



SToP Project eNewsletter

November, 2008

Consumers play an essential role in fighting counterfeit activities.

(European Crop Protection Association, 2008)

SToP eNewsletter is issued quarterly. Each edition contains a short overview of the project achievements and information on related topics.



Strategies to fight counterfeit trade

Strategies to fight counterfeit trade can be ascribed to one or more of the following categories: securing the company's supply chain, eliminating production of counterfeit products, hampering their distribution, discouraging or preventing users or consumers from purchasing faked goods, and limiting the damage that may result from illicit products. In order to achieve the corresponding goals, measures are required which can be categorized as organizational, technological, legal, and communicative in nature. Companies usually choose a combination of these measures to tailor a mitigation approach which reflects their individual risk profile.

Mitigation strategy	Organizational	Technological	Legal	Communicative
Securing the supply chain	++	++		
Eliminating illicit production		+	+	+ ²⁾
Hampering illicit distribution		+	+	+ ²⁾
Stopping deceptive consumption	+	++		+
Stopping non-deceptive consumption		+ ¹⁾	+	+

1) Only if security mechanisms can affect the functionality.

2) Only indirectly over legal measures.

Figure 1: Generic mitigation strategies to avert counterfeit trade

In line with the SToP project orientation, especially the **technological and organizational measures** hence need to be exposed.

From the *organizational* perspective, of supply chain security, companies have to take care of two threat scenarios: first, non-original components that the company purchases itself (and that may end up in their products); and second, faked versions of the company's product which are traded as deceptive or non-deceptive counterfeits on the target market. For the first scenario a careful selection of

component suppliers and subcontractors is of particular importance. When purchasing goods companies should consider the risk imposed by completely counterfeit products as well the risk of substandard parts that have been built into otherwise genuine products. Therefore manufacturers have to rely on their suppliers – and should include counterfeit-related aspects in their auditing process. Anti-counterfeiting measures should also be reflected in purchasing strategies for B and C goods (for example power cords, batteries, etc.) since these categories are frequently targeted by illicit actors. Even if a supplier is well-known and trustworthy, its problem awareness has to be questioned. To hamper the distribution of imitations, it is desirable to maintain tight control over the distribution channels. Tightly controlled distribution networks greatly reduce the number of deceptive counterfeit cases in consumer markets.

Here, *technological* measures are of the high importance and being integral part of many anti-counterfeiting strategies. They serve as a means to verify genuine goods and thus help to distinguish them from counterfeits, or, for certain product categories, increase the production costs for illicit actors and confine the functionality of faked articles. Holograms, flip colors and micro printings are all prominent examples of established protection mechanisms. However, copying these static features constitutes an ever-lower barrier for illicit actors, and many imitations today resemble their genuine counterparts so closely that their inspection becomes a time-consuming process. Thus the ability to verify products in a fast and reliable way is an important success factor of technology based anti-counterfeiting strategy. More secure features such as

chemical and biological markers are often not suitable for large-scale testing – but in a market where an increasing number of counterfeit goods intermingle with mass-produced items, large samples or even complete checks are necessary. The latter factor also renders covert security features impractical, which, in this scenario, would require a large number of insiders to know about the characteristics of the hidden feature, which again would impose a security risk.

Another severe drawback of established anti-counterfeiting technologies is the limited ability or motivation of the user to check for the product's authenticity. Since security mechanisms are usually changed after being compromised, their users must be constantly kept up to date. Genuine products with different features often coexist until an old product line has been sold out, which complicates the checking process even more. As a consequence counterfeiters try to leverage the confusion among licit stakeholders which renders many technologies ineffective.

Emerging RFID-based countermeasures constitute a new approach to consolidate supply chain performance and security. Potential advantages over existing technologies are the possibility to automate large-scale tests to enable significantly higher check rates, the ability to change underlying security protocols while maintaining the user interface, and the potential high level of security. Overall, compared to the old technical countermeasures, RFID can provide brand-owner companies with better trade-offs between the usability (e.g. read distance, read time, effort to verify a product) and level of security.

