RESCUEIT: sécuRisation dE la Chaîne logiStique orientée serviCe depUis le mondE des objets jusqu'à l'univers InformaTique

J-P Deutsch[1], J. Hue[2], Y. Gaffé[2], L. Gomez[3], M. Khalfaoui[3], M. Laurent[4], A. Levieux[5], E. El Moustaine[4]

[1]LogPro Conseil, Paris

[2]SOGET, Le Havre

[3]SAP Research, 06250 Mougins

[4]Telecom Sud Paris

[5]ISEL, Le Havre

jpdeustch@logpro.fr, julien.hue@soget.fr, yoann.gaffe@soget.fr, laurent.gomez@sap.com, mehdi.khalfaoui@sap.com, Maryline.Laurent@it-sudparis.eu, levieux.aurelien@gmail.com, ethmane.elmoustaine@telecom-sudparis.eu

Abstract – In global supply chains, many organizations (be it public or private) are involved, and each may own its supply chain software. From a collaborative perspective, they need to work on the global process; first in terms of planning, second from an operational perspective, with a view on the management of attacks and on resilience. From a modeling perspective, RESCUEIT proposes to represent a complete supply chain in the public security area. It also proposes to integrate security requirements, and to design a database about risks and mitigation procedures related to supply chains. From a requirements perspective, the project proposes to identify the relevant security parameters, which need to be monitored and controlled. From an Internet of Things perspective, the project will enhance the usage of wireless sensor networks and of RFID systems, tailored for the specific needs of a secured supply chain. In this paper, we present a scenario related to importation of dangerous products in Europe. Elaborated with major actors of the supply chain, we secure this scenario following end users requirements. To that purpose, we propose a set of security mechanisms for secure tracking and monitoring of products. They are all integrated into a joint platform, detailed in this paper.

1. Context

1.1 RESCUEIT: a joint German-French research project

In our flat world and in public security in particular, one cannot see a supply chain as a single process, managed by a single entity. Several entities – be it public or private entities are involved, each potentially using a dedicated supply chain management software. Yet as a whole, these entities need to work from a global process perspective; first in terms of planning, second in terms of operating, with a view on how to handle interruptions (possibly due to attacks) and on how to manage recovery. By focusing on how to ensure that real world information – through RFIDs and wireless sensor networks (WSN) – can enhance the security of the supply chain, this project answers to the ANR CSCOSG 2009 topic: "SECURING THE LOGISTICS CHAIN". With the growing pressure from regulations to enhance security, while needing to control and lower the costs, Supply Chain Management (SCM) has to face an end-to-end problematic: the proper modeling of a complete supply chain, while including relevant security requirements, and leveraging real world information to both assess the security level and enforce the security requirements. At a modeling level, RESCUEIT-FR proposes to model a complete supply chain in the area of public security. At a requirements level, it proposes to identify the relevant security parameters that need to be monitored and addressed. At a real world level, it proposes to enhance the use of WSN and RFIDs for the specific needs of a secured SCM.

1.2 Scenario: Importation of dangerous goods from China

In order to illustrate our approach, we propose to use a supply chain scenario defined in the scope of the RESCUEIT [1] project. Related to the importation of dangerous products from China to Europe, this scenario

has been elaborated and validated by end users such as Kuehne and Nagel (K+N) and the group Casino [2].

Chemicals are imported from a Chinese harbour toward the harbour of Le Havre, in France. Shipped products are household and gardening chemicals. These products are meant to be shipped by boat from a Chinese harbour. When received at the Le Havre harbour, the merchandise is checked by customs against REACH [3] regulations.

REACH is the European Community Regulation on chemicals and their safe use (EC 1907/2006) [5]. It deals with the registration, evaluation, authorisation and restriction of chemical substances. The aim of REACH is to provide an additional layer of protection for humans and the environment through the better and earlier identification of the intrinsic properties of chemical substances. To that extend, REACH introduces specific constraints on chemicals along the supply chain. They include the flash point, incompatibilities between products, and humidity conditions for chemicals.

