SOLUTION BROCHURE

Secure Manufacturing From Factory to Field With Cryptographic Trust

ENTRUST

SECURING A WORLD IN MOTION

Build Once. Ship Everywhere. Trust for Decades.

OVERVIEW

Today's manufacturers aren't just shipping products – they're shipping connected, software-defined systems expected to operate securely for years, often decades. From industrial equipment and medical devices to automotive systems and consumer electronics, trust is no longer established at deployment – it must be embedded from the very beginning. This shift introduces a new requirement: **Cryptographic trust must span the entire device lifecycle, from factory provisioning to long-term operation in the field.**

The Challenge: A New Class of Manufacturing Risk

As devices become more connected, distributed, and long-lived, manufacturers face a growing set of cryptographic and operational challenges:

Trust Breakdown at Manufacturing

Device keys and identities are created during manufacturing – often across global factories and third-party partners.

If keys are exposed, reused, or mishandled, entire product lines can be compromised before devices ever leave the factory.

Software and Firmware Integrity Risk

Without strong signing and verification processes, attackers can tamper with firmware or deliver malicious OTA updates – enabling remote control or persistent compromise across entire fleets.

Long-Lived Devices, Shorter Cryptographic Lifecycles

Devices often remain in service for 10–40 years, while cryptographic standards continue to evolve.

The rise of post-quantum cryptography (PQC) introduces new urgency; today's encryption may not withstand tomorrow's threats.

Operational Complexity at Scale

Manufacturers must securely manage millions of device identities, certificates, and keys across environments – often with limited visibility, fragmented tools, and manual processes that don't scale.

Why It Matters

A single weakness in device identity, key protection, or firmware integrity can be exploited at scale, turning isolated vulnerabilities into fleet-wide compromise.

The business impact is significant:

- Revenue loss from counterfeit or cloned devices
- Safety and regulatory risk from tampered firmware or unauthorized updates
- Operational disruption due to expired or unmanaged certificates
- Long-term reputational damage from compromised products

And critically – if cryptographic keys are exposed during manufacturing, the "keys to the kingdom" are in the wild. That's not something you can fix after deployment.

The Entrust Approach: Factory-to-Field Cryptographic Trust

Entrust helps manufacturers embed and maintain trust across the entire device lifecycle – combining hardware-rooted security with centralized governance and automation.

With the Entrust Cryptographic Security Platform, organizations gain unified visibility and control over keys, certificates, and secrets – enabling secure provisioning, trusted software delivery, and long-term crypto-agility.

1. Establish Device Identity at Scale

Every device is issued a unique, cryptographically verifiable identity at manufacturing – often as a long-life "birth certificate."

- Prevent cloning and counterfeit devices
- Enable secure authentication (mTLS) across systems
- Support trusted communication and access control

2. Protect Keys and Secure Provisioning

Cryptographic keys are generated, stored, and used inside tamper-resistant hardware – ensuring zero key leakage during manufacturing.

- Secure key generation and injection on the production line
- Protection from insider and third-party risk
- Consistent, repeatable provisioning across global factories

3. Ensure Firmware Integrity and Trusted Updates

Only authorized software is allowed to run on devices - protecting against tampering and unauthorized updates.

- Secure code signing within protected hardware boundaries
- Verified firmware and OTA updates
- Protection against malicious or modified code

4. Govern Lifecycle and Enable Crypto-Agility

Centralized lifecycle management ensures devices remain secure over time – even as cryptographic standards evolve.

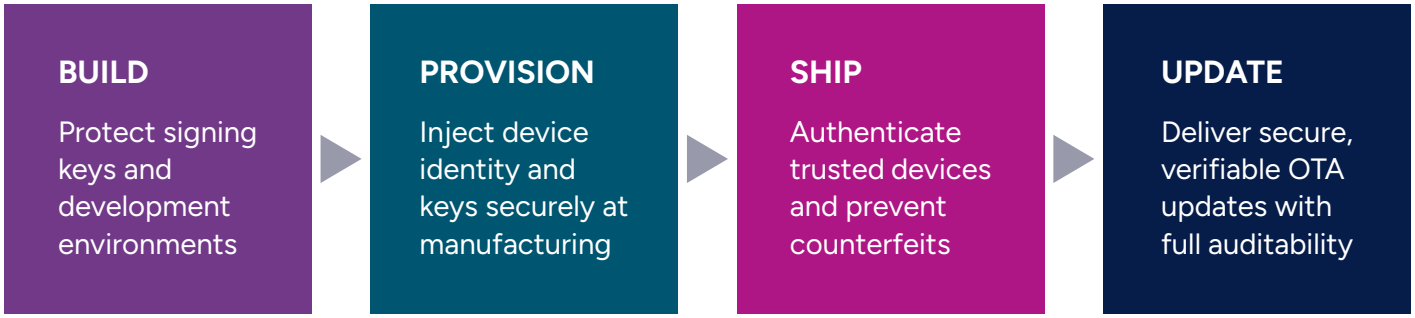
- Automated certificate issuance, renewal, and revocation
- Full visibility into cryptographic assets across device fleets
- Support for post-quantum cryptography (PQC) and future algorithm transitions

Did you know?

Devices often remain in service for 10-40 years – far longer than the lifespan of most cryptographic standards.

Secure the Entire Device Lifecycle

Entrust enables a secure, scalable trust model across every stage of manufacturing and deployment:



When trust is established early and governed centrally, **one vulnerability no longer exposes an entire fleet.**

Business Outcomes

With Entrust, manufacturers can:

- **Reduce operational complexity** with centralized lifecycle management and automation
- **Prevent large-scale device compromise** through hardware-rooted trust and strong identity
- **Help ensure compliance and audit readiness** with full visibility and governance
- **Future-proof long-lived devices** with built-in crypto-agility and post-quantum readiness

Why Entrust

Entrust brings decades of leadership in cryptographic security to the manufacturing industry:

- Proven expertise in PKI, HSMs, and lifecycle management
- Hardware-rooted trust for the highest level of key protection
- Unified platform approach spanning identity, keys, certificates, and compliance
- Post-quantum readiness today – supporting both current and next-generation cryptography

Build Trust That Lasts the Life of Your Product

In a world of connected, long-lived devices, security can no longer be an afterthought.

Entrust helps manufacturers move from reactive protection to **proactive, lifecycle-driven trust** – ensuring every device is secure from the factory floor to the field.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit www.entrust.com.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION