smallstep

Device Identity in 2025

A Practical Guide on the State of the Device Identity Ecosystem

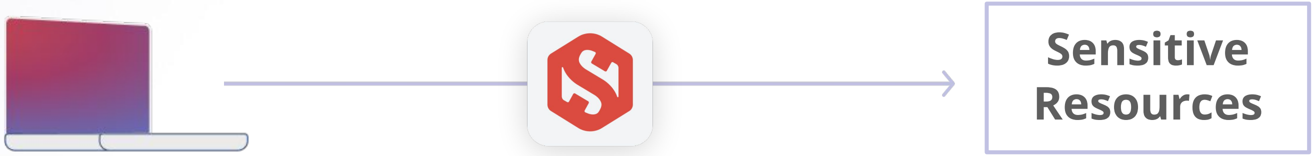
June 18th, 2025

Hi, I’m Mike from Smallstep

- CEO / Founder of Smallstep
- Software Engineer. Kinda into large distributed systems.
- Open source & standards.

sigstore OpenSSF OPEN SOURCE SECURITY FOUNDATION MASQUE OpenID spiffe OAUTH

The World’s First Device Identity Platform



Device Identity

Ensure that only ***trusted devices*** can access sensitive resources.

smallstep

Device Identity is Half of Zero Trust

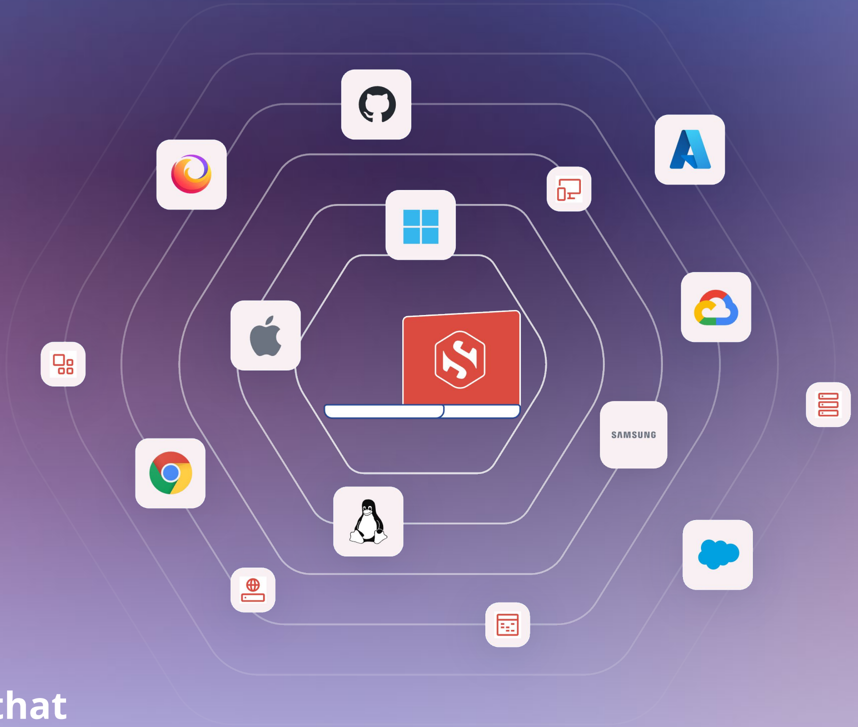
- Ensure employees do work on their work computers
- Invisible protection against phishing and other credential compromise
- Numerous operational & UX benefits