High costs for the infrastructure, objections to data access and sharing, and privacy concerns among consumers are viewed alongside the technology's potential to avert counterfeiting, to achieve higher supply chain visibility, enhanced production, inventory and distribution control, and to implement efficient replenishment procedures. However, before the RFID technology reaches a sufficient level of maturity, the read errors as well as slow read and writes rates can make it unusable in some commercial applications. This is especially the case for the health care industry that needs to produce large volumes of uniquely identifiable products, with a minimal rate of identification errors.

A further benefit of technical countermeasures is the elimination of the borderline cases where a licit supply chain partner can state that he had no reason to think the products he traded were of counterfeit origins. By providing all players with a standardized means of verifying the origins of the products, players involved in the borderline cases have no more excuses not to detect the counterfeit origins, and will face full liability.

FIELD TRIAL – production of electric and combined water heaters

In October 2008, SToP partners conducted trial to demonstrate the verification of the SToP PVI in the real-world environment. The trial took place in Gorenje Tiki Ltd., Slovenia – producer of electric and combined water heaters. For the trial purposes, the integration of SToP PVI and Warehouse Management System, named e-logis® at the industrial partner has been achieved. Basic trial characteristics:

- Actors involved: Oria & SAP (SToP partners), Gorenje Tiki Ltd., (industrial company)
- The pallets (nested handling units) were tagged with barcodes. The pallets can carry more items; usually they carry 4-10 electrical water heaters. Single items (HU – handling unit) were tagged with RFID tags. Each NHU can carry one or more HUs. At the end of production line each handling unit is tagged, scanned and stacked on carrying unit. At the same time setup data for each HU is sent to PVI. When verifying products in PVI user can therefore scan:
 - NHU - one scan sends multiple verification requests to PVI
 - HU - scanning product by product where each scan sends one verification request to PVI
- Technology and equipment:

Hardware: Datalogic Kyman (Laser + RFID), Button RFID Tags from Texas Instruments (Standard ISO - 15693), Barcode labels

Software: E-logis®, E-logis® PVI module

Trial processes:

PVI integration in production

When the user scans each item to receive it from production line to warehouse management system, the system itself in a back process, not seen directly by the end user, send setup data to the PVI. Most important part in this part of trial is that existing process is untouched by the PVI

integration. It is achieved with back process which collects all items that need to be sent as a setup data to PVI. For this part of trial the existing warehouse management system had been upgraded, so that responsible users had been able to see the communication log of sending setup data to PVI.

Identified potential issues in the production process:

- PVI communication error: Blocking shipment of goods not reported to PVI (e-logis® allows warehousing it but keeps status 'Quarantine' to prevent shipping to customer until response 'accepted' is received from PVI)
- Finding 'duplicate' items: If the setup data was sent by our company, we may have problems with counterfeits or errors in applying unique identifiers, at those cases we need to apply new tag or label and resend setup data
- Damaged RFID tags or barcode labels: Applying new tag or label, Resending setup data (should also send update to setup data of damaged HU)

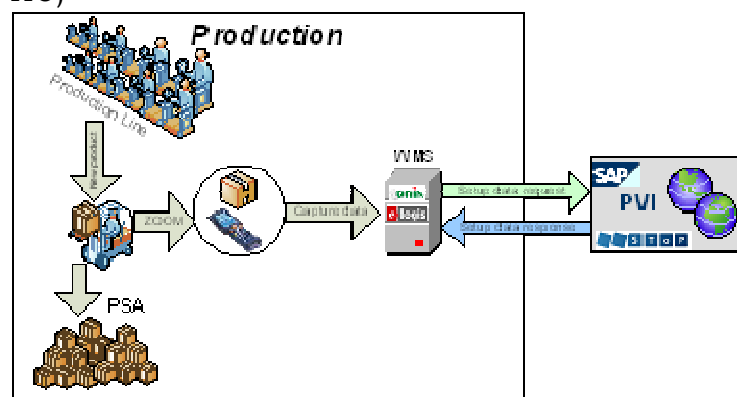


Figure 2: Process at the end of production line

PVI integration in warehousing

Usually the company has more than one warehouse and the items need to be moved from one warehouse to another. Moving items from one

warehouse to another warehouse can be an entry point for counterfeit items also. It should be therefore achieved that all items shipped from one warehouse are verified before sending, and than all items received at end warehouse are verified. Change of warehouse for warehouse management system can also be moving items from one PSA (Production Supply Area) to warehouse.