At the Le Havre harbour, French customs with the support of an Approved Economic Operator [4] proceed to a merchandise integrity check. After a check of administrative document describing the content of the cargo, customs verify the quantity and quality of the products received.

Once quality checks have been performed at Le Havre harbour, and customs have verified that the merchandise is compliant with safety regulations, products are shipped by pickup trucks toward the warehouse located close to Savigny le Temple. This K+N warehouse, dedicated to the storage of dangerous products, is classified SEVESO II. This classification defines a set of safety management systems, emergency planning and land-use planning and a reinforcement of the provisions on inspections to be carried out by classified sites.

In this case, specific safety measures are implemented on site, such as storage rules (e.g. limited quantity of chemical stored at the same place). Finally, household and gardening products are distributed to retailers (e.g., Casino supermarket).

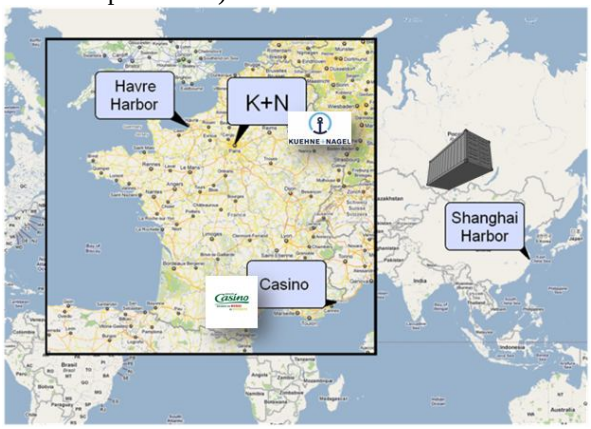

FIG 1: IMPORTATION OF DANGEROUS GOODS FROM CHINA

1.3 Identified products constraints

In the scope of this scenario, we identify three gardening and household products ICPE-classified. ICPE [5] is a French nomenclature for ”Installation Classee pour la Protection de l’Environnement”. This classification defines a set of measures to be enforced for the handling, storage and transport of dangerous products. Each of the identified products has specific normative ICPE constraints: ICPE 1412, 1432, 1172.

Inflammable liquids are classified under ICPE 1412. In order to manipulate this product, gloves, glasses, protective clothing helmet and eye wash are mandatory. Products classified 1412 are a harmful and polluting product. Its flash point is 66 Celsius degrees. The flash point of a volatile liquid is the lowest temperature at which it can vaporize to form an ignitable mixture in air. In addition, this type of product must not be mixed with acids, bases or oxidizing. In addition, it is self flammable in large quantity at high temperatures.

Therefore, in addition to risks of pollution along the supply chain, this product represents a significant risk of fire, if exposed to high temperature. In order to mitigate this risk, monitoring of ambient temperature is crucial.

ICPE 1432 products are liquefied gas inflammable. To manipulate this type of product, gloves, classes, protective clothing, wash eye, are mandatory. With respect to transport, they are classified UN 1950 or aerosol, with the mention of the restricted quantity, and a tag code 2.1-5F. Their flash point is between 13 and 13,4 Celsius degrees. It must not be in contact with acids and metal. Same as for ICPE 1412 products, in order to mitigate risk of fire, it is important to monitor ambient temperature.

Products classified as ICPE 1172 are dangerous for environment, extremely toxic for aquatic organisms. Gloves, classes, mask, and eye wash are required for the handling of Ronstar.

Ronstar is classified UN 3007. In addition, this is irritanting. Packaging of Ronstar is classified type III.

For transport, those dangerous products are classified UN 3082 [8], meaning dangerous products for the environment.

