-63B (Authenticator and Lifecycle Management): https://csrc.nist.gov/pubs/sp/800/63b/4/final
- NIST SP 800-63-4: https://csrc.nist.gov/pubs/sp/800/63/4/final
- NIST SP 800-63A (Identity Proofing and Enrollment): https://csrc.nist.gov/pubs/sp/800/63a/4/final
- NIST SP 800-63C (Federation and Assertions): https://csrc.nist.gov/pubs/sp/800/63/C/4/final
- CISA, Implementing Phishing-Resistant MFA: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
- OMB M-22-09: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

Related reading

- What Is Phishing-Resistant MFA?
- What Is FIDO2?
- What Are Passkeys?
- What Is Identity Proofing?
- Compliance Mapping: NIST and CISA
- Phishing-Resistant Web Authentication