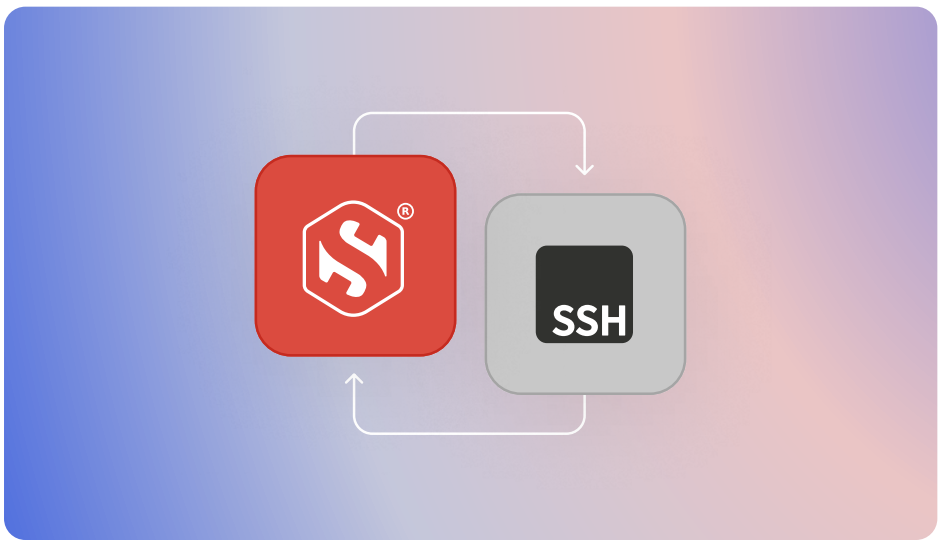
DATA SHEET

SSH Device Identity

Prevent untrusted device SSH access



Smallstep SSH Device Identity ensures that **only trusted, company-owned devices can access your critical infrastructure**.

This solution seamlessly integrates with SSH clients to manage hardware-bound SSH certificates, each containing a unique, hardware-attested identifier for the device.

This means you get significantly stronger security than traditional authentication methods, with hardware attestation and hardware-bound keys preventing sensitive key material from ever leaving the device.

By using SSH Device Identity, you can prevent unauthorized access from personal or untrusted devices, giving your developers and operators secure, controlled access while maintaining peak operational efficiency.

How it works

- **Attested Device Identity:** SSH certificates include a unique, permanent device identifier, verified via ACME Device Attestation.
- **Hardware-Bound Keys:** SSH certificate keys are secured within each device's **TPM or Secure Enclave.**
- **Automated Credential Management:** Eliminates manual pubkey distribution and SSO for SSH, making credential management invisible to users.
- **Shorter Certificate Lifetimes:** Automated management allows for very short-lived SSH certificates, significantly reducing risk exposure if a device is compromised.
- **Identity Provider Integration:** Add user principals to SSH certificates using existing company identity provider metadata.
- **Simplified Revocation:** Manage SSH Key Revocation Lists (KRLs) efficiently via the Smallstep platform.
- **Seamless Compatibility:** Works with existing OpenSSH, sshd, and popular tooling across platforms with minimal setup.
- **Smallstep SSH Pro Compatibility:** Advanced capabilities adding workflow, access control, and auditing features.

Coming Soon

Git and GitHub Protection
Secure sensitive codebases using Smallstep's compatible Git and GitHub integrations in the same manner as SSH hosts.

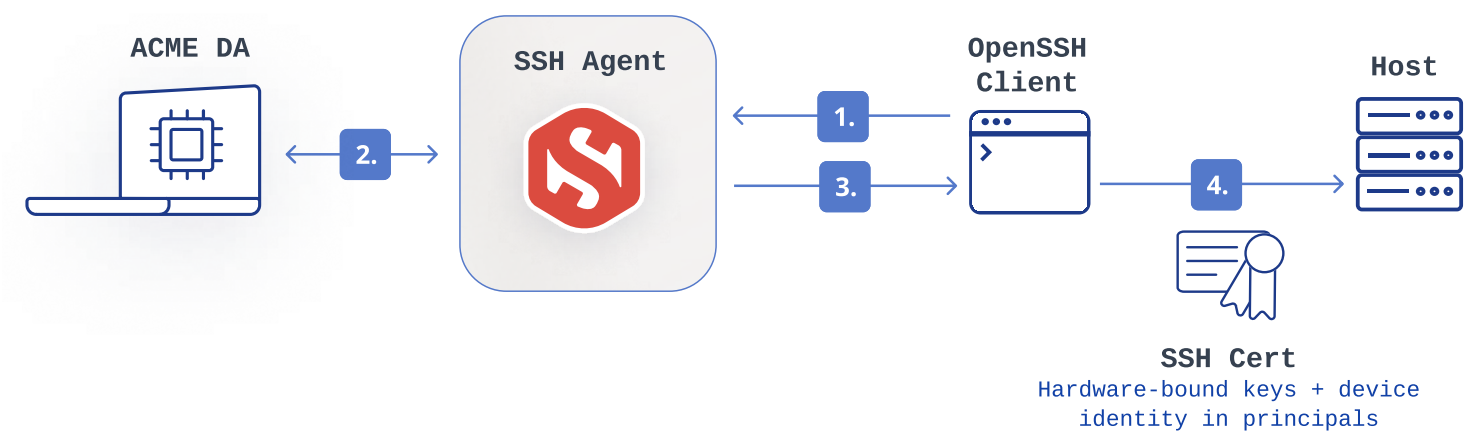
Under the hood

Smallstep employs a unique method to link a user's SSH certificate directly to their device's permanent hardware identifier. During certificate renewal, the Smallstep agent first obtains an X.509 certificate from the Smallstep CA using ACME Device Attestation.

The identifier within this X.509 certificate can only be signed by that specific device's hardware.

The agent then leverages this X.509 certificate to authenticate its request for an SSH certificate from the Smallstep CA, embedding the device's identifier in its principals.

Once issued, the Smallstep agent's integrated ssh-agent makes the new SSH certificate and its hardware-bound keys (secured in the device's TPM) readily available to all SSH clients.



"Adopting Smallstep SSH has enabled us to fully deprecate long-lived SSH key pairs in favor of a robust, short-lived certificate-based authentication model. By incorporating hardware-bound, device-attested keys, we have achieved a **dramatic elevation of our overall security posture while simultaneously streamlining engineer workflows**."

– Security Architect

Smallstep is the world's first Device Identity Platform™, enabling Zero Trust, certificate-based access to infrastructure, applications, and networks. Built in partnership with Apple and Google, Smallstep uses cryptographic attestation and short-lived, hardware-backed credentials to replace passwords, SSH keys, and VPN clients. By integrating with tools like Jamf, Intune, and Okta, Smallstep ensures that only trusted users on compliant devices can access sensitive systems—delivering true Zero Trust security without user friction.

smallstep

“**Smallstep let us eliminate long-lived SSH keys and move to short-lived certificates** tied directly to our IdP, which immediately tightened our security posture. It offered us strong authentication without the overhead of a full access-plane product we’d never fully use.”

– Director of DevOps