Proof of Machinehood

Extending silicon-level attestation to rollups Proof of Machinehood , orPoM is the key concept of Automata 2.0, bringing hardware-level attestation on-chain by equipping systems with immutable and inherent properties, as well as mutable and measurable computation. Visit the PoM demo running on ourtestnet for a hands-on experience.

?

Features

- Fully On-Chain Attestation:
- The entire attestation is fully verified on-chain to ensure that a genuine device is interacting with the blockchain. Many types of devices are supported via their own vendor-specific attestation protocol.
- Account Abstraction:
- Through the integration ofSafe
- , a device directly controls a smart contract account that can be used as an ephemeral and intermediate wallet that completes the attestation protocol, holding the attestation result as a non-transferrable NFT.
- Privacy Goes First:
- Each attestation creates an ephemeral keypair generated and stored secretly in the secure element of the device. All RPC requests are sent through1RPC
- , our privacy-protecting relay, to avoid metadata exposure of IP addresses and device fingerprint information.
- Seedless & Walletless:
- The PoM demo eliminates the need for a wallet extension or memorizing the seed phrase. This also allows a gas-free experience - fees for attestation are subsidized by the relayer.
-

Supported Devices

- Android SafetyNet
- Windows TPM
- YubiKey
-

ReadAttestation Statements & Privacy Impacts for more device-specific information

Workflow

1. Click the "Attest Your Device" button.
2. ?
3. The device employs a random salt to determine a Safe proxy address. This address serves dual purposes: as the abstract account; and the challenge during device attestation.
4. The device's attestation is invoked in compliance with theWebAuthn standard
5. . The following attestation options are utilized to generate in-device attestation requests:
6.

```

Copy authenticatorSelection: { attenticatorAttachment:"platform", userVerification:"preferred", residentKey:"preferred", }, attestation:"direct"

```

Specifically, while the YubiKey device employs a cross-platform authenticator's attachment, other devices utilize the platform input.

Using Apple MacBook as an illustration, the attestation process prompts users to employ TouchID for completion. Upon confirmation, the system returns an attestation object and client data JSON.

- Attestation object contains the attestation format, attestation statement, and authData. The attestation signatures, attested cert chain,authenticator
- , and generated credential public data are included.
- Client data JSON contains the attestation challenge, the origin initiating the attestation, and the attestation type. These elements undergo on-chain verification.
-

?

1. Once the device secures a successful WebAuthn response, it forwards the essential inputs to the relayer. This relayer activates theAuthModule

2. to deploy the Safe proxy, establishing an abstract account. Subsequently, this account triggers the on-chain device attestation verification function. This ensures the originating request is from a verified device and validates the challenge against the abstract account. Successful verification results in the minting of the attestation NFT for this abstract account.
3. Users can then inspect the attested details and the attestation NFT.
4.

?

References

- Android SafetyNet WebAuthn standard
- YubiKey WebAuthn standard
- TPM WebAuthn standard
- EIP4337
- Automata Testnet
-

Previous Stateless Executor Next Smart contract libraries Last updated25 days ago On this page *Features * Supported Devices * Workflow * References

Was this helpful?