BRIDGE

Newsletter - January 2008

BUILDING RADIO FREQUENCY
IDENTIFICATION SOLUTIONS
FOR THE GLOBAL ENVIRONMENT

Welcome to the BRIDGE Project Newsletter !

This newsletter is published every two months to keep you updated on the happenings within the BRIDGE project. Each edition contains topical information arising from the various Work Packages within BRIDGE as well as other BRIDGE related information.

In this issue, updates are provided on:

- WP3 - Serial-Level Supply Chain Control
- WP5 - Anti-Counterfeiting
- Agenda of events
- Agenda of the upcoming Webinars
- About the BRIDGE project

Any feedback or questions contact emilie.danel@gs1.org

BRIDGE

Information Society Technologies

WP3 - Serial-level Supply Chain Control

by Mark Harrison (University of Cambridge)

The main aim of this work package is to encapsulate information from the EPC Network, analyse the information and utilise it to enhance existing supply chain business processes and/or decision-making processes.

The previous edition of the BRIDGE newsletter provided an introduction to Discovery Services and an update about the work that WP2 has recently completed in terms of requirements gathering, technical design and evaluation and most recently, development of a software prototype of a Discovery Service, which will be made available to all work packages within the BRIDGE project for use within the pilot and trial activities.

WP3 – providing tools for enhanced serial-level track and trace

This article provides an overview and update about WP3, which focuses on enhanced track and trace models for serial-level control. WP3 has already published a document describing a theoretical model for enhanced track and trace capabilities at serial level and is currently working on converting this design into a working software prototype that can be used in the various pilot and trial activities of the BRIDGE project. The WP3 software will provide more user-friendly integration to applications, together with a number of convenient track & trace functions, including the ability to gather EPCIS events from across the whole supply chain or lifecycle, as well as enhanced track & trace information derived from event data that has been enhanced using probabilistic algorithms to analyze historical event data in order to 'learn' flow patterns.

Automated data capture technologies such as RFID are not 100% reliable; there can be false negative observations, in which a reader fails to detect an object that is within its proximity; likewise there can be false positive observations, in which a reader reports the observation of an object that was not within its vicinity, perhaps because the tagged object happened to be next to another reader, so that the tag was effectively receiving power from both readers and could temporarily be read at a distance beyond its usual read range.

In many applications, RFID provides advantages over optical barcodes, since it does not rely on line-of-sight to the tag and can often eliminate the need for manual scanning of each individual object. However, there is a danger that occasional unreliability of RFID data capture and the reduction of human interaction and supervision can lead to more serious errors and wrong decisions.
For this reason, BRIDGE WP3 is developing enhanced serial-level track and trace models that gather the relevant event data from across the supply chain, then use probabilistic algorithms and machine-learning techniques to refine the raw event data, to provide more reliable information to business applications.

Furthermore, WP3 is developing an additional application programming interface (API) layer above the envisioned EPCglobal Network Architecture, in order to provide business people with a more convenient way of making use of the EPC Network to answer business questions, such as tracking of shipments, identifying where delays and deviations are happening and also providing them with predictions about when objects will reach their intended destination – or the probability that they will arrive by a particular deadline.

WP3 - bridging the gap between the EPC Network architecture and business applications

The current EPCglobal Network Architecture is primarily concerned with the processing of event data and the use of standard interfaces to enable exchange of information among multiple organizations about uniquely identified objects.

Figure 1 illustrates the various layers of the EPC Network and how the work of WP2 and WP3 extends this to interface more seamlessly to business-level queries and applications.