Device Identity is a Mess

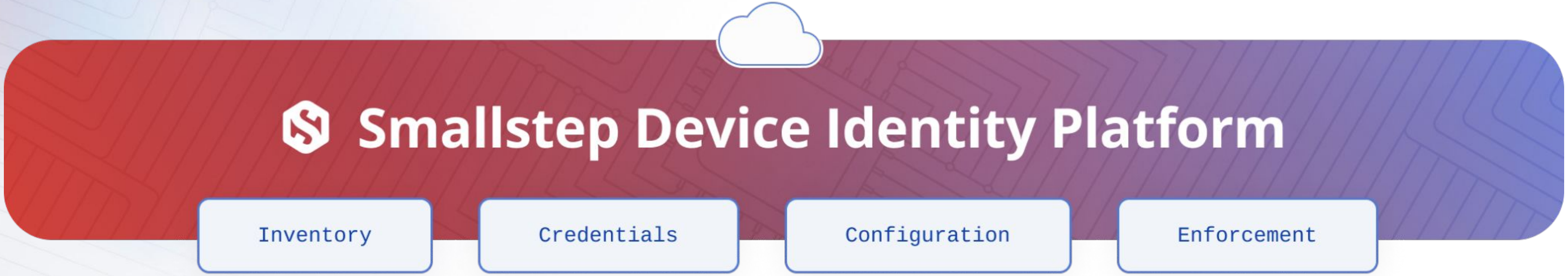
- **Operating Systems**
  Windows, Mac, Linux, Chrome OS, iOS, Android
- **Browsers**
  Chrome, Edge, Safari, Firefox, Island, ...
- **Enforcement Points**
  ZScaler, WARP, Okta, Entra ID, RADIUS, ...
- **Resources**
  SaaS apps, WiFi, SSH, Git, Cloud APIs, ...

Consistent enterprise-wide enforcement is *hard*.

Most organizations end up making compromises that impact security and user experience. This results in expensive solutions that nobody likes.



A Framework



Smallstep Device Identity Platform

Inventory

Credentials

Configuration

Enforcement

Enforcement Strategies

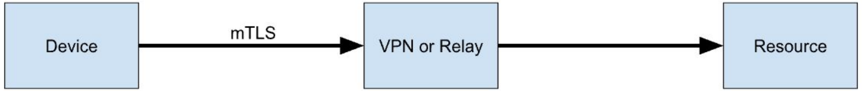
You'll want all three and therefore want a consistent **device identity fabric** that works across enforcement points.

Certificates are the right foundation. Supported by:

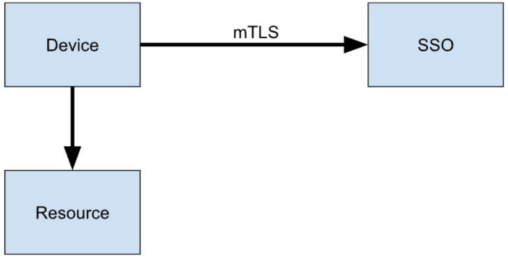
- Basically all ZTNA/VPNs
- WiFi (EAP-TLS)
- IdPs (Okta, Entra ID, Google)
- SSH & Github (SSH Certs)
- Clouds (AWS, Azure, GCP)

Biggest Gap: most SaaS apps don't support mTLS. Use SSO or ZTNA + IP Allow List for now 💩

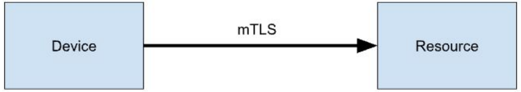
Middlebox (VPN / ZTNA + IP Allow List)



Single sign-on (delegated)



Resource Configuration (e.g., mTLS)



Self-reported Device Identity (Please Stop)

A surprisingly common (anti-)pattern

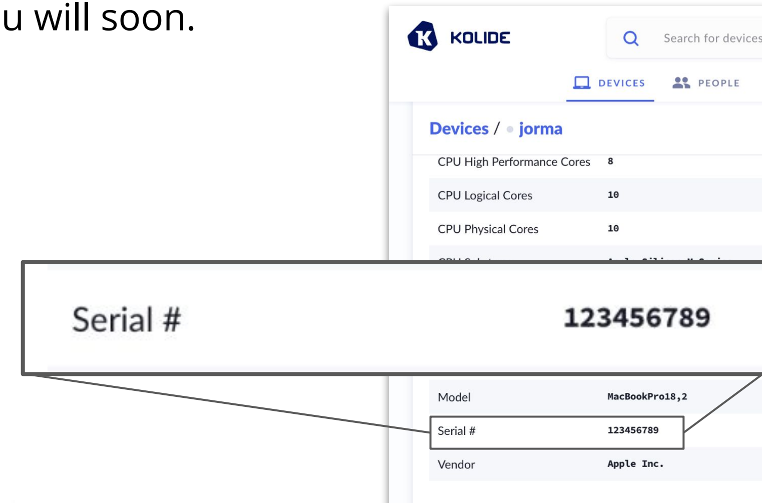
- Agent calls an API to get serial number, used for “authentication”
- It’s a username without a password

