Securing disaster supply chains with cryptography enhanced RFID

Gianmarco Baldini and Franco Oliveri
Joint Research Centre – European Commission, Ispra, Italy
Michael Braun
University of Applied Sciences Darmstadt, Darmstadt, Germany, and
Hermann Seuschek and Erwin Hess
Corporate Technology, Siemens AG, Munich, Germany

Abstract

Purpose – Humanitarian logistics is an essential element of disaster management and it presents many challenges due to the unique disaster relief environment. The paper describes the main features and challenges of humanitarian logistics and the potential role of technology. Radio frequency identification (RFID) technology has been increasingly considered to improve the efficiency of supply chain management. Security is an important requirement for disaster management. The purpose of this paper is to propose and describe the application of secure RFID technology to improve the management and security of relief supply chains.

Design/methodology/approach – The paper describes the challenges of disaster of supply chains and how secure RFID can address them in the overall framework of disaster management.

Findings – The paper describes the efficiency of the crypotgraphic algorithm used in the design of the secure RFID, the system architecture and the deployment workflow.

Practical implications – The establishment of a logistics tracking framework based on secure RFID has the potential to greatly increase the effectiveness of future emergency crises response operations.

Originality/value – The originality of the paper is to present the application of secure RFID to the context of disaster management, where the security of supply chains is often not addressed.

Keywords Radio frequency identification, Disaster management, Supply chain management, Distribution management, Emergency response, Natural disasters, Security

Paper type Technical paper

1. Introduction

The management of the supply chain in disaster relief operations is considered an essential element in the resolution of a crisis since the Tsunami in South East Asia (December 26, 2004) and the Katrina Hurricane (August 2005). The scale of these disasters is huge both in geographical size and in severity. The Katrina Hurricane affected 92,000 square miles of land katsize and hundreds of thousands of people were displaced from their homes.

The enormous scale of these disasters has highlighted the need for improving the management of relief supply chains through new organizational procedures or technologies. Supply chains used in disaster management are usually called disaster supply chains or relief chains. Both definitions will be used in this paper. The management of logistics in disaster relief operations is also called humanitarian logistics and it may be quite different from business logistics in many aspects including the operational requirements, the resources and the user needs. Unique and secure identification of items shipped to disaster areas is crucial to guarantee that first responders receive the proper type and quantity of supplies. There have been many

Disaster Prevention and Management
Vol. 21 No. 1, 2012
pp. 51-70

0965-3562
DOI 10.1108/09653561211202700

cases (as in the disaster of the Indian Ocean Tsunami), where boxes of goods were uncoordinated and unmarked (Richardson, 2006). Therefore they were lost, stolen or damaged and they could not be used to bring relief to the victims of the crisis. A nonprofit agency have indicated, in a recent report (Fritz Institute, 2005), that most of the organizations involved in the 2004 Tsunami disaster were lacking in supply chain expertise and technology. The supply chain used in the resolution of emergency crises must have capabilities of agility and flexibility to respond to the challenges, which are typical of these crisis scenarios.

Emergency crises are often characterized by a chaotic environment and by a general lack of infrastructures, which are usually degraded or destroyed because of the severity of disaster. These conditions may delay or impede the supply chain and the delivery of correct equipment and goods to the right places and at the right time. Kovacs and Spens (2007) presents an excellent overview of the specific characteristics of humanitarian logistics in disaster relief operations and the related challenges. Information and communication technologies have an important role in relief chains. Radio-frequency identification (RFID) technology has been increasingly considered as a powerful enabler to improve tracking and tracing in supply chain management. RFID is a device applied to a person or goods for identification and tracking purposes through radio waves. RFID could be used to create a virtual infrastructure, which can be used to track cargo and goods and their delivery. The strategic importance of RFID in supply chain management is described in Tajima (2007), which investigates the potential of RFID to sustain a competitive advantage for supply chain managers in the commercial domain. Even if the paper is not focussed on the application of RFID for emergency crisis supply chains, the benefits for tracking and supply chain efficiency are clearly identified. The major benefits of RFID in supply chain management are also presented in Jungbae Roh *et al.* (2009). Theft reduction is considered the main expected benefit as it translates to cost savings in the commercial domain, while it will be even more important in crisis situation where replacements for stolen goods, may not be readily available. Criminals may take advantage of the chaotic situations to steal relief goods or items from ruined homes or buildings as in the case of Katrina disaster (US House of Representatives, 2006).

Consequently, all the components of the supply chain should be made secure: RFID devices must not be tampered with and they should be resistant to security attacks (e.g. spoofing, eavesdropping and cloning) to ensure that the supply chain is not disrupted by criminals and that cargo and goods are not stolen. In this context, this paper will present the application and benefits of the recent technological breakthroughs in the field of secure RFID. Secure RFID can prevent the tampering or replacement of the shipment through cloning of the RFID. A preliminary investigation on the application of secure RFID for disaster management has also been presented in Baldini *et al.* (2009).