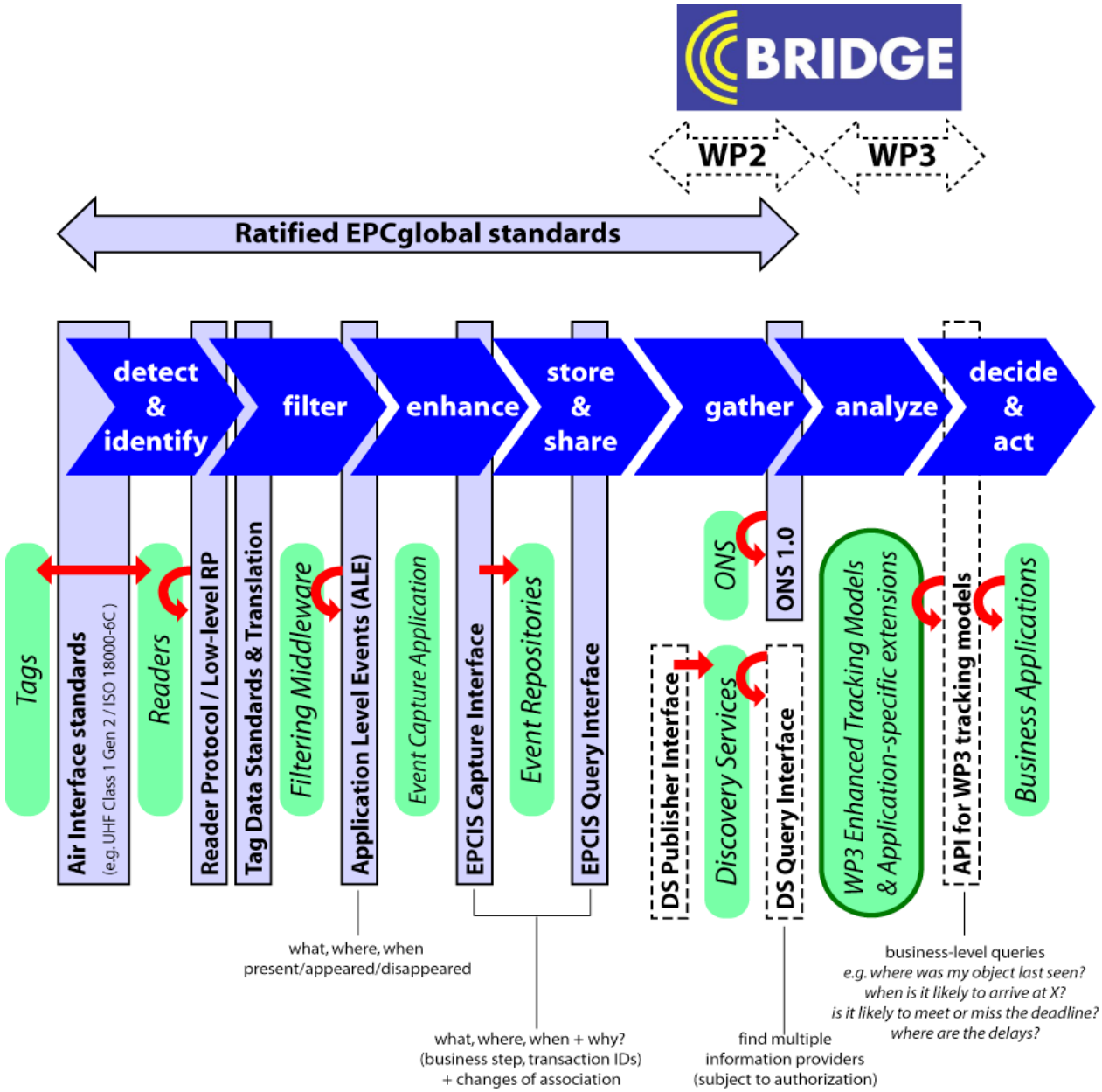

Figure 1. EPCglobal architecture and extensions being developed by BRIDGE WP2 and WP3.

Probabilistic tracking algorithms developed in WP3

The first public deliverable (D 3.1) from BRIDGE WP3 describes the theoretical models and design in further detail. Locations across the supply chain, including hierarchical sub-locations within each organization are represented as nodes on a user-definable graph and recorded as a configuration within a relational database table. Historical event data is gathered either via single one-off queries to Discovery Services and multiple EPCIS repositories – or else continuously, via standing query subscriptions. The event data is then analysed and used to update database tables that record statistics about the transit times between nodes and the branching probabilities of an object of a particular class or type moving from one node to another. A state transition model represents the partial probabilities of an object changing from one state (e.g. location) to another. A sensor model represents the partial probabilities that an object is in a particular state (e.g. location) given a particular observation. This is illustrated in Figure 2,

A number of algorithms, involving first order Hidden Markov Models are used iteratively with these models, in order to filter and smooth the data, as well as predicting the current and future location of objects and the individual path that an object is most likely to have taken.

