

Apple

Apple Anonymous Attestation in the WebAuthn Specification

In the WebAuthn specification, Apple introduced an anonymous attestation method called "[Apple Anonymous Attestation](#)". The primary purpose of this method is to protect user privacy. Specifically:

- Apple's anonymous attestation uses a fixed AAGUID. This means that all Apple devices will return the same AAGUID when undergoing WebAuthn authentication.
- Since all devices return the same AAGUID, relying solely on the AAGUID is insufficient to determine the authenticity of the device. This design aims to ensure user privacy but also presents certain challenges.
-

New Attestation Method in macOS Ventura and iOS 16

Based on the [information](#) from the Apple Developer forum, Apple has made changes to its authentication method in macOS Ventura and iOS 16:

- The traditional device-bound platform authenticator has been replaced by "Passkeys".
- These "Passkeys" do not provide an attestation statement. This is because the attestation model currently defined in WebAuthn was not designed with syncing credentials in mind.
-

In conclusion, Apple has made some changes to WebAuthn authentication in its latest operating system versions, notably introducing "Passkeys" as a new authentication method and providing an anonymous attestation method in the WebAuthn specification to enhance user privacy protection.

The behaviors of this new attestation are different in various browsers. Safari won't provide any information related to attestation statement and authData, while the other browsers will use self-attestation and their own AAGUID to achieve this attestation. Based on this fact, we can verify the device attestation response within an approximate range.

- Safari
- attestationObject.fmt = "none"
- attestationObject.attStmt = {}
- attestationObject.authData.attestedCredentialData.aaguid = "00000000-0000-0000-0000-000000000000"
- Chrome / Edge / Chrome-dev
- attestationObject.fmt = "packed"
- attestationObject.attStmt contains the self-attestation signature
- attestationObject.authData.attestedCredentialData.aaguid = "adce0002-35bc-c60a-648b-0b25f1f05503"
- Brave / Edge-dev
- attestationObject.fmt = "packed"
- attestationObject.attStmt contains the self-attestation signature
- attestationObject.authData.attestedCredentialData.aaguid = "b5397666-4885-aa6b-cebf-e52262a439a2"
-

More AAGUID specs can be found in [chromium](#).

[Previous](#) [Android](#) [Next](#) [Windows](#) Last updated 6 months ago On this page * [Apple Anonymous Attestation in the WebAuthn Specification](#) * [New Attestation Method in macOS Ventura and iOS 16](#)

Was this helpful?