



SToP Project eNewsletter

February 2008

Counterfeited and pirated articles threaten the health and safety of EU citizens, their jobs, Community competitiveness, trade, and investment in research and innovation.

(Taxation and Customs Union, 2007)

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



INTERMEDIATE SToP PROJECT RESULTS

Main drivers and mechanisms of illicit trade and the roles of different actors (D1.1.)

SToP consortium presents the results of an empirical study on counterfeit supply reveals, the existence of different types of counterfeit producers, each with distinctive properties with respect to production capabilities, required skills and investment, malfeasance, and consequences in case of prosecution. The classification of counterfeit producers is made, which allows for differentiated analyses of the potential threats as well as for the development

of anticounterfeiting strategies that reflect the weaknesses of each type of actor.

The study furthermore stresses the investment-risk-return-driven considerations that are likely to heaving lead to the formation of the individual groups. The findings substantiate a more realistic picture of the illicit supply chain and the way it interfaces with licit supply.

Leading partner: University of St. Gallen, Switzerland

Description of technical and organizational requirements for product authentication solutions based on ambient intelligence (D1.2)

The report presents analysis on technical, business and regulatory requirements for a product verification system (PVI) in different types of industries have been done - requirements of the pharmaceutical industry, requirements of the luxury goods industry and requirements of the aerospace industry.

In addition, SToP consortium presents the agreed use cases by industry. The use cases define the functional requirements for the design and development of the PVI. They include

registering a product at the manufacturer, issuing authorization to verify products, updating product, authentication of single and multiple products, incident warning, and statistical analysis. Finally, also the outcome of the end-user and consumer privacy requirements is presented in deliverable of WP1 Problem and Requirements Analysis.

Leading partner: University of St. Gallen, Switzerland

Description of the impact of the main drivers and mechanisms fostering illicit trade on the financial framework (D2.1)

The report provides a description of the impact of main drivers and mechanisms of illicit trade on the financial framework of affected companies. Based on extensive literature review and interviews with representatives from the luxury goods, pharmaceutical, and the aerospace industry, the key components mostly affected by illicit activity are identified; namely short term revenue, brand value, legal expenditures, costs of awareness programs, and costs of

technical countermeasures. In accordance to current research, the report also provides an overview over possible positive effects of illicit trade on affected enterprises. The report builds upon the related scientific work and advances the state-of-the-art by in-depth investigations of the three industries under study.

Leading partner: University of St. Gallen, Switzerland

Definition and first estimation of the key cost drivers of the proposed solution (D.2.2)

Based on the available literature on cost evaluation of IT system implementations, SToP consortium provides definition and first estimation of key cost drivers of a technical anti-counterfeiting solution. Common factors include costs for technology assessment, prototyping and trial runs, technology procurement, software and hardware installation, security features, hardware maintenance, and product authentication. These expenses are

analyzed in accordance to a standard technology implementation process, which is made up of three steps:

- Technology selection
- System setup & installation
- System operation

While each of these sub-processes is described in detail, concepts are shown how the identified cost drivers can be quantified commensurably.
Leading partner: University of St. Gallen, Switzerland

State-of-the-art analysis on relevant research, existing technologies and products (D3.1)

The report describes approaches and methods for authenticating products and securing the supply chain. It includes a review and comparison of authentication techniques, comprising direct authentication, authentication by means of a difficult to reproduce feature, verification of unique identifiers, plausibility checks of track and trace data and secure object authentication enabled by cryptographic methods. The conclusion is oriented towards two classes of authentication methods:

some methods are reliable but costly and slow, while others (particularly the check of track and trace data) are well suited for bulk checking, but not as secure. In addition, the report provides also an overview of commercially available authentication solutions and the state of implementation of technical anti-counterfeiting measures in industries that are of particular interest to the SToP project.

Leading partner: SAP, Germany

Report and Analysis on State-of-the-Art Tagging Technologies Specific to the SToP Project Requirements (D4.1.)

The report presents currently available anti-counterfeiting technologies. There are broadly speaking 3 families of anti-counterfeiting approaches – identification, authentication, and tamper proof either used alone or in combination.

