digicert

DIGICERT DEVICE TRUST MANAGER

Complete IoT Security, Across The Entire Lifecycle

Security from Birth to Decomission

DigiCert Device Trust Manager enhances IoT device security throughout their lifecycle, from initial design to decommissioning, ensuring they meet stringent global security standards. This comprehensive approach not only boosts operational efficiency but also underpins privacy, consumer safety, and business continuity.

Unique Device, Unique Security

At the core of its functionality, Device Trust Manager equips each device with a hardware-backed identity right from the manufacturing stage, establishing a robust root of trust. This foundational security is vital for maintaining device integrity and trust from the outset. As devices navigate through various environments, Device Trust Manager adeptly manages their security credentials and settings, addressing potential network attacks, misconfigurations, and malware threats. It also lays the groundwork for crypto-agility, preparing devices for future security challenges, including the transition to post-quantum cryptography.

Deployment that Meets Requirements

Device Trust Manager supports diverse deployment scenarios, from on-premises to the public cloud, integrating seamlessly with existing systems to ensure that security measures scale effectively with device deployment. By deploying Device Trust Manager, companies can effectively safeguard their IoT devices, ensure compliance, minimize the risk of security breaches, and maintain a strong market presence, all while reinforcing customer trust in the brand's commitment to comprehensive device security.

Compliance, Efficiency, and Scalability

Enhanced Compliance and Risk Management:
Streamlines adherence to global regulations and reduces risks by supporting detailed SBOMs and minimizing the impact of security incidents.

Operational Efficiency and Market Responsiveness:
Automates security processes to reduce manual effort, boosting productivity and speeding up time-to-market with advanced features like zero-touch provisioning.

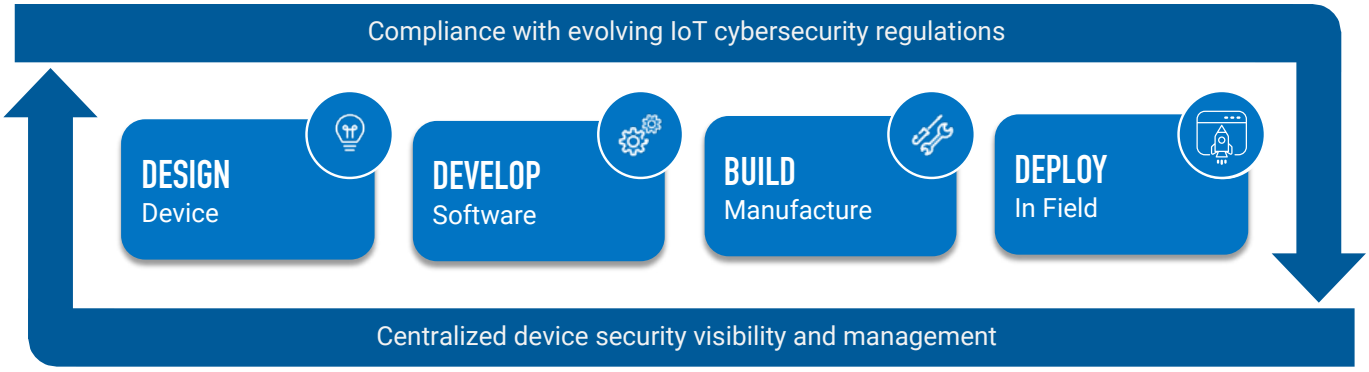
Scalable and Versatile Security Solutions:
Adapts and scales to fit various device ecosystems, providing consistent and comprehensive security across all deployment sizes and types.

Brand Protection and Innovation Enablement:
Strengthens customer trust and loyalty through robust security measures, while freeing resources to focus on innovation and readiness for emerging technologies.

Working Together to Secure Devices

Device Trust Manager seamlessly integrates with Software Trust Manager, offering an expanded suite of products for comprehensive device and software security. This partnership enhances protection against vulnerabilities through advanced software scanning, digital signing, and the generation of Software Bills of Materials (SBOMs).

Device Trust Manager Framework



Features and Technological Innovations

Design Phase

- Crypto-Agility & Compliance: Ensures that device security architecture can adapt to new cryptographic standards quickly, facilitating compliance with evolving security protocols.
- Secure Hardware Integration: Integrates security features at the hardware level during the design phase, establishing a device's trustworthiness and identity.

Develop Phase

- Crypto-Agility & Compliance: Ensures that device security architecture can adapt to new cryptographic standards quickly, facilitating compliance with evolving security protocols.
- Secure Hardware Integration: Integrates security features at the hardware level during the design phase, establishing a device's trustworthiness and identity.

Build Phase

- Hardware-Backed Identities: Establishes secure, unique identities for each device with a hardware root of trust. This fundamental security layer authenticates each device's origin and protects against counterfeit intrusion, serving as the foundation for all subsequent security measures throughout the device's lifecycle..
- Certificate Distribution & Management: Manages the secure distribution and management of digital certificates essential for device identity and secure communications.

Deploy Phase

- Continuous Threat Monitoring: Enhances security with device audit logging and alerting, integrating seamlessly with SIEM tools for efficient threat detection and management. SBOM monitoring provides notifications of vulnerabilities in device software.
- Secure Software Updates: Offers a turnkey solution for deploying updates across devices, enhancing security and compliance, reducing development costs, and speeding time-to-market without compromising on device integrity.
- Zero Touch Provisioning: Enables devices to be securely configured and activated with minimal human intervention, reducing the risk of human error and increasing the efficiency of device deployment.

To learn more or schedule a demo of DigiCert® Device Trust Manager please email sales@digicert.com.

About DigiCert, Inc.
DigiCert is the world's leading provider of digital trust, enabling individuals and businesses to engage online with the confidence that their footprint in the digital world is secure. DigiCert® ONE, the platform for digital trust, provides organizations with centralized visibility and control over a broad range of public and private trust needs, securing websites, enterprise access and communication, software, identity, content and devices. DigiCert pairs its award-winning software with its industry leadership in standards, support and operations, and is the digital trust provider of choice for leading companies around the world. For more information, visit digicert.com or follow @digicert.

© 2024 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.