UN code is four digit used for the transport of dangerous products. As this type of products is considered as slightly dangerous, packaging of type III is mandatory, with the mention of the restricted quantity. We therefore identified three additional constraints: shock, falling, opening. Shock and fall deal with any shock, falls occuring to the product, pallet or container, which might damage the product. Regarding opening, it refers to any attempt to product theft with the opening of container or packaging.

FIG 2. summarizes identified constraints per ICPE classification. Those constraints are meant to be monitored by sensor nodes.

1.4 Impacts

In case of accidents along the supply chain, the impact on population safety, and on the environment can be disastrous. We identified three major impacts: fire, gas emission, dispersion of extinction waters.

Depending on its intensity, fire can have more or less serious impact on individual health (e.g., slightly burning to death). In addition, merchandises and their packaging are combustible.

They both have a strong calorific potential. In case of fire, the combustion of stored products would cause an important radiation of heating flux through the other storage areas in the warehouse. Toxic gases are also emitted in case of fire.

Depending on the quantity of emitted gas, the effects on individuals can be lethal. In addition, under the effect of heat, dangerous products can cause the emission of toxic gas such as hydro-cyanic acid, oxides of sulphur. Fire fighters use specific products in order to extinguish fire. Those products (e.g., water plus chemical, powder, foam) contains chemical which aim at either decreasing the heat, or stifling the fire. Nevertheless those products drain polluting products which must not be thrown into the environment (e.g., river). Such incident may cause pollution of ground, underground or surface waters. It is therefore important to handle properly liquids used for fire extinction in order to avoid them to be thrown outside of the building.

Classification	Shock	Falling	Opening	Flash Point
ICPE 1412	X	X	X	13C
ICPE 1432	X	X	X	66C
ICPE 1172	X	X	X	-

FIG.2 : CONSTRAINTS PER ICPE CLASSIFICATION

2. Our approach

2.1 Delegation of tracking and monitoring to sensor / RFID

As depicted in FIG.3, whereas RFID are used for products tracking, sensor nodes can be used at different levels of the supply chain. Depending on the product value, sensor node can be used either at product level, packaging or pallet. In the scope of the RESCUEIT project [1], we have validated this assumption with end users of the project, K+N and the Casino Group. As we are addressing only low valuable products (e.g., household, gardening products), tagging RFID and sensor monitoring is done at pallet level.

Whereas RFID is rather focusing on identification of products (e.g., identification, classification), WSNs (Wireless Sensor Networks) are meant to monitor and control the supply chain environment. To some extent, RFID are not restricted to unique identification of products along the supply chain, but can be associated to information related to the classification, and dangerousness of products. Based on those classifications, and with regards to the regulations (e.g., safety, quality), the handling, storage, and transport constraints are identified. In this context, WSNs are meant to enforce those constraints (e.g., incompatibilities with other products, flash points). Based on the sensed supply chain context at runtime, sensors tend to evaluate mismatches between the constraints defined by regulations and the current context. Any violation of constraint is therefore reported to the supply chain management system as a risk of incident.

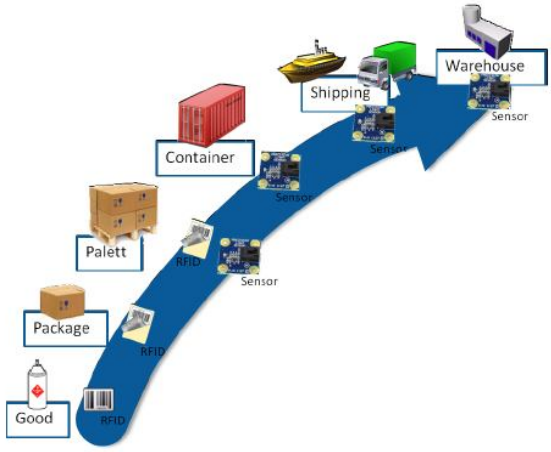

FIG. 3 : DELEGATION OF TRACKING AND MONITORING TO RFIDS AND SENSORS

2.2 Good tracking with RFID

To automate goods tracking along the supply chain, our technical approach defines an RFID-based component that implements the specifications of EPCIS [3] and an RFID middleware. That is, the RFID middleware contains all the information including traceability, and classification for every received or exported tagged good. The EPCIS module is interacting with the whole RFID system (readers, middleware, and external services like other EPCIS). It serves as an interface to the RFID system, by giving access to serialized product information generated by EPC-tagged products and available in the middleware. A large volume of data might be handled by EPCIS.