This information processing combined with further analysis and the use of user-definable 'rules' enables the detection of delays and unexpected behaviour, such as diversion and deviation from expected routes.

The initial theoretical framework is currently being developed as an extensible software prototype and will be tested against real data gathered from pilot activities involving the tracking of individual objects across multiple organizations. An example of such an activity is the pharmaceutical traceability pilot within BRIDGE WP6.

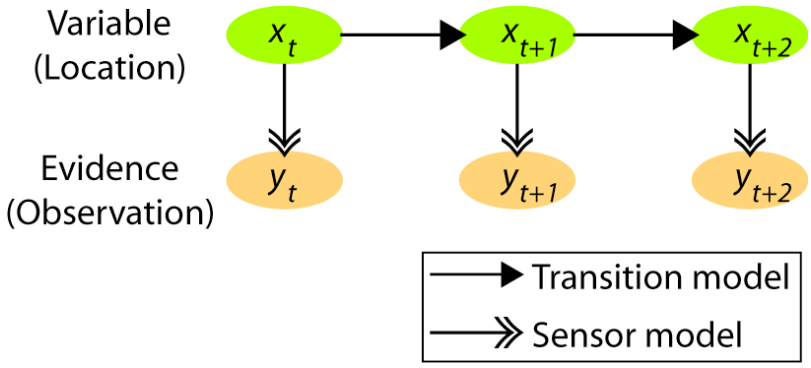

Figure 2 – The sensor model relates the state variable x to observed evidence y, while the transition model expresses the sequence of transitions over time.

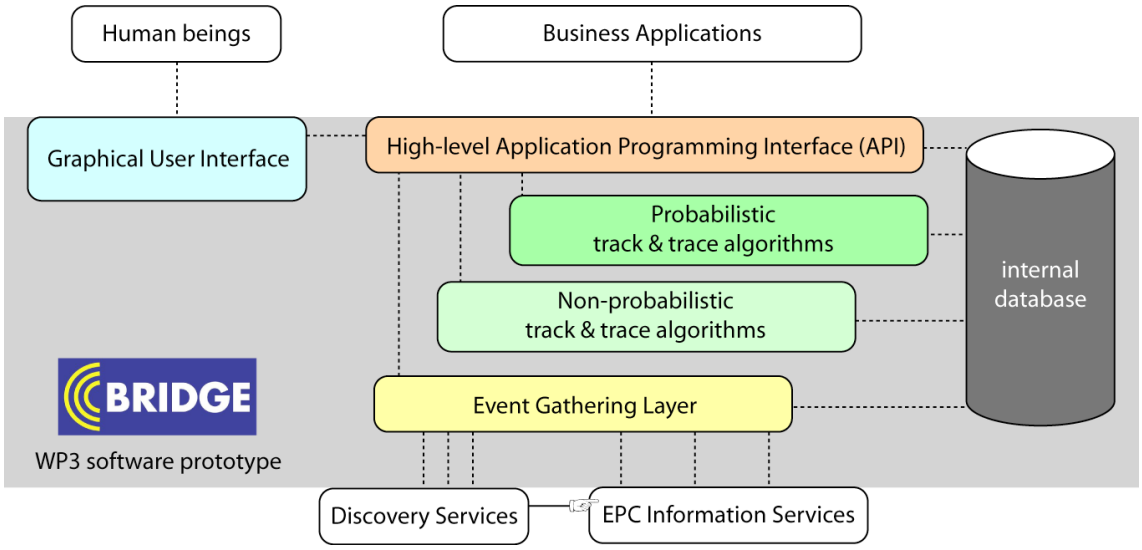

Figure 3 – modular design of the software prototype from BRIDGE WP3

WP3 Software Prototype for enhanced track & trace – now under development

Figure 3 shows the modular design of the software prototype, which will include an event gathering layer that interfaces to multiple EPCIS and Discovery Services, an internal database, algorithms for both non-probabilistic and probabilistic track & trace queries, a high-level application programming interface (API), as well as a graphical user interface.

The high-level application programming interface (API) to the enhanced tracking models will allow business applications to make requests or set rules at a high level of semantics, while the API takes care of co-ordinating the required data collection and choreography of algorithms to process the event data into meaningful information. For example, it will be possible to set rules through the API to monitor a shipment and raise an alert if a shipment is unlikely to reach its destination before the expected deadline or if its condition has deteriorated to an extent where it is no longer usable.

