intertrust®

Product Brief

Platform

Securing the cold chain with Intertrust Platform and Intertrust PKI

Introduction

As countries across the world focus on sustainability, the retail supply chain has come under scrutiny. Breakdowns in supply chain infrastructure and efficiency are among the main contributors to food waste and greenhouse gas emissions. This is especially true of the "cold chain," or temperature-controlled supply chain. Within its two major sectors, food and pharmaceuticals, the cold chain is a complicated ecosystem that manages products throughout their lifecycle.

In order to maintain the highest quality standards for the product in question, organizations in the cold chain rely on IoT devices such as temperature sensors, automation control systems, and power monitoring tools. The data streaming from these connected devices is full of invaluable information on maintenance, product integrity, and more. As a result, IoT data management is critical to all supply chain activities including production, storage, and distribution. With numerous organizations within the ecosystem, being able to protect the data from malfeasance and share the right data with the right stakeholders is business-critical.

Cold chain challenges

A cold chain is a complicated, multi-stakeholder environment that spans multiple industries. Whether the product is ice cream or a life-saving vaccine, global cold chain transportation logistics typically involve refrigerated trucks ("reefers"). According to Statista, "refrigerated storage will be the largest segment of the global food cold chain market in 2024, accounting for 59 percent of the market."[1] Reefer trucks transport frozen and cold-sensitive products over long distances, maintaining the temperature within the container at a certain level. Temperature monitoring systems include RFID or wireless sensors located within the reefer. These sensors collect and transmit IoT data such as temperature or humidity at regular intervals, sometimes via satellite link. A change in temperature can ruin millions of dollars worth of perishable goods.

Along each step of the cold chain, thousands of IoT devices share information about issues such as maintenance, product integrity, and more. These devices can monitor temperature readings, test asset performance, investigate incidents remotely, identify performance issues, plan for predictive maintenance strategies, and improve overall operating efficiency. Yet these same technologies expose the cold chain to enormous risk.

Cold chain security challenges include issues around data privacy, data protection, and data governance. It's not surprising that top supply chain priorities in 2021 included improving security and understanding / mitigating third-party risks.[2] For the continued safety and stability of their products, cold chain stakeholders must ensure that their connected devices, and the data they gather and transmit, are legitimate and secure. As determined by Symantec, IoT devices experience an average 5,200 attacks per month.[3] IoT devices can serve as entry points for attacks that steal sensitive data, transmit false information, take control of a device's functionality, and even compromise development and manufacturing systems. Some of these obstacles can be overcome through the use of secure data exchange platforms.

Rules and regulations

The cold chain has an additional challenge—numerous complex regulations[4] that vary according to location and sector. For example, in the U.S., food safety and contamination prevention falls under the U.S. Food and Drug Administration (FDA)'s Food Safety Modernization Act (FSMA).[5] The pharmaceutical industry must comply with strict federal and international regulations around drug safety and efficacy, including three key FDA regulations that specifically address cold chain requirements.[6] Pharmaceuticals are also subject to international safety guidelines developed by the International Conference on Harmonization of Technical Requirements for Registration of Pharmaceuticals for Human Use (ICH).[7]

Having full operational visibility into IoT data and unified data governance across multiple data sources is absolutely imperative for cold chain regulatory compliance. Automated processes are also required; manual processes are simply not scalable when the data is coming from thousands of refrigerated container trucks with hundreds of thousands of sensors. All of this is necessary to maintain a robust audit trail.

Key benefits

Extend device lifetime

- Securely update software and firmware
- Reconfigure identities, embed custom attributes, and control access and actions
- Capitalize on new capabilities and meet the changing requirements in refrigeration technology
- Improve performance

Scalable, cost-effective provisioning

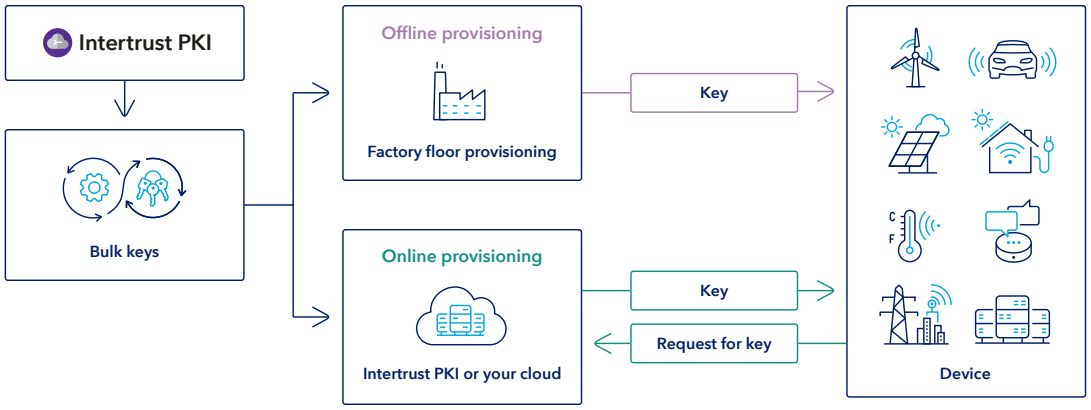
- Provision upwards of 10 million device identities per day
- Save 50-85% over the cost of provisioning device identities in-house
- Deliver device identities for all stages of the cold chain (manufacturing, transportation, storage) through Intertrust's scalable cloud provisioning service