In our approach, the role of RFID-subsystem is twofold: (i) automatic identification of goods along the supply chain, as made possible by the EPCglobal standard for RFID, (ii) and tracking of tagged goods along the supply chain for sensors to adapt their monitoring mechanisms according to the location and status of the goods (transportation and storage, etc.). That is, each time goods are identified by the RFID system, the RFID middleware reports to the upper-level monitoring the good information including the good EPC identifier, classification, location and status.

2.3 Risk assessment of monitored products

Any disruption of regulation check might jeopardize the execution of the supply chain process. Therefore continuous risk assessment is critical for supply chain management systems.

But, so far, risk assessment has been addressed only locally, within each unit of the supply chain. Meaning that non compliance of previous actor of the process can have a direct or non direct impact of the compliance with regulations. In order to cope with the disruption of risk assessment at the execution of the supply chain process, we propose to delegate risk assessment to sensor nodes attached to the products. Empowered with monitoring capabilities, wireless sensor nodes can evaluate continuously, and at runtime, the compliance with regulations. Sensor nodes are therefore capable of continuous evaluation of any mismatch between product's context and the constraints defined by regulations. To that extend, they support us with early detection of risks.

As depicted in FIG.4, our approach is organised around the four following steps: (i) constraints extraction, (ii) node configuration, (iii) in-node risk evaluation, and (iv) nodealerting. At (i) constraint extraction, constraints over product classification and supply chain activity are defined. For that purpose, regulations (e.g., safety, quality) are evaluated in order to extract per asset classification (e.g., chemicals, food), and per supply chain activity (e.g., transportation, storage) a set of constraints. For efficiency reasons, this task is meant to be performed outside of the node. At (ii) node configuration, the identified constraints are therefore pushed to sensor nodes attached to assets. Once pushed on nodes, those constraints are evaluated in real time by the sensor nodes during the (iii) in-node risk evaluation step. Whenever a sensor observes a mismatch between the current context and its set of constraints, it triggers an alert ((iv) node alerting).

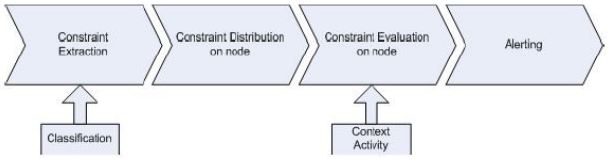

FIG. 4 : SENSOR BASED RISK ASSESSMENT

2.4 Confidentiality of the trace and monitoring with secure Tracker

We propose a secure and efficient product tracking mechanism based on wireless sensor nodes. In that context, sensor nodes are use as secure storage of the product trace. The product trace is composed of a sequence of steps. Each step is defined as a tuple ´Action, Actor Identity´. An Action describes any action performed at a given step on the product, such as upload in a truck, storage on rack. The Actor Identity provides information on the entity performing the Action.

In order to provide a secure and efficient solution for product tracking, we have to address the three following requirements:

- Battery and memory efficiency

  Wireless sensor nodes are considered as resource restricted device. To that respect, our solution has to be efficient, battery and memory wise. Our solution has to provide a mean to optimise battery and memory consumption on the nodes. Battery wise, we aim at reducing processing on the node; while memory wise, we propose to compress the trace. As the trace is composed as a sequence of steps, we provide a mean for compressing the set of steps.

- Actors privacy

  In order to preserve the actors privacy, the steps have to be kept secret. Encryption appears to be a straightforward solution in order to preserve the confidentiality of the information stored on the sensor nodes. We therefore propose to store in the sensor node a sequence of encrypted steps.

