



## **SToP Project eNewsletter**

**May 2008**

*In 2006, EU Customs seized more than 128 million counterfeit and pirated goods and handled more anti-counterfeiting cases than ever before.*

*(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.



## REQUIREMENTS OF LUXURY GOODS INDUSTRY AGAINST ILICIT TRADE

SToP project partners conducted the analysis on technical, business, and regulatory requirements for a product verification system (PVI) in different types of industries (*D1.2. Description of technical and organizational requirements for product authentication solutions*).

This section of Newsletter outlines the requirements of the luxury goods industry:

### *Business objectives*

- The system must contribute towards improved brand protection. (Primary)
- The system must allow a none-brand-expert to identify a fake product fast and easy. (Primary)

### *Object authentication*

- The system must be able to authenticate different kinds of products including: watch, clock, jewellery, pen, accessories, leather goods, eyewear, perfumes, cosmetics, wines and spirits. (Primary)
- The system must be able to authenticate one metallic good at a time. (Primary)
- The system must be able to authenticate multiple leather goods at once. (Secondary)

### *Location*

- Products can be authenticated in the manufacturer's premises, in a partner company, at the point of sales, in after sales services, by private investigator, and in customs. (Primary)
- Products can be authenticated by the end-user/consumer. (Secondary)

### *Level of automation*

- Products can be authenticated with or without human oversight. (Secondary)

- System can authenticate several leather goods in few seconds in bulk mode. (Secondary)

### *Process and environment*

- The security features must resist temperature range from -20C to +80C without becoming permanently nonfunctional. (Primary)
- The security features must resist physical stress of pressing, water proof and dry cleaning without becoming permanently non-functional. (Primary)
- Only an individual number can be visible on a product, other security features must be covert (no aesthetic impact). (Primary)
- Security features must be active all along the life cycle of the product till product destruction, which can be from 1 to 100 years. (Secondary)
- The security features must be resistant to after-sales operations (repair, polishing, and component exchange). (Secondary)

### *Other authentication features and needs*

- Tampering of the security features must be identifiable.
- The system must provide flexibility regarding authentication methods and technologies, user input, access levels, output, and decision process.
- The security feature must be upgradeable if a feature is copied or cracked. (Secondary)
- Product's identifier is not readable without the user's consent. (Secondary)
- The system must know the allowed sales locations of products to detect diversion. (Secondary)
- The anti-counterfeiting system must be linked to supply chain management system to allow data transfer. (Secondary)

## IMPACT OF METALLIC ELEMENTS ON RFID SYSTEMS – “WATCH” CASE

Metals interfere with the propagation of radio waves, acting as an electromagnetic shielding. The behavior of radio waves in the presence of metals is determined by three main factors: shape and position of the metallic object, nature of the metal and wavelength. These parameters were studied in order to select a satisfying frequency band. Low frequency (125 kHz) proved to be the most resilient to the presence of metal as a rule. A specific simulation of the watch case was made, and confirmed this expectation.

Typical product development comprises 3 phases, 3 core components that generate solutions, in a staged approach:

- *Component development-essential* R & D phase of foundation technology (Chips – focus on either standard or proprietary, Tags - focus on form factor and performance and Readers – focus on standard or proprietary, form factor, performance)

Based on the simulation result a first prototype was made, SpaceCode, France developed a specific tag able to be inserted into the watch case.



Figure 1: RFID Watch reader prototype (tag)

Also a reader antenna has been developed to read through the metallic part of the watch



Figure 2: RFID Watch reader prototype (antenna)

- *Solution development and integration:* Components are combined into self sufficient RFID hardware solutions, also combined with requisite software.

In partnership with SAP, a UHF Impinj and a LF Spacecode reader have been integrated to the SAP system.

- Phased rollout: *typical industrialization of developed solutions follows 3 stage approach:*

- Prototype/feasibility: essential proof of concept to demonstrate the solutions works as described.

- Pilot: live implementation and integration of the solution into customer's products and processes.

- Roll out/scale-up: where solution becomes way of business for the customer.

- Commercialization: full commercialization occurs in close succession/in parallel to completion of first 'test bed' customer and comprises typical marketing, advertising, and sales force promotion.

## SToP ACHIEVEMENTS – DISSEMINATION ACTIVITIES

### PAST EVENTS

#### *Demonstrations:*

SToP demonstrations at the Internet of Things conference 2008, March 26-28, 2008, Zurich, Switzerland  
<http://www.iot2008.org/>

*Demo title: "Integrated Processes for Product Authentication with Special Consideration of Mobile Phones"*

The demo has featured feature a multi-step authentication via the mobile phone in which both item IDs and visual authentication was demonstrated. Furthermore, the demo also presented the latest additions to the PVI including a more elaborated reporting and statistics module.

*Demo title: "Synchronized Secrets Approach for RFID-enabled Anti-Counterfeiting"*

The demo was intended to demonstrate how standard low-cost RFID tags can be used for anti-counterfeiting in a non-conventional but efficient way. A method that detects desynchronization when cloned tags are introduced in a protected channel was used. It thus helps to prevent the further distribution of the counterfeit products.

#### *Invited Talk:*

*Talk title: "RFID in Anti-Counterfeiting: From Security to ROI".* Invited talk in RFIDJournal LIVE! Conference 2008, Las Vegas, April 16-18, 2008.

### UPCOMING EVENTS

#### *Demo:*

SToP demo at RFID Sys-tech Conference - 4th European Workshop on RFID systems and technology (RFID Sys-tech)

Freiburg, Germany, June 10-11, 2008  
<http://www.rfid-systech.org/>

#### *Panel:*

»Issues and Opportunities for product e-tampering prevention« at 21st Bled eConference - eCollaboration: Overcoming Boundaries Through Multi-Channel Interaction  
Bled, Slovenia, June 15-18, 2008  
<http://BledConference.org>

#### *Research papers:*

*Anti-Counterfeiting Based on Supply Chain Proximity*

The research paper will be available in Jens Strueker, editor, 4th European Workshop on RFID Systems and Technology (RFID Sys-tech), 2008.

Authors: Ali Dada and Carsten Magerkurth, SAP Research, Germany

*RFID-based Anti-counterfeiting Utilizing Supply Chain Proximity*

at the 2nd International Workshop on RFID Technology (IWRT)

<http://www.iceis.org/workshops/iwrt/iwrt2008-cfp.html>

Authors: Ali Dada and 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](mailto:harald.vogt@sap.com)