



Apple Device Attestation

Hardware-backed certificate enrollment for Apple devices

The challenge

Modern enterprises increasingly rely on device certificates to secure access to Wi-Fi, VPNs, applications, Zero Trust networks, and enterprise resources. However, traditional certificate enrollment methods often rely on shared secrets or enrollment passwords that can be copied, replayed, or used by unauthorized devices.

As organizations expand Apple device fleets and adopt Zero Trust architectures, they need stronger assurance that certificates are issued only to trusted hardware, not simply to devices that possess a credential.

At the same time, shorter certificate lifecycles, automated certificate management, and evolving security standards require that organizations modernize device enrollment without increasing operational complexity.

Traditional enrollment methods are no longer enough.

The solution

DigiCert® Trust Lifecycle Manager now supports ACME Device Attestation for Apple devices, enabling standards-based, zero-touch certificate enrollment using hardware-backed device identity.

Using the emerging device-attest-01 ACME challenge, Trust Lifecycle Manager validates Apple device attestation before requesting certificate issuance from DigiCert® ONE Private CA. The result is automated certificate enrollment that verifies certificates are issued only to genuine Apple hardware.

Combined with DigiCert's existing Jamf integration, organizations can automate certificate enrollment, renewal, and lifecycle management across managed Apple devices while strengthening Zero Trust and device identity assurance.

This enables:

- Hardware-backed device identity verification
- Zero-touch certificate enrollment
- Standards-based ACME workflows
- Automated certificate lifecycle management
- Stronger Zero Trust device authentication
- Reduced risk of unauthorized certificate enrollment

How it works



Attest

The Apple device generates a hardware-backed attestation proving its identity using Apple's secure attestation service.



Validate

Trust Lifecycle Manager validates the device-attest-01 challenge before requesting certificate issuance from DigiCert ONE Private CA.



Issue

Certificates are automatically issued using DigiCert ONE Private CA based on verified device identity.



Enroll

Using the existing Jamf integration and ACME enrollment profile, managed Apple devices receive certificates automatically without manual intervention.



Manage

Trust Lifecycle Manager automates certificate renewal, lifecycle management, monitoring, and policy enforcement throughout the device lifecycle.

Value

Key feature	Description	Business value
ACME Device Attestation	Validates hardware-backed Apple device identity before certificate issuance	Prevents unauthorized certificate enrollment
DigiCert ONE Private CA	Issues certificates only after successful device attestation	Improves trust and certificate integrity
Jamf integration	Automates enrollment across managed Apple devices	Simplifies large-scale deployment
Zero-touch enrollment	Eliminates manual provisioning and shared secrets	Reduces administrative overhead
Certificate lifecycle automation	Automates issuance, renewal, and policy enforcement	Improves operational resilience
Zero Trust device identity	Hardware-backed authentication for enterprise devices	Strengthens access security and compliance

Why DigiCert

Device identity begins before a certificate is issued.

DigiCert Trust Lifecycle Manager combines hardware-backed device attestation, automated certificate lifecycle management, and enterprise Private PKI to ensure certificates are issued only to trusted Apple devices. By integrating ACME Device Attestation with Jamf and DigiCert ONE Private CA, organizations can modernize Apple device enrollment, eliminate shared-secret enrollment methods, and strengthen Zero Trust security with standards-based automation.

As certificate lifecycles shrink and machine identities continue to grow, DigiCert helps organizations automate device trust from enrollment through renewal, creating a scalable, crypto-agile foundation for modern enterprise identity.

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management to secure infrastructure, software, devices, messages, and AI content, agents, and models. Learn why more than 125,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com.

© 2026 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.