Ensure trusted data interoperability and privacy

- Maintain authenticity of device identities on site or in the field
- Create secure communications across internal and external data sources
- Safely share data with pre-authorized partners across the entire cold chain
- Strongest cryptographic key protection

Comply with regulations

- Manage a robust audit trail
- Apply unified data governance across multiple data sources
- Conform to general and industry-specific regulations, standards, and guidelines with secure identity protocols
- WebTrust compliant and ISO 9001:2015 certified
- Supports compliance with NIST's IoT device cybersecurity guidelines (NISTIR 8259A)



Provision devices with identities when manufactured or when they boot.

Building a trusted cold chain IoT data ecosystem

The global IoT market is predicted to grow from approximately $381 billion in 2021 to more than $1.8 trillion in 2028.[8] Best practices dictate a defense-in-depth approach to IoT security, employing controls such as network segmentation and threat monitoring and response. The core of IoT security strategy, however, must be built into connected devices themselves. Thus, the foundation of a trusted IoT ecosystem begins with embedding secure identities into each device. Public key infrastructure (PKI) is a framework for delivering and managing cryptographically secure device identities to meet critical IoT security needs around authentication, encryption, and code signing.

Intertrust PKI™ is a certificate authority and managed PKI service specifically built for IoT. PKI for IoT operates at a completely different level of scale and complexity from standard enterprise PKI setups. It must be able to handle provisioning of very large numbers of devices—in the order of millions per day. It also requires a more nuanced data structure that contains various types of metadata, authorization statements, multiple cryptographic credentials, and mechanisms to securely manage and update the device's identity throughout its lifecycle.

The Intertrust Platform™ is a trusted data exchange ecosystem that acts as a secure data virtualization, data aggregation, and data collaboration layer for many different data sources and formats, regardless of location. It enables secure and efficient data orchestration, maintains data privacy protection, and ensures complete data governance. Applying better data governance protocols allows admins to enforce strict access controls to prevent unauthorized viewing or distribution of data.

The Intertrust Platform in combination with Intertrust PKI provides the following functionality:

- Secure authentication of device identities on site or in the field
- Secure communications across internal and external data sources
- Protected access and unified control over a wide variety of immutable datasets
- Managed governance of complex data rights
- Ability to collect real-time data securely, in a manner that respects the rights and regulations of all participants across the cold chain
- Protected portability of data sources and analytics into governed execution environments for collaboration and sharing

Intertrust Platform™

As a complement to its PKI system, Intertrust offers the Intertrust Platform, an edge-to-cloud data interoperability layer that uses secure data virtualization and identity and access management to enable governed data collaboration in secure workflow environments. It facilitates secure and efficient data collaboration amongst multiple parties, internal or external. It works across data silos and clouds and ensures compliance with security regulations and privacy protections.

Identity and Access Management

Device and user identity, authentication, and authorization; maintains platform objects and their relationships.

Secure Execution Environments

Secure network-isolatable environments for workload execution and controlled, interactive data exploration.

Data Virtualization

Data object definitions, permissions, restrictions. Provides data interfaces, manages DBs and virtualized datasets.

Time Series Database

Scalable, efficient, high performance database designed for time series data.

The need for trusted data

IoT data has the potential to vastly improve the sustainability and efficiency of the global cold chain, whether in the food or pharmaceutical space. Transportation management, operations logistics, and manufacturing all benefit from full visibility into IoT data. Within the cold chain, tracking the location, storage conditions, and travel speed of perishable goods can help stakeholders identify potential efficiency gains and cost savings, prevent critical failures, and meet compliance regulations. With its trusted data management ecosystem, Intertrust provides IoT device authenticity, enables organizations to maintain strict data governance, and facilitates secure data collaboration.

Sources

1 https://www.statista.com/statistics/1121010/global-food-cold-chain-market-share-segment/

2 https://www.statista.com/statistics/1196032/supply-chain-priorities-health-services-provider-and-pharma-executives/

3 https://cybermagazine.com/top10/top-10-cyber-security-threats-2021/iot-devices

4 https://www.coleparmer.com/tech-article/cold-chain-management-regulations

5 https://www.fda.gov/food/guidance-regulation-food-and-dietary-supplements/food-safety-modernization-act-fsma

6 https://www.elangham.com/2020/12/23/understanding-the-complexities-of-cold-chain-logistics-and-fda-compliance/

7 https://www.ich.org/page/ich-guidelines

8 https://www.fortunebusinessinsights.com/industry-reports/internet-of-things-iot-market-100307

intertrust®

Building trust for the connected world.

Learn more at: intertrust.com/platform
Contact us at: +1 408 616 1600 | dataplatform@intertrust.com

Intertrust Technologies Corporation
400 N McCarthy Blvd, Suite 220, Milpitas, CA 95035