Related anti-pattern: Misuse of Device Health (e.g., Kolide, Crowdstrike) for Device Identity. No shade, they’re great, they just don’t do device identity.

Trivial to bypass. If you’re not seeing compromises already, you will soon.

Chrome Endpoint Verification bypass:
https://www.youtube.com/watch?v=BJkBAtCJhhs

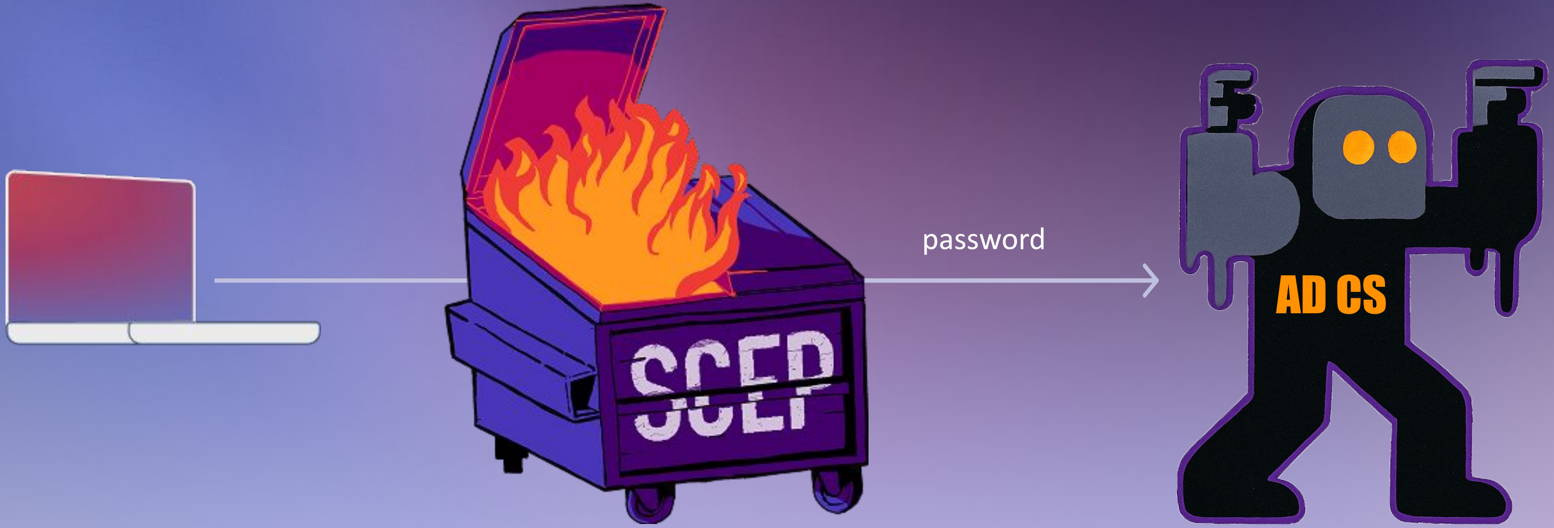
Project Indago - Impersonating Devices at MDM Enrollment
https://github.com/ripeda/Indago



Devices / jorma

CPU High Performance Cores	8
CPU Logical Cores	10
CPU Physical Cores	10
Serial #	123456789
Model	MacBookPro18,2
Serial #	123456789
Vendor	Apple Inc.