In addition, in order to avoid any malicious update of the trace, actors have to authenticate themselves, to the sensor nodes. Actor authentication is therefore our third requirement for our solution. To that respect, we place ourselves in a semi honest model. We assume that all the actors are trusted, and are not meant to send fake, or corrupted steps to the sensor node.

2.4.1 Overall approach

As depicted in Fig. 1, our approach is decomposed in three main phases: (i) initialisation, (ii) trace update, (iii) trace verification. In addition, a trusted entity, the supply chain manager, is in charge of the overall process. The supply chain manager is the only entity to be able to decrypt the stepIDs (see "actor privacy" requirement).

At initialisation phase, our supply chain manager distributes encrypted steps to each actor of the supply chain (see "actor privacy" requirement). We denote the encrypted steps as stepID in this paper. In addition, the supply chain manager initialises the product trace on the node with an initial stepID. The latter is mapped to the step "node initialisation", "supply chain manager". Then the node is attached to the product to be tracked.

At update phase, the sensor nodes is updated with a stepID, mapped to the current action performed an actor. For example, when the freight forwarder uploads the product in a truck, he/she sends the stepID mapped to this action to the nodes. For the trace update on the node, the actor has first to authenticate himself (see "actor authentication" requirement). Once the actor's authentication is performed, the actors pushed to the node a stepID. The latter is encrypted (see "actor privacy" requirement). In addition, in order to optimise sensor memory, the product trace is compressed on the node.

At verification phase, the supply chain manager retrieves the trace from the node, and checks that the product went through all the steps of the supply chain

process. In case of an accident, it enables the supply chain manager to check the stored stepsIDs before the incident.

The main features of the suggested product tracking scheme are as follows:

- It guarantees the non disclosure of trace information to non authorized entities. To that extent, it preserves actors' privacy at the execution of the supply chain.
- Supply chain manager is authorized to verify the legitimacy of the path taken by a product at anytime at the execution of the supply chain. More precisely, it allows the supply chain manager to verify the overall step sequence for a tracked product.

2.5 Access Control to product tracking and monitoring

We define an access control to track and monitor products within the supply chain. Firstly, we split our scenario into several flows concerning the importation of goods from China to Europe. The different flows are listed below:

- Transport between the manufacturer and Shanghai harbor,
- Transport between Shanghai harbor and Chinese territorial waters,
- Transport in international waters,
- Transport by road in France,
- Transport between Le Havre harbor and Kuehne & Nagel warehouse,
- Internal flows in Kuehne & Nagel warehouse,
- Transport between Kuehne & Nagel warehouse and Casino.

For each flow, we built a matrix of access control. In rows of this matrix, we have the different constraints and risks to be monitored. There are some risks which are a combination of events. For example, fluid leakage is the combination of pallet squashing, overturning, shock and of box opening. In column, we have the actors of the studied supply chain. Depending on the risk, alerts content is specific for each actor. There are five types of information that could be disseminated:

- Geolocation,
- Nature of product,
- Incident of transport,
- Potential consequences,