The graphical user interface will provide business people with visual tools to map out their supply chain, while also providing a 'dashboard' visualization of where objects are, where delays, deviations or other problems are occurring, in order that human supervisors can be alerted to any significant problems and can take corrective action.

Further extensions to the model and software prototype are envisaged during the remainder of the BRIDGE project, in order to adapt the model for use in the manufacturing sector, for use with returnable transport items such as pallets, roll-cages and trolleys, as well as integration of sensor data for monitoring the condition of objects throughout the supply chain or throughout their lifecycle.

WP3 includes members of the following organizations: Auto-ID Labs (Cambridge), ETH Zürich, BT, SAP and Bénédicta. The WP3 prototype is currently being performed as a collaboration between Cambridge, BT and SAP.

For more information on this topic, contact:
Mark Harrison
(Auto-ID Labs Cambridge, WP3 leader)
Tel: +44 (0)1223 338178
E-mail: mark.harrison@cantab.net

WP5 - Anti-counterfeiting

by Oliver Kasten and Jasser Al-Kassab (SAP)

The objective of this work package is to secure the licit supply chain from counterfeit products. To this end, we are developing a software solution based on RFID and EPCglobal standards. It allows supply-chain partners to collaborate, making it much more difficult for illicit actors to introduce counterfeits into the supply chain, while at the same time increasing their risk of being discovered as well as reducing their profit margins.

Background

Counterfeit products can endanger the health of individuals and damage companies' brand images. While counterfeit medicine and luxury watches are featured most prominently in the media, today virtually all kinds of products are affected by counterfeiting. Despite common belief, counterfeit products are not only sold through the Internet and sales booths in holiday destinations. In fact, even in Europe large numbers of counterfeits find their way into licit distribution channels. That means that counterfeits could end up on the shelves of your favourite retail store just around the corner. In Switzerland, for example, counterfeits of high-priced branded perfume made it into the country's largest supermarket chain[1].

Figure 1
Counterfeit and genuine SD memory card

[1] http://www.migrosmagazin.ch/index.cfm?id=17144

[2] D5.2 Anti-Counterfeiting requirements Report, available at http://www.bridge-project.eu/

Anti-Counterfeiting Challenges

Counterfeiting has been recognized as a problem not only by the affected companies, but also at national and international levels. Today several technical approaches exist to distinguish counterfeits from genuine products. Though highly effective in making this distinction, these techniques are generally not sufficient to stop counterfeiting. Because they require human intervention, they are typically very costly and time consuming, effectively representing a bottleneck in today's fast supply chains. As a consequence, many supply chains cannot afford more than sporadic testing in a few selected locations. Even customs can only test a small percentage of all products entering European boarders (for example, around 5% in Switzerland[2] and 5-8% in Germany). Sporadic testing cannot prevent counterfeits from entering the licit supply chain, nor is it sufficient to pinpoint counterfeiters and their accomplices. As a consequence, illicit actors can still expect high profits while facing a low risk of being detected and prosecuted.

WP5 Goals

Work Package 5 in BRIDGE aims to develop a technical solution that protects the licit supply chain by making it much harder (albeit not impossible) to introduce counterfeits in a protected supply chain, while at the same time increasing the illicit actors' risk of detection as well as by reducing their profit margin. A key factor in our solution is that it allows the licit supply-chain partners to cooperate in order to lock out illicit actors or, at least, to make illicit behaviour unattractive.

Detecting Counterfeits based on Product Traces

The basic idea behind our approach is to individually trace all products throughout the supply chain using passive RFID technology and EPCglobal standards. At each step in the supply chain, every product's individual trace is automatically analyzed for anomalies and deviations from normal patterns. If anomalies are detected, the products in question are subjected to physical counterfeit testing using traditional approaches. This solution can easily and effectively prevent many counterfeits from entering the licit supply chain by detecting and locking out products with suspicious traces. Only products with valid EPCs and normal traces can pass.

