

Next Generation Logistics, Secure Track and Trace

Logistical and manufacturing systems must merge and evolve with tracking technologies if the supply chain is to be truly secure.

By Magnar Løken d.y., CEO, Kezzler AS



Since the new millennium, there has been a notable change in how physical products and merchandise are expected to be handled. In general, safety and security requirements concerning counterfeiting, diversion, theft, tampering, dangerous and contaminated products and recall efficiency are more stringent as a response to safeguarding the supply chain. However, there still is a discrepancy and imbalance in regards to the quality and security measures under which a product is manufactured, and the protection of it once it has left the factory door. Beyond this point, brands are exposed and vulnerable to dangerous attacks as a result of being unattended and uncontrolled in the supply chain. In view of this, it is vital that product security is conveyed and executed all the way to the final consumer — through all stages of the product's life-cycle — so that the guaranteed product safety that was originally established is not lost on the way to its destination.

The requirements and regulations continuously and increasingly adjust to the situation of constant monitoring and security controls of the single product item and the selling units (SKU). The handling processes in the supply chain are changing to accommodate the new security regime. These systems are now generally known as Secure Track-and-Trace.

Most significant is the EU Regulation 178/2002 (Food Traceability, Article 18) and FDA Anti-Counterfeit Initiative that mandates extensive and granular tracing of the individual products in a secured supply chain. CIES estimates that in Europe alone there are one million businesses in need of aligning to the new requirements enforced as of January 1, 2005. Numerous initiatives are undertaken to prepare specific industries for secure track and trace and to inform and assist the public in product security matters. In the U.S., PhRMA has recently sponsored and introduced www.buysafedrugs.info, a dedicated website for fighting counterfeited drugs.

This presents a tremendous compliance challenge to the industry — at the same time as the demand for solutions continues to grow, technologies and solutions are in short supply.

Three *new* major capability factors are crucial in the shaping of the new secured supply chain and handling of (physical) goods:

- A) unequivocal identification of single items and selling units
- B) tracking of single items and SKUs in hierarchies throughout the entire supply chain
- C) real-time supply chain policies enforced on the basis of A) and B)

Supply chain policies, what are they ?

During the manufacturing process the security and quality of a product is guaranteed by enforcing manufacturing procedures. The same general concept applies for the secured supply chain. For a secured supply chain the most significant capability is the controlling protocols enforced when a product is transferred from one party to another, for instance from a pharmacy to a doctor.

Basically a supply chain policy has three building blocks, root policy (and root authority), the protocols and the parameters. The protocols are abstract rules and rule sets that govern when, who and how in a transient interaction session. The parameters are specific ranges, values, restrictions, lists and inputs obeyed and referenced during the carrying out of the protocols. Root policy is the authority and governing body regulating the supply chain policy infrastructure and its evolution.

To illustrate the differences between the protocols and the parameters the following simple example is given:

Protocol: { If drug has expired [parameter; **Expiry date**], do not sell }

The efficient enforcement and operation of an industry supply chain policy relies on two or more parties interacting simultaneously so that their individual supply chain policy and appropriate protocols and parameters *combined and additively* result in a negotiated *transient* session where all policies are enforced for that given situation. This means that if a second and/or third party fulfills the parameters of the first party's policy, the transaction can be performed. This enables seamless policy-based interaction with all unknown parties for any given situation.

This is similar to the Public Key Infrastructure (PKI) and Identity Management concept. Two prominent advantages with the concept are realized as there is no need to have any prior agreement or approval with any member of the infrastructure to interact. Secondly, the members do not need to update or keep track of changing parameters for the other members.

This allows industry and company managed changes in policies (protocols) (even if expected to be relatively infrequent), and parameters that are expected to be changed frequently. Further the internal policies for an organization can be ensured to stay in line supporting the external industry policies.

A company or organization operating a secured supply chain benefits by always being able to document effortlessly that their practices are in accordance with regulations and industry standards.

The most important parameter for a secured supply chain is the product identity

To illustrate the practical implications of product supply chain policies, three examples are given:

1. A pallet of a product from a foreign country is received by a hospital. In the secured supply chain the hospital signs (tracks) the security code on the pallet. Immediately after the tracking of the product there is a policy inconsistency alarm. The policy that

has been violated is the following: the product is not allowed to be handed over to a hospital before having been approved and registered by customs.

2. A consumer checks out a package of drugs at the pharmacy counter. The retail system scans the product and it is automatically controlled for consistency with the manufacturer's supply chain policy. The system responds with an alarm and the product is not allowed to be sold to the consumer due to a product recall.
3. A retailer is about to receive a pallet of drugs from a distributor. When attempting to transfer the pallet to the retailer, the pallet's security code is controlled against the supply chain policy. A violation alarm is given to the distributor, stating that the receiving retailer has its license for handling drugs revoked and that the goods are not to be handed over.

The power of secured supply chain policies is the "automatic" enforcement and the fact that the "content" of the policies are dynamically changed, i.e. expiry dates and product recalls.

Issues regarding conventional logistical, manufacturing and packaging systems

Conventional logistical systems are designed to streamline the transportation of goods between locations. Typical goods transported are pallets, containers, packages and the like, and it is done without security measures concerning the overall product and supply chain. These systems do not divide or mesh a production batch, nor do they enforce supply chain policies relating both to the product identity *and* an associated third party (owner), and thus do not tie the supply chain together as one logical procedure.

