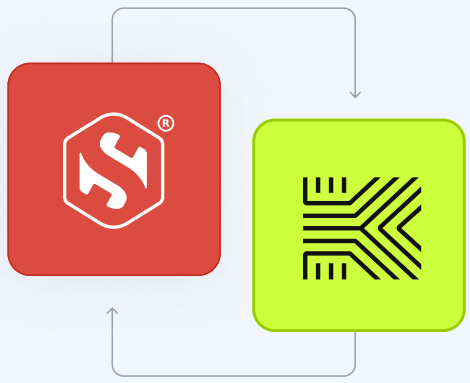
DATA SHEET

# Keycard + Smallstep

## Secure access to Agentic AI



AI agents are powering autonomous systems that execute complex, multi-step workflows across organizations. Developers increasingly rely on Agentic AI to accelerate software delivery, but security teams must ensure these tools only access sensitive resources under strict identity and trust controls.

By combining **Keycard's policy-driven OAuth authorization** with **Smallstep's ACME-based device attestation**, organizations can enable secure, frictionless agent workflows for developers and other internal users without sacrificing compliance or risk posture.

## Key Features

**Strong, Multi-Layered Identity**
Enable the development and integration of AI Agents and MCP Servers without sacrificing security.

**Multi-OS support**
Extend trust to developers across macOS, Windows, Linux, iOS, Android, and ChromeOS environments.

**ACME Device Attestation**
Smallstep co-developed the standard for high-assurance device identity with Google at the IETF. ACME DA prevents credential exfiltration, phishing, and impersonation attacks.

**Frictionless for Users**
Let developers use AI agents that can safely access source code, internal APIs, and data platforms (e.g., Snowflake, Google, GitHub) without extra logins or manual approvals.

**Seamless Integration**
Automation-first certificate issuance with integrations with Intune, Jamf, AWS IAM, and modern CI/CD pipelines.

**Backward compatibility**
Support for legacy systems (e.g., SCEP, ADCS, AD-joined servers).

**Scale & Reliability**
Globally distributed teams, enterprise support, and consultative engagement with each security team.

Keycard

When **Smallstep** is added to **Keycard**, you get a single control plane that combines OAuth-based policies with hardware-backed device identity, so only trusted agents on compliant devices can access sensitive resources.

## Keycard is even better with Smallstep

Enable the development and integration of AI Agents and MCP Servers with strong, multi-layered identity—without sacrificing security. Ensure only authorized users on verified devices can leverage these tools—preventing AI misuse or data exfiltration.

### Keycard

Keycard provides fine-grained, access control and policy enforcement for agent interactions via agent protocols like MCP and A2A, integrated with OIDC-compatible IdPs like Okta and Entra ID, for internal & external services and SaaS via drop-in SDKs.

### smallstep

Smallstep strengthens your access controls by ensureing that only trusted components can access sensitive resources by identifying Devices, Agents, and MCP Servers using hardware-attested, non-exfiltratable credentials.

**With Keycard and Smallstep you can combine user identity with device attestation to get agent identity for *every* request.**

### Ecosystem interoperability

Extend trust to developers across macOS, Windows, Linux, iOS, Android, and ChromeOS environments. With backward compatibility, you can leverage the same solution to support for legacy systems (e.g., SCEP, ADCS, AD-joined servers).

### Seamless integration

Together, Keycard and Smallstep form one integrated solution that spans identity, device security, and authorization. Smallstep's industry-leading PKI and attestation, paired with Keycard's OAuth-based developer access, raise security standards without adding friction for developers.

**Turn your team into an AI powerhouse**

Ship safe, powerful, production-ready agents today.

**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