Our solution requires each product to be uniquely identifiable, typically by attaching an RFID tag to it. As the products move through the supply chain, each partner reads the products' EPCs and stores them for analysis by an entitled authority. This authority may be the brand owner, customs, or a trusted third party, such as an anti-counterfeiting alliance. Our approach allows to easily detect anomalies that indicate counterfeit insertions, for example, two or more products carrying the same (i.e., duplicate) EPCs, products carrying EPCs that have not been assigned to products or that belong to products that have been sold already, and other suspicious product traces in general.

An Airtight Solution?

Though we cannot entirely prevent counterfeit insertions, our solution makes it much less attractive. In fact, counterfeits can only be injected if they carry an RFID tag that is indistinguishable from a valid tag. Creating two indistinguishable tags can be achieved by tag cloning, that is, copying a valid EPC from one tag to another, rendering two tags with the same EPC. Even in the protected supply chain, an illicit actor can replace original products by counterfeits that carry RFID clones of the originals.

[3]Anti-Counterfeiting Requirements Report, http://www.bridge-project.eu/

But since the protected supply chain detects duplicate EPCs, an illicit actor could only pass on *either* the counterfeit *or* the original product, but never both. Therefore, the only way for an illicit actor to realize a profit out of counterfeit insertions is to sell the original products to illicit, unprotected markets, were no product traces are recorded. Such markets are likely to render less profit and may require more effort. In the trade-off between risk, profit, and effort, protected supply chains become much less attractive to illicit actors.

Customizable Rules Provide Flexibility

Above we have described several anomalies (such as invalid and duplicate EPCs) that trigger physical counterfeit testing and possibly investigation. Though these tests are standard elements in our solution, they are not hardcoded into it. Rather, each test (and its potential reaction) is specified as a separate rule in a rule-description language. Existing rules can be modified and new rules can be created on the fly. This provides a great deal of flexibility, which is required to adapt to the ever-changing strategies of counterfeiters. It also allows customized tests using business-knowledge specific to the industry, product types, and supply-chain partners at hand. This is a key requirement, since supply chains as well as the behaviour of counterfeiters differs significantly depending on these factors[3].

In addition to supporting user-configurable rules, we investigate machine-learning techniques to automatically generate near-optimal rules for the detection of cloned products. To achieve this goal, we have statistically analyzed product traces to find out which factors determine the reliability of clone-detection rules. When the intended supply chain is suitably modelled and the locations of products are accurately known, cloned products can be detected yet more reliably. Since in the future, EPC and RFID technologies will improve supply-chain visibility and the accuracy of logistics data, they will simultaneously provide companies with better means of protecting their distribution channels from counterfeit products.

WP5 Prototype Status

WP5 has started implementing the anti-counterfeiting software and will deliver an initial demonstrator around April 2008. Our solution is based on passive RFID technology and existing as well as emerging EPCglobal standards. Concretely, we will build largely on EPC Information Services and will leverage results from BRIDGE Work Packages 2 (Discovery Service), 3 (Track-and-Trace Infrastructure), and 4 (Security). Additionally we are in close collaboration with the SToP EU project (Stop Tampering of Products)[4]. We are currently setting up the basic infrastructure required for collecting and accessing product-trace data in supply chains. We have finished evaluating rule representations and rule-execution software. Several anti-counterfeiting rules have already been implemented and tested on a small scale. We are currently approaching the pilots within BRIDGE to obtain real-life trace data in order to evaluate the prototype and confirm the initial results.

[4] http://www.stop-project.eu

The WP5 team in alphabetical order: Jasser Al-Kassab, Ali Dada, Erica Dubach, Oliver Kasten, Mikko Lehtonen, Florian Michahelles, Nina Oertel, and Thorsten Staake.

Conclusion

The WP5 anti-counterfeiting solution, which builds on existing EPCglobal standards, can help protecting supply chains. It does so by effectively preventing large-scale injections of counterfeits and by significantly reducing the counterfeiter's profit margin, while increasing its risk at the same time. Our solution is intended to be practical and efficient, but—of course—cannot guarantee the complete absence of counterfeits in licit supply chains. With our solution in place, counterfeits can only be introduced as a one-to-one replacement of original products. The profit that an illicit actor can realize by introducing counterfeits into the protected supply chain is determined by the profit of selling the genuine product on the illicit market (minus the cost of acquiring/producing the counterfeit). This is much less attractive compared to the situation before (i.e., in the unprotected supply chain), where illicit actors could sell several counterfeit copies plus the original product.