Numerous technologies are evaluated and filtered according to SToP objectives, arriving at a shortlist of currently available technologies most suited to the end user requirements specifically RFID, digital watermarks

& detection patterns, security printing, and laser surface authentication.

In addition, these shortlisted technologies, combinations thereof, or even developments of new approaches, will be considered for the next phase of the SToP project.

Leading partner: SPACECODE, Switzerland

IN RESEARCH: COLLABORATIVE PRODUCT AUTHENTICATION

Collaborative product authentication is a novel scenario for consumers using RFID-enabled mobile phones to identify products. This academic and not yet practically applied approach was studied in the frames of the SToP project, resulting in a poster displaying it at the conference UbiComp 2007 (the paper by Felix von Reischach and Florian Michahelles is available at <http://www.im.ethz.ch/people/freischach>). The fundamental idea is that consumers discover fake products in a particular shop and share this experience with other consumers in a community-like fashion. These are warned accordingly and avoid buying counterfeit products from the corresponding shop. The procedure is divided into two sub processes: contributing to the community and benefiting from the community.

CONTRIBUTING TO THE COMMUNITY

Consumers who contribute to the community notify a server that they have discovered a fake product in a particular store at a certain point in time. The process is structured as follows: a consumer gets hold of a product and notes that it is counterfeit. The consumer scans the product's RFID tag using his mobile phone. Accordingly, he selects the seller who offers the product, using a menu in the mobile phone. Having specified the product type and the shop, a warning is transferred to the backend using a wide area connection. The data is stored in the

backend and can be queried by other consumers from now on.

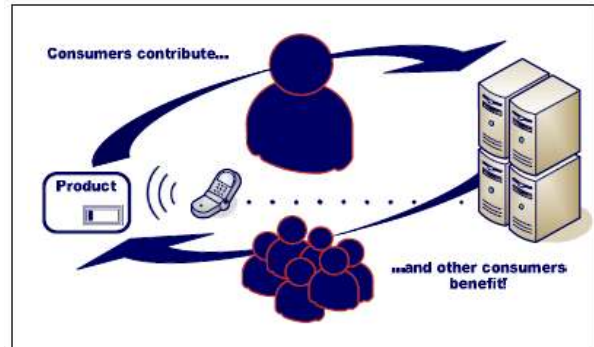


Figure 1: Collaborative Product Authentication

BENEFITING FROM THE COMMUNITY

The more warnings users have transmitted to the system, the higher the benefit for other users. They scan random products in shops and receive information if the scanned product type has been reported counterfeit for the particular shop. This takes place as follows: a consumer discovers a product in a shop and is tempted to buy it. But before buying the product, the consumer would like to confirm that the product on hand is genuine. He uses his mobile phone with an integrated RFID reader and scans the RFID tag of the product. Knowing the product type and having selected a shop from a list, the client installed on the mobile phone queries the backend for warnings for the given product type and shop. The data is transferred to the mobile phone and visualized to the user, who can now decide whether to buy the product.

CALENDAR OF EVENTS

PAST EVENTS

SToP Exhibition at the Conference & Exhibition on RFID
November 15-16, 2007, Lisbon, Portugal <http://www.rfid-outlook.pt>
Demonstration of the first working PVI prototype - remote interface using an NFC equipped mobile phone in order to demonstrate the interplay of product authentication processes at a retailer and at a manufacturer's back office. *Responsible partner: SAP, Germany*



FUTURE EVENTS

"Internet of Things 2008" Conference
March 26-28, 2008, Zurich, Switzerland <http://www.iot2008.org>
Demo: "Integrated Processes for Product Authentication with Special Consideration of Mobile Phones"
Responsible partner: SAP, Germany
&
Demo: "Synchronized Secrets Approach for RFID-enabled Anti-Counterfeiting" *Responsible partner: University of St. Gallen*

Journal Live! (Conference/exhibition)
Las Vegas, NV, USA, April 16-18, 2008
<http://www.rfidjournalevents.com/>
SToP consortium partner, University of St. Gallen, Switzerland will participate at the session on RFID usage in anti-counterfeiting.

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