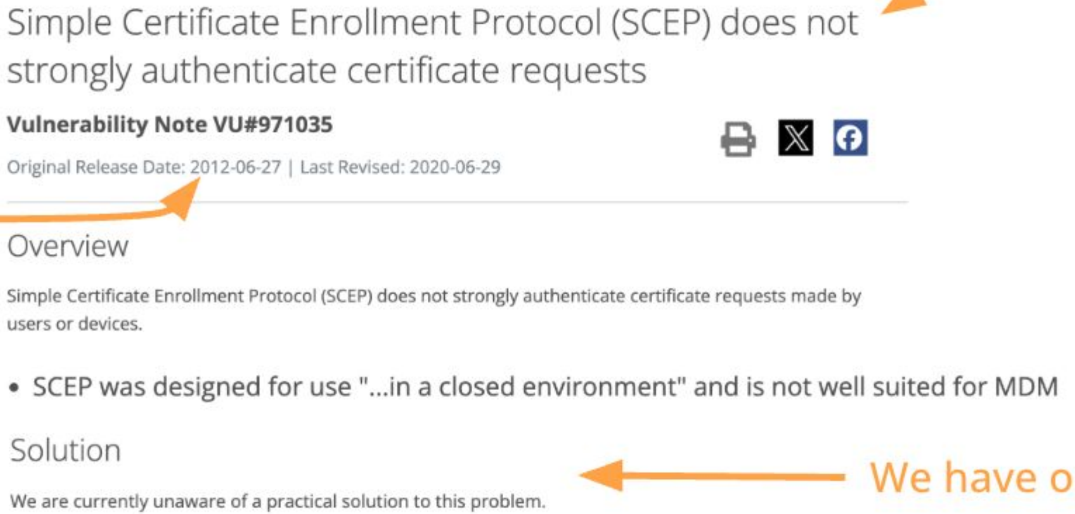
SCEP is a dumpster fire



password

We've known SCEP is broken for at least 13 years

Lol, yep.



Simple Certificate Enrollment Protocol (SCEP) does not strongly authenticate certificate requests

Vulnerability Note VU#971035

Original Release Date: 2012-06-27 | Last Revised: 2020-06-29

Overview

Simple Certificate Enrollment Protocol (SCEP) does not strongly authenticate certificate requests made by users or devices.

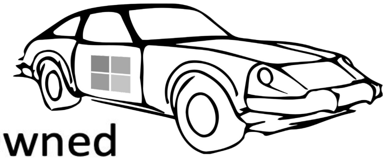
- SCEP was designed for use "...in a closed environment" and is not well suited for MDM

Solution

We are currently unaware of a practical solution to this problem.

OMG,
SERIOUSLY?
2012!?

We have one



140 page report on all the ways to own AD CS

Certified Pre-Owned

Abusing Active Directory Certificate Services

https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf

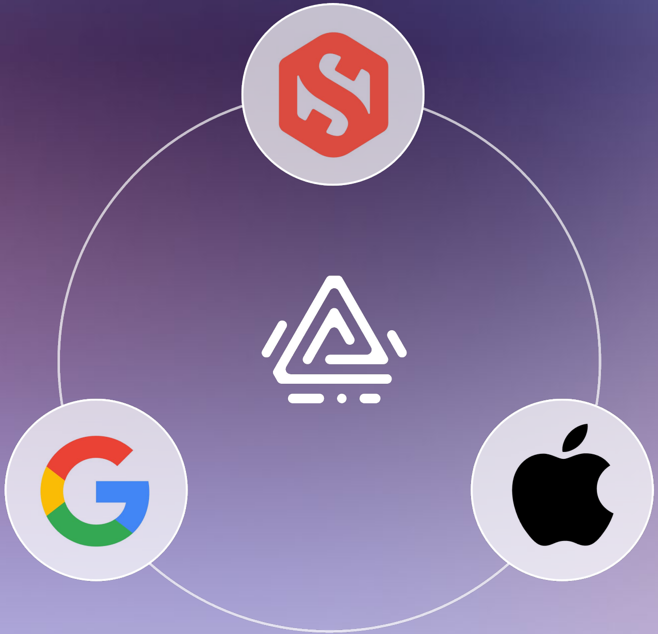
Use ACME Device Attestation

IETF Standard developed by Google & Smallstep

- Apple called it “Managed Device Attestation”
- Hardware-attested & hardware-bound certificates
- Works on all mobile and laptop operating systems
- Some limitations on macOS, but “Apple is aware”