Identified potential issues in the Warehousing process:

- PVI communication error: Further investigation – items can not be shipped to another warehouse until successfully verified
- Finding ‘unknown’ items: Possible infiltration of counterfeit goods or Mistakes at production line while receiving items to PSA. In this case user has to receive item from production line on the basis of production order
- Damaged RFID tags or barcode labels: Applying new tag or label, Resending setup data

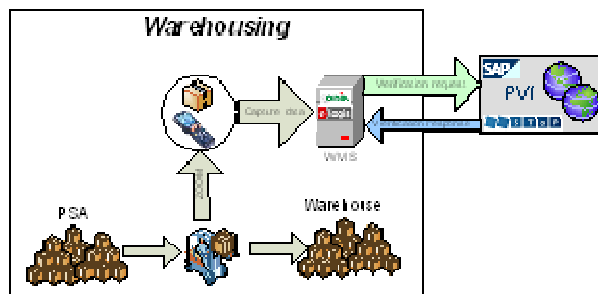


Figure 3: Warehousing process

PVI integration in shipping process

From warehouse management system this process is almost like process of warehousing, when we move items from one warehouse to another.

Identified potential issues in the shipping process:

- PVI communication error: Blocking shipment of unverified goods
- Finding ‘unknown’ or ‘Counterfeit’ items: e-logis® status ‘Quarantine’ unable to ship, Remove

items from shipment, Damaged RFID tags or barcode labels, No manipulation with unidentifiable items

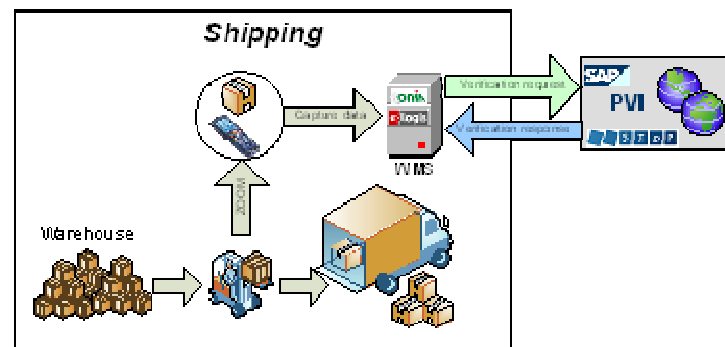


Figure 4: Shipping process

Towards future development:

- The integration of company’s existing Warehouse management system (e-logis®) and PVI was successful.
- The use of versatile RFID equipment such as RFID Portal system for FLT manipulations was perceived as being suggestible. Such kind of gates could be build on enters and exits of warehouses, that the system would scan all the items that pass those gates.
- Extended PVI integration, such as sending track & trace data to PVI, or receiving whole e-pedigree from the PVI: The company could also send the “shipping” data to the PVI when they ship items to their customers, or the “receiving” message when they receive items from their suppliers. To improve the security of those messages, we could have use secure connections. For trial purposes we have used unsecured connections to the PVI.

SToP DISSEMINATION ACTIVITIES

PAST ACTIVITIES

- SToP presentation at European Associated Laboratory in Microtechnics (EAL) Workshop September 8-9, 2008 <http://www.lea-ut.org/arcetsenans2008/>

Reference: F. Gourmanel, Richemont

- SToP poster at the "Towards a European policy on RFID" Conference & Exhibition September 19, Brussels, Belgium <http://www.rfid-outlook.pt/>

- "Securing Global Supply Chains" - Session at the Value Chain Forum 2008,

October 10, 2008 <http://www.value-chain.net/>

Co-moderators: Carsten Magerkurth and Ali Dada - SToP project & Barabara Flügge - ITAIDE EU project
Scenario: Presentation of SToP project and PVI prototype (authenticating pharma packages at a pharmacy).

UPCOMING ACTIVITIES

Reference: Carsten Magerkurth, SAP Research, Germany

CONTACT & INFORMATION

Additional information is available at SToP project website <http://www.SToP-project.eu/>

Technical project coordinator:
Mr Harald Vogt
Phone: +49 721 69 02 51
E-Mail: harald.vogt@sap.com