Alert content

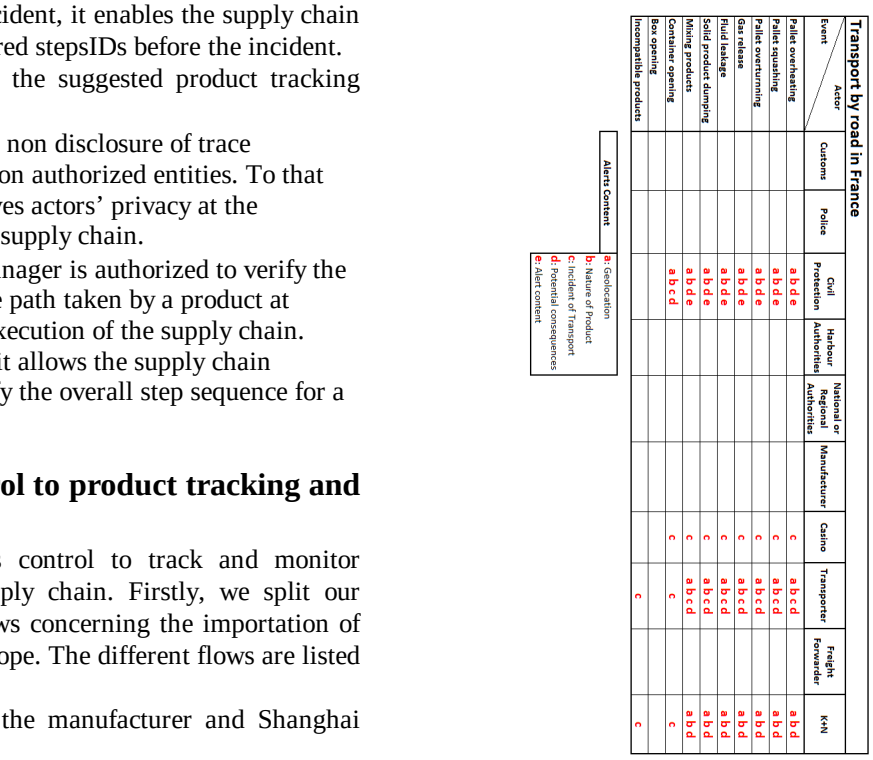

FIG 5. ACCESS CONTROL MATRIX FOR THE TRANSPORTATION OF DANGEROUS GOODS BY ROAD IN FRANCE.

On FIG 5., we can see for example that in case of pallet squashing, the Kuehne & Nagel warehouse only receives the following information: the nature of the product, its geolocation and the potential consequences of the incident. On the contrary, for the same incident, Casino will only receive an alert that notify the incident of transport.

3. Prototyping

3.1 Architecture

FIG. 6 depicts our overall architecture. It is organized around three layers: supply chain management, mediation layer, and RFID and wireless sensor networks.

Supply chain management systems aim at monitoring assets along the execution of the supply chain. They have to be alerted in case of any incident which might disrupt the supply chain process. In our case, we use the container tracking system from SOGET.

A mediation layer finally eases the integration of RFID and sensor nodes with supply chain. MDI is a mediation layer developed by SAP Research for the integration of smart items (e.g., WSNs, RFID) into business applications. Based on an OSGi Service Platform, MDI is an agent-based middleware which enables both monitoring and controlling of smart items.

Finally, we use sensor nodes for monitoring and for secure storage of the product trace, while product tracking is supported with RFID tags.