Key Resources

- https://datatracker.ietf.org/doc/draft-acme-device-attest/
- https://smallstep.com/blog/managed-device-attestation/
- https://support.apple.com/guide/deployment/managed-device-attestation-dep28afbde6a/web
- https://jedda.me/managed-device-attestation-a-technical-exploration/

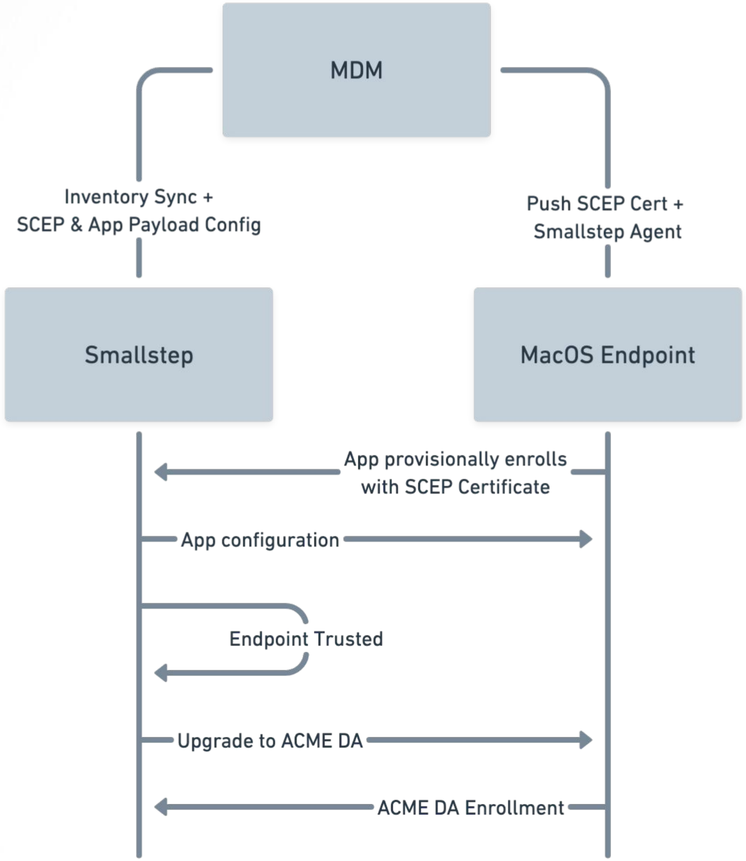


Agent-based ACME DA

Smallstep supports agent-based ACME DA **now**

- MDM-deployed headless agent & SCEP payload
- Trusted endpoints upgrade to ACME DA
- Certificates can be used by any application
- Agent automates certificate renewal