==========

Since the start of the BRIDGE project, WP5 has prepared three reports: D5.1 Problem-Analysis Report on Counterfeiting and Illicit Trade (Dec 06), D5.2 Anti-Counterfeiting requirements Report (Apr 07), and D5.3 Business-Case Report (Dec 07). D5.1 and D5.2 are available and D5.3 will soon be available on the public BRIDGE website http://www.bridge-project.eu/

For more information on this workpackage, please contact:
Oliver Kasten (SAP, WP5 leader)
Tel: +41-58-871-7840
E-mail: oliver.kasten@sap.com

CALENDAR OF EVENTS

6th Annual Global RFID-ROI Summit 2008
29-30 January 2008
Munich, Germany
http://www.rfid-roi.com/

BRIDGE representatives Henri Barthel (BRIDGE coordinator, GS1), Otto Url (Norhtland), John Jenkins (JJ Associates) and Paul Roberts (Nestle) will be presenting the BRIDGE project's progress on the second day of this major RFID event.

RFID Smart Labels USA 2008
20-21 February 2008
Boston, USA
http://rfid.idtechex.com/rfidusa08/en/

CeBIT Forum 2008
4-9 March 2008
Hannover, Germany
http://www.cebit.de/homepage_e

Internet of Things 2008, International Conference for Industry and Academia
26-28 March 2008
Zurich, Switzerland
http://www.internet-of-things-2008.org/

Interoperability Conference
6 & 7 February 2008
Warsaw, Poland
http://www.interoperabilityconference.org/Homepage.htm

Project coordinator Henri Barthel will present BRIDGE in a session on RFID standards

RSA Conference 2008
7-11 April 2008
San Francisco, USA
http://www.rsaconference.com/2008/US/home.aspx

WP4 on Security will be presented at this conference

RFID Journal LIVE! 2008
6th Annual Conference & Exhibition
April 16-18, 2008
The Venetian Resort Hotel * Las Vegas
http://www.rfidjournalevents.com/live/

RFID Journal LIVE! Europe 2008
4th Annual Conference & Exhibition
Nov. 3-5, 2008 * Clarion Congress Hotel * Prague
http://www.rfidjournalevents.com/liveeurope/

Agenda of the upcoming Webinars

Would you like to learn more about the BRIDGE project?
Attend our Webinars where the project partners present their work and progress

Webinars are seminars that you can attend from home or from your office. All you have to do is call the conference call number and go to the website address that will be given to you once you register.
You will then be able to follow the presentation directly on your computer and hear the speaker on the phone.

23 January 2008 - 11:00 CET
Presentation of the Portable Demo
Speaker: Michal Grabia, GS1 Poland
Work Package 13 - Dissemination & Adoption Tools

06 February 2008 - 11:00 CET
Speaker: Oliver Kasten, SAP, WP5 leader
Work Package 5 - Anti-Counterfeiting Business Application

20 February 2008 - 11:00 CET
Speaker: Miguel Angel Guijarro Moreno, AT4wireless, WP2 leader
Work Package 2 - Serial-Level Lookup Service

5 March 2008 – 11:00 CET
Speaker: Jean Marc D'Hooghe, GS1 Global Office, WP12 Leader
Work Package 12 - Overview of the BRIDGE Training material

If you would like to attend one of these Webinars, please contact us at **webinar@bridge-project.eu** to register. We will then send you the necessary access information.

****

ABOUT THE BRIDGE PROJECT

BRIDGE is a European Union funded 3-year Integrated Project addressing ways to resolve the barriers to the implementation of RFID and EPCglobal technologies in Europe. The project consists of a series of business, technical development and horizontal activities. Seven Business work packages have been set up to identify the opportunities, establish the business cases and perform trials and implementations in various sectors including anti-counterfeiting, pharmaceuticals, textile, manufacturing, re-usable assets, products in service and retail non-food items. The project includes an important research and development program in various aspects of RFID hardware, software, network and security. A series of horizontal activities will provide training and dissemination services, enabling the adoption of the technology on a large scale in Europe for the sectors addressed by BRIDGE and beyond.

URL
http://www.bridge-project.eu

If you have questions regarding the BRIDGE project contact:
info@bridge-project.eu