Most current manufacturing systems and Enterprise Resource Planning (ERP) systems do not accommodate for safe tracking and tracing in the supply chain, because there is no direct link with the products they are handling (which is a fundamental principle for security tracking and tracing). They neither assemble nor record the products and the transportation unit(s) in a hierarchical manner, a prerequisite for tracking and tracing units as they are broken up and are continuously being de-fragmented in the supply chain.

Conclusions

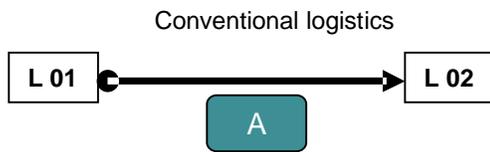
Logistical and manufacturing systems must merge and evolve with security tracking technologies to provide a secured supply chain continuously enforcing industry supply chain policies and the industry supply chain policy infrastructure.

A new concept introduced by security logistical systems is the absolute availability of real-time information from the supply chain to all participants for their respective internal confidential analysis. Previously, the brand owner gained only limited access to such information, in the secured supply chain the brand owner will transport their products by "remote control." It must be emphasized that these capabilities are delivered by the secure tracking and tracing software infrastructure, and must therefore operate on all data carriers capable of carrying a digital identity.

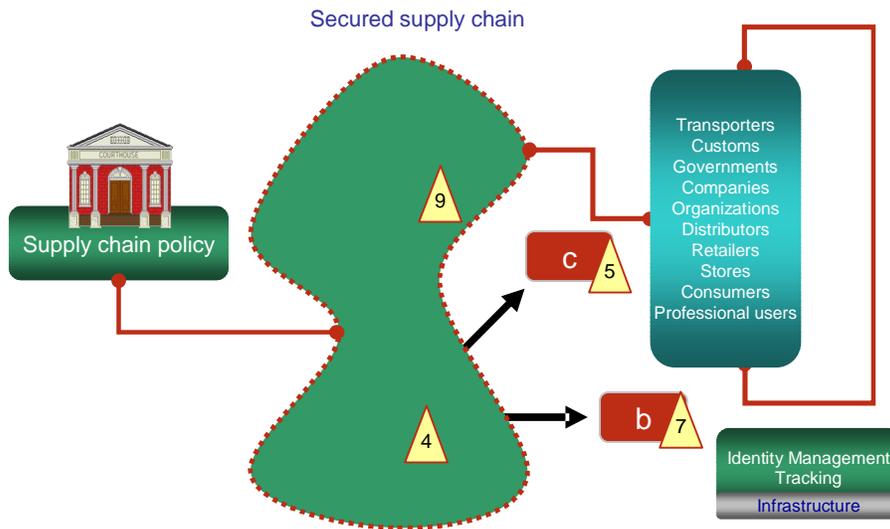
Companies, governments and organizations can establish supply chain operation centers that monitor and ensure product safety on a 24/7/52 basis for the benefit of all, especially consumers.

Traditional logistical systems can be seen as having a horizontal focus, i.e. moving goods from point A to point B without considering the purpose or content of the transportation. Security tracking adds to the complexity of the horizontal dimension (e.g. more stringent protocols for the transaction of goods), but one of the most significant new dimensions is the vertical handling of the transported goods from A and B — that is, the packaging hierarchy (mother-child(ren)-grandchild(ren)) and its inherent dynamics. When transportation units eventually are split, the remaining content must be tracked without losing the previous history of all the transportation units involved. The hierarchical tracking concept results in an ever-increasing number of units to track (securely), as they are transported to an increasing number of different locations, and most of the units' logistical packaging "disappears and evaporates."

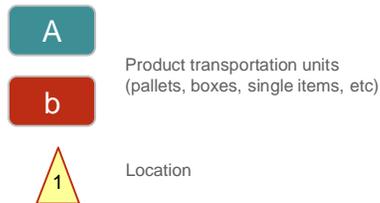
The difference between the conventional logistical chain and the secured supply chain is illustrated below.



Pallet A is transported from Location L01 to Location L02



Legend



Pallet A at Locations 4 is broken up (split) and a box d from its content is transferred to Location 9 and another party. The green shaded area illustrates that the transfer is carried out according to and being protected by the supply chain policy. The remaining boxes originally the content of pallet A are transported to locations 7 and 5.

About the Author

Magnar Loken d.y. is the founder of Kezzler. Loken has been the architect for several large national IT projects, with particular responsibility for security architecture and Public Key Infrastructure (PKI). He was the initiator of the Takisai project, one of the first web-based electronic workflow and content management systems of its kind based on PKI. As the Chief Technology Officer with the Norwegian Patent Office he worked with the standard using PKI for the World Intellectual Property Organization (WIPO). Loken is the Chief Software Architect and inventor of Kezzler's core technologies.

Kezzler delivers secure track and trace solutions to the pharmaceutical and fast moving consumer goods industry. Kezzler's award winning software and technologies manage every single product item and logistical unit with a digital identity (kezzlercoding) giving the brand owner full visibility of the supply chain.

For more information, contact:

Kezzler AS

Wergelandsveien 1, Oslo

office@kezzler.com

+47 926 68 785

www.kezzler.com