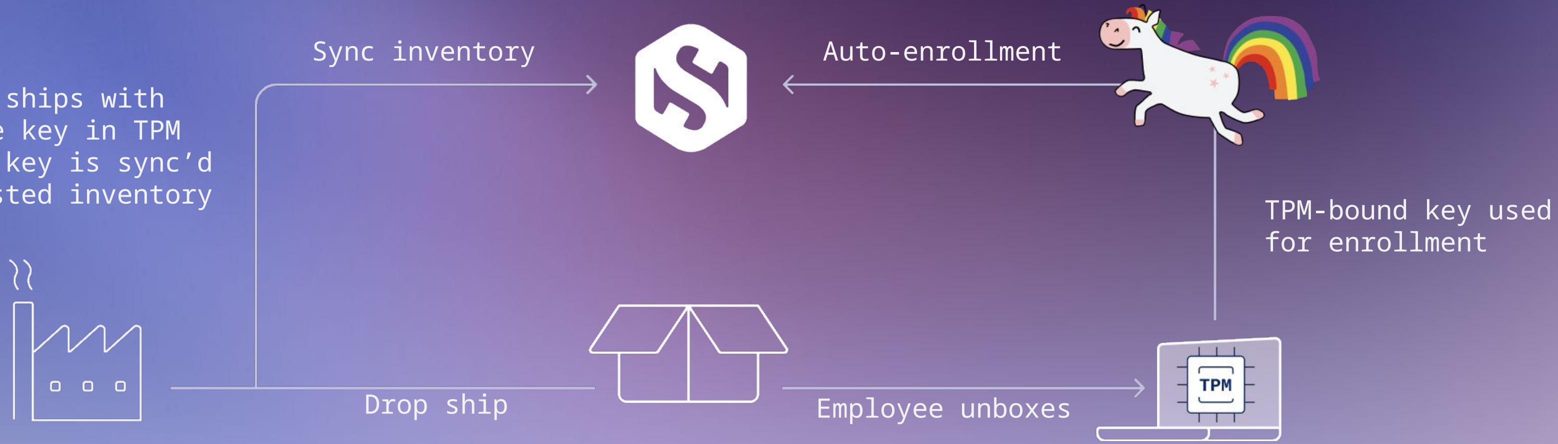
Works on MacOS*, Windows, Chrome OS, and Linux.



* Agent-based ACME DA on MacOS is not as robust as native ACME DA but much better than SCEP.

Trusted Inventory + Zero Touch Enrollment

- Device ships with private key in TPM
- Public key is sync'd to trusted inventory



Sync inventory

Auto-enrollment

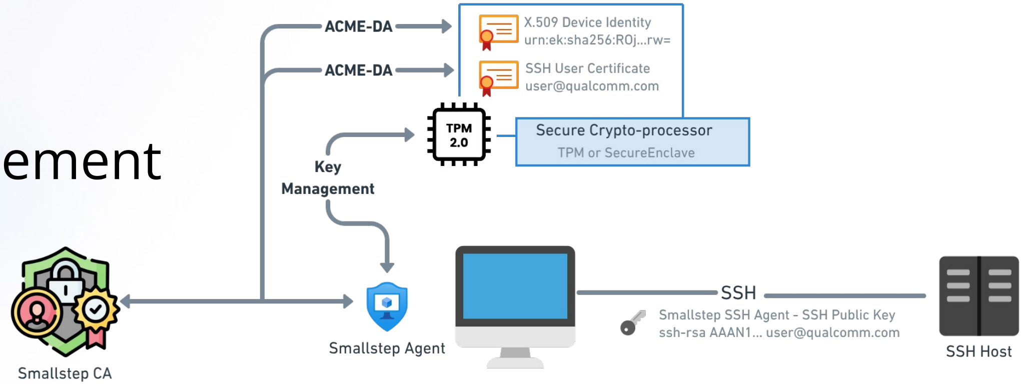
TPM-bound key used for enrollment

Drop ship

Employee unboxes

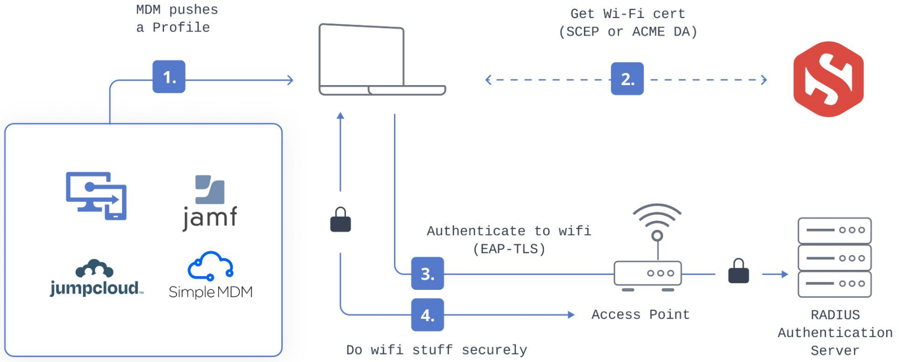
SSH / Git

- SSH Certificate Workflow
- Bastion and/or Host Enforcement
- SSH Agent
- Client Configuration