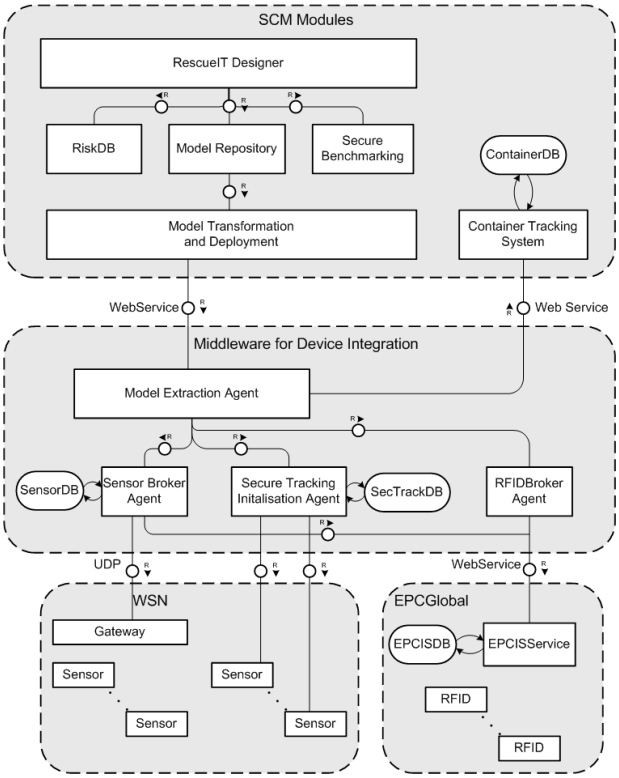

FIG. 6: OVERALL ARCHITECTURE

3.2 Message Flow

In the scope of our collaboration with the German consortium of the RESCUEIT project, a model of the supply chain is generated by the RESCUEIT Designer. It contains the required set of information for the configuration of product tracking and monitoring.

The model transformation and deployment extracts from the model the following information: (i) supply chain process id, (ii) a set of physical steps, (iii) the classification of the supplied product, (iv) a set of access control rules on tracking and monitoring information.

The model extraction agent collects the required information for the configuration of monitoring and tracking on RFIDs and sensor nodes.

First of all, the processID and the set of access control rules are pushed to the container tracking system. The latter generates a container tracking demand, and configure it dynamically with the defined access control rules.

Sensor nodes are programmed based on the classification of the supplied product. Based on the product classification, a set of constraints is extracted from SensorDB. A sensor attached to the product is programmed with this set of constraints. Whenever a constraint is violated, an alert is triggered to the container tracking system.

An EPCIS service is in charge of the mapping between the product and the attached RFID. The set of physical constraints and the supply chain process ID are mapped to the EPCIS service. Each time a RFID device is tagged, a notification is sent to the container tracking system.

Finally, the secure tracking mechanism is initialized with the set of physical steps, and potential alerts triggered by the sensor node attached to the product. Each time an alert or a new physical step is triggered, the secure tracker agent is notified. As new trace stored on the node is updated.

At the execution, any alert from the sensor nodes, or physical steps updates are pushed to both container tracking system and to the secure tracking agent. By this mean, the container tracking system can check the validity of the trace at any time. The secure tracker agent enables the verification of the trace, by extracting and generating a trace for the container tracking system.

4. Conclusion

We've proposed in this paper our approach for a secure supply chain management system. With the integration of sensor networks and RFIDs, we enable the supply chain actors with real time tracking and monitoring of products. In addition, we propose a set of security mechanisms ensuring the confidentiality of the product related information at the execution of the supply chain process. Those mechanisms are all integrated into a joint prototype with our French German partners.

Mobility of supply chain actors is foreseen as future activities for this project. In order to optimize reaction time of supply actors in case of incident, we propose to empower end users with mobile generation of supply chain process, together with tracking and monitoring. Mobility of supply chain actors introduces new security challenges related to the confidentiality of delivered information.

Références

[1] L. Gomez, M. Khalfaoui, E. El-Khoury, C. Ulmer, J. Deutsch, O. Chettouh, O. Gaci, H. Mathieu, E. El-Moustaine, M. Laurent, H. Schneider, C. Daras, and A. Schaad, "Rescueit : securisation de la chaine logistique orientee service depuis le monde des objets jusqu'a l'univers informatique," Workshop Interdisciplinaire sur la Securite Globale, 2011.

[2] Casino. [Online]. Available: http://www.groupe-casino.fr/

[3] E. C. Agency, "Guidance for identification and naming of substances under reach," 2007.

[4] DGDDI, "Direction des douanes et droits indirects,approved economic operator," 2005. [Online]. Available: http://www.douane.gouv.fr/page.asp?id=3421

[5] IPCE, "Installation classifiee pour la protection de l'environnement," 2010. [Online]. Available: http://www.installationsclassees.developpement-durable.gouv.fr/

[6] UNECE, "United nations economic commission for europe, recommendations on the transport of dangerous goods - model regulations," 2005. [Online]. Available: http://www.unece.org/trans/danger/publi/unrec/12e.html