digicert®

DigiCert® Device Trust Manager Case Study

CASE STUDY

Scaling Patient Safety and Manufacturing Security with DigiCert® Device Trust Manager

Executive Summary

Industry: Medical Devices / Digital Health
Headquarters: United States

Key business requirements:

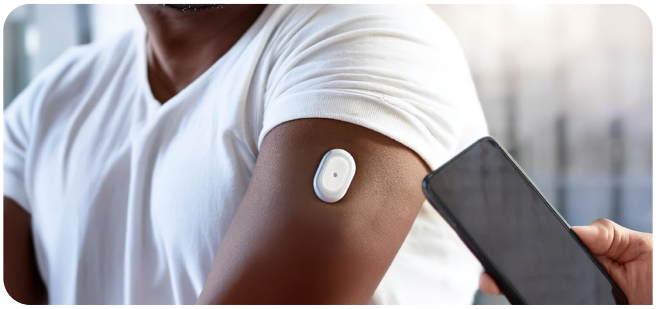
- Automate PKI and certificate lifecycle management for millions of devices
- Ensure compliance with FDA, HIPAA, and global medical device regulations
- Eliminate production downtime tied to certificate issuance or rotation
- Reduce operational overhead tied to managing internal PKI infrastructure
- Support real-time device authentication across global manufacturing plants

Solution:

- DigiCert® Device Trust Manager

Key outcomes:

- System maintained issuance of hundreds of certificates per second to meet production demand
- Automated platform handled provisioning, renewal, and revocation of device credentials
- Teams gained real-time compliance visibility and were always prepared for audits
- Cloud-based service eliminated the need for internal HSMs and on-prem PKI infrastructure



Requirement

Scaling Security for Life-Critical Devices

Continuous Glucose Monitoring (CGM) devices provide real-time glucose readings to millions of people, improving diabetes outcomes and enabling continuous, connected care. As adoption expanded globally—and integrations with mobile apps, insulin pumps, and cloud platforms grew more sophisticated—the company faced the challenge of securing a massive, decentralized device estate.

Every CGM device needed a unique, verifiable identity that could be authenticated from the moment it left the factory floor to the moment it connected with a patient or healthcare system. Device security had always been critical, but the scale, speed, and expectations of modern connected care had outgrown existing PKI processes.

Traditional certificate workflows involved manual steps, brittle integrations, and homegrown tools for issuing and tracking device credentials. Manufacturing tens of millions of devices annually was pushing this system to its limits. Any delay in certificate issuance risked production bottlenecks and delayed device delivery to patients.

Meanwhile, regulatory scrutiny was intensifying. In addition to FDA, HIPAA, and ISO 13485 requirements, new cybersecurity mandates—such as software bills of materials (SBOMs), cryptographic agility, and secure device identity at birth—demanded a more robust, automated approach. The risk was real: a failed audit, certificate outage, or device rejection could undermine trust with patients.

Finally, internal PKI operations were becoming costly and time-consuming. Security engineers spent significant effort troubleshooting expired certificates and authentication issues instead of advancing proactive security initiatives.

The device manufacturer needed to eliminate manual processes, reduce points of failure, and implement a high-speed, globally scalable device identity pipeline—one that could ensure continuous compliance and support the company's growth in a highly regulated, life-critical market.

Solution

Device Trust Manager Delivers Scalable Device Identity and Continuous Compliance for Global Medical Manufacturing

Device Trust Manager was selected to serve as the backbone for secure device provisioning and lifecycle management. The solution offered cloud-native certificate issuance with automated enrollment, rotation, and revocation services, integrated directly into global manufacturing workflows. Critically, DigiCert demonstrated the ability to sustain hundreds of certificate operations per second in live environments, a requirement to match current production velocity and projected growth.

The platform also offered:

- **Resilient OCSP and CRL services** that supported real-time authentication in production and field environments
- **No required on-premises infrastructure**, eliminating the need for hardware security modules or dedicated certificate management servers
- **Regulatory alignment**, with built-in capabilities to support FDA, HIPAA, and international device security mandates
- **24/7 expert support and strict SLAs**, ensuring uninterrupted operations and immediate response if anomalies were detected

The integration process was guided by a joint deployment team from both the device maker and DigiCert, which collaborated to embed Device Trust Manager into manufacturing processes across multiple regions and device platforms.

