Yubikey

Introduction of Yubikey

YubiKey, a popular hardware security key, provides strong two-factor authentication and can be used to protect online accounts, services, and applications from unauthorized access. One of the key features of YubiKey is its ability to generate cryptographic keys and signatures that can be used for authentication and attestation. By leveraging these cryptographic capabilities, YubiKey can prove its identity and integrity to a relying party.

Yubikey Attestation

Performing device attestation with YubiKey using WebAuthn involves a series of steps that ensure the authenticity of the device and the integrity of the attestation statement. The process begins when a user triggers their YubiKey to generate a new key pair, along with an attestation statement that attests to the device's authenticity. This attestation statement is then sent to an on-chain contract for verification.

The verification process on the blockchain involves several steps:

1. Verify WebAuthn Attestation Signature:
2. The on-chain contract first verifies that the signature in the WebAuthn attestation statement (attStmt) is valid. This is done by checking that the signature was created by the certificate (x5c[0]) included in the attStmt, and that it was signed over specific data.
3. Verify Certificate Chain :
4. The contract then verifies the certificate chain (x5c) included in the attStmt. This ensures that each certificate in the chain is signed by the next certificate, establishing a chain of trust.
5. Verify Root Certificate:
6. Finally, the contract verifies that the last certificate in the x5c chain is issued by a trusted Certificate Authority (CA). In the case of YubiKey, for example the "Yubico U2F Root CA Serial 457200631." This step confirms that the attestation statement comes from a genuine YubiKey device.
7.

By following this process, the on-chain contract can verify the authenticity of the YubiKey and the integrity of the attestation statement. This provides a transparent and tamper-proof record of the attestation, which can be publicly accessed and verified by anyone on the blockchain.

Previous Device Attestation Next Andriod Last updated4 hours ago On this page *Introduction of Yubikey * Yubikey Attestation

Was this helpful?