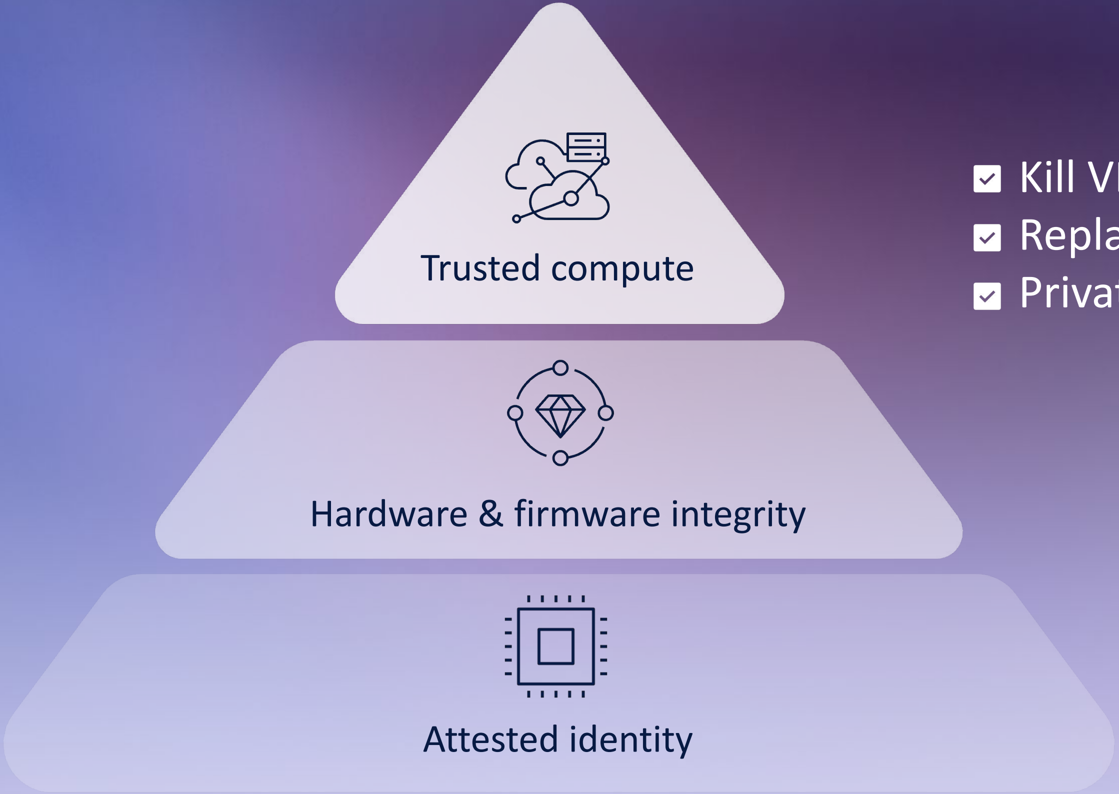
WiFi

- X.509 Certificate Workflow
- RADIUS / 802.1x Enforcement
- MDM Integration
- EAP-TLS Client Config (e.g., on Linux)



The Future ✨

- ☑ Enterprise IT
- ☑ Cloud
- ☑ Agentic AI



Trusted compute

Hardware & firmware integrity

Attested identity

- ☑ Kill VDI
- ☑ Replace secrets
- ☑ Private LLM Chat

Summary

- Device Identity is invisible security that can stop phishing without MFA fatigue, prevent insider threats, and even save you money on shipping.
- But, it’s really hard and kind of a mess
    - Many permutations of (OS, Client, Enforcement Point, Resource) to consider
    - Requires inventory, credentials, configuration, and enforcement
- Certificates are the right identity fabric.
    - Don’t use self-reported device identity
    - Start migrating from SCEP to ACME DA as soon as you can
- The future is bright. We’re working with everyone in this ecosystem to make Device Identity easier. Hit me up if you have ideas or want to help.

If you have questions or want to learn more about Smallstep, I’m **mike@smallstep.com**.

Questions?

smallstep