Outcome

Enabling high-speed device identity to support global production demands

Device Trust Manager transformed the way the customer managed device identities across their global manufacturing lines. Certificate issuance now occurs in near real-time—hundreds of certificates per second—enabling simultaneous production in the U.S., Asia, and Europe without bottlenecks or manual intervention. Devices leave the factory floor fully provisioned with unique, verifiable identities that ensure authenticity from day one.

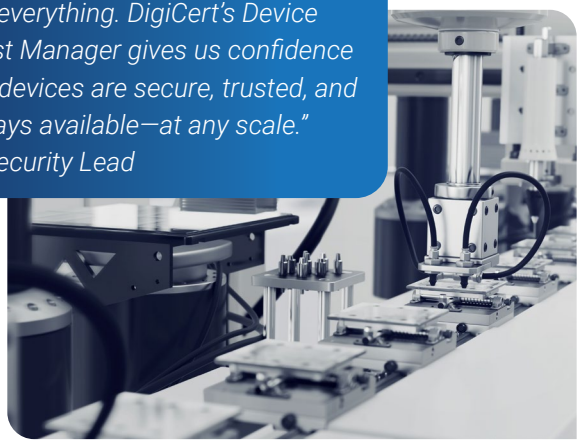
This high-speed identity framework directly supports their commitment to patient safety and product reliability. As one security leader explained, ***"Patient safety and product integrity are everything. Device Trust Manager gives us confidence our devices are secure, trusted, and always available—at any scale."***

Improving compliance readiness with automated credential management

Operating in a highly regulated medical device environment, adherence to FDA, HIPAA, and ISO 13485 standards is required, as well as emerging cybersecurity requirements such as SBOM tracking, cryptographic agility, and secure device identity at birth. By integrating Device Trust Manager into their manufacturing processes, automated certificate provisioning, renewal, and revocation were achieved—ensuring every device meets strict regulatory expectations without manual oversight.

Automated compliance has eliminated audit gaps and significantly reduced the risk of production delays or market interruptions. Every device is now born into a zero trust architecture, enabling demonstration of full lifecycle control during any inspection or regulatory review.

"Patient safety and product integrity are everything. DigiCert's Device Trust Manager gives us confidence our devices are secure, trusted, and always available—at any scale."
— Security Lead



Reducing operational overhead by offloading PKI infrastructure management

Previously, internal PKI operations required substantial engineering effort to manage certificate expirations, maintain on-premises HSMs, and troubleshoot device authentication issues. Offloading certificate lifecycle management to Device Trust Manager removed these operational burdens, delivering continuous uptime for certificate-related operations and freeing engineers to focus on proactive security initiatives.

The shift from homegrown infrastructure to an automated, cloud-based platform has reduced costs and simplified security operations. By removing points of failure and streamlining device identity management, the company has created a scalable foundation for future growth—without expanding their internal PKI team or infrastructure footprint.

Conclusion

Leading the Way in Secure Device Manufacturing at Scale

The customer fundamentally changed how they manage device security across their global manufacturing operations. By automating certificate issuance and offloading PKI infrastructure, the company can maintain continuous production without bottlenecks or manual intervention. Devices now leave the factory fully authenticated, compliant with regulatory requirements, and ready for patient use.

This approach has eliminated fragile, in-house PKI systems and the operational risks they carried. Engineering teams no longer devote time to certificate management or troubleshooting, instead focusing on developing new features and advancing the next generation of connected medical devices. With this secure, high-speed identity framework in place, this creates a scalable foundation for growth that ensures devices remain trusted from manufacturing through their entire lifecycle.

Enabling Innovation with Secure, Scalable Manufacturing

With automated device identity and lifecycle management in place, the customer is positioned to expand its connected medical device portfolio with confidence. The new security framework ensures that as production volumes increase and regulatory requirements evolve, every device will leave the factory authenticated, compliant, and ready for patient use.

By eliminating manual PKI processes and operational bottlenecks, Device Trust Manager has created a foundation for innovation—allowing engineering and security teams to focus on advancing the next generation of life-critical devices rather than managing certificate infrastructure. This proactive approach to manufacturing security ensures continued delivery of trusted solutions to patients worldwide, even as connected care continues to grow in scale and complexity.

Get started today with DigiCert® Device Trust Manager by contacting sales@digicert.com.