The paper has the following structure: Section 2 describes the features of natural disasters and emergency crises and the main phases (mitigation, preparedness, response, recovery). The specific issues and challenges of humanitarian logistics and relief supply chains are described in Section 3. Section 4 describes the role of RFID in supply chain management. Section 5 provides a description of authentication mechanisms for secure RFID tags. Section 6 shows the overall system architecture. The section also describes how the proposed solution addresses the issues and challenges described in Section 3. Finally Section 7 provides the conclusions and future developments.

2. Disaster management

There are many definitions of natural disaster; if we consider the following definition (Bankoff *et al.*, 2003): "a natural disaster is the effect of a natural hazard (e.g. flood, tornado, volcano eruption, earthquake, or landslide) that affects the environment, and leads to financial, environmental and/or human losses. The resulting loss depends on the capacity of the population to support or resist the disaster, and their resilience," *t* appears clear that what is relevant is the effect of the disaster on the human lives, assets and activities in the affected area.

Natural disasters and emergency crises can have different types of classification based on their features. One main classification is natural and man-made disasters. Natural disasters are the consequences of natural hazards like earthquakes, flooding, avalanche or Tsunami while man-made disasters are caused by human actions (e.g. terrorist attack) or human oversight.

Other taxonomies are based on the predictability of the event. For example, the flooding of a river can be predicted on the basis of the weather conditions. Another classification is based on the severity of the event. An avalanche can affect only a limited geographical area or population while an earthquake can impact a large part of a nation. A pandemic flu can even affect the population across entire continents. Natural disasters can also generate cascade effects. For example, natural disasters can trigger multiple and simultaneous chemical accidents with off-site consequences, can destroy or degrade existing critical infrastructures like electrical power distribution lines leading to blackouts or they can breach dams leading to mudslides and inundations.

Table I provides an overview of the most typical disasters or emergency crises and their features from a qualitative point of view.

Even if natural disasters or emergency crises may have different features, the effects are similar and quite devastating.

A common factor for all these events, is that they create unexpected and extraordinary conditions for the relief actors participating in the resolution of the event. They have to make urgent decisions on the basis of incomplete information and resources, which may remain unavailable for the duration of the crisis (Rosenthal *et al.*, 1989).

Type of disaster	Natural/ man made	Predictability	Potential impact	Geographical extension
Earthquake	Natural	Low	High	Large (national)
Tsunami	Natural	Low	High	Large (multi-national)
Storm/hurricane	Natural	Medium	Medium/high	Large (national)
Vulcanic eruption	Natural	Medium	High	Large
Pandemic disease	Both	Low	High	Large (global)
Terrorist attack	Man made	Medium	Medium	Local
Transportation incident	Man made	Low	Medium	Local
Armed conflict	Man made	Medium	High	Large (multi-national)
Landslide	Natural	Medium	Low	Local
Avalanche	Natural	Medium	Low	Local
Chemical plant incident	Man made	Low	Medium	Medium
Nuclear incident	Man made	Low	High	Large (multi-national)

Table I.
Features of natural disasters and emergency crisis

2.1 Phases of an emergency crisis

Disaster management is usually composed by four different phases (see Figure 1) as described in Miller *et al.* (2006):

(1) Mitigation, which includes the activities needed to prevent the natural disaster, reduce its impact and minimize ensuing losses and damages. For example, the geometry of an hillside may be artificially modified to reduce the risk of avalanches or snow fences are placed in the most critical areas.

(2) Preparedness, which has the objective to prepare the resources or facilities for a response. This include the identification of threats, determine the capabilities of organizations if a disaster strikes, define scenarios for training purposes, identification of main partners like suppliers, identification of critical assets and so on.

(3) Response, which includes those immediate actions taken to deal with a disaster or an emergency. Response activities should have the purpose of mobilizing emergency responders, resources and services for the affected region. In this phases, the coordination among the relief actors is an essential activity.

(4) Recovery, whose objective is to try to restore the disaster area to the state before the crisis. Recovery is a stabilization phase, which may be conducted for the long term.

Each phase has a set of specific activities: coordination, media communication, healthcare, rebuilding and repairing degraded or destroyed assets.

In this paper we focus on the difficult task of supporting an effective and timely delivery of goods where they are needed from the actual event onwards; i.e. we focus on humanitarian logistics and relief supply chains.

3. Humanitarian logistics

It has been proven, over and over again, that in the immediate aftermath of a disaster, as soon as the world community has taken note of the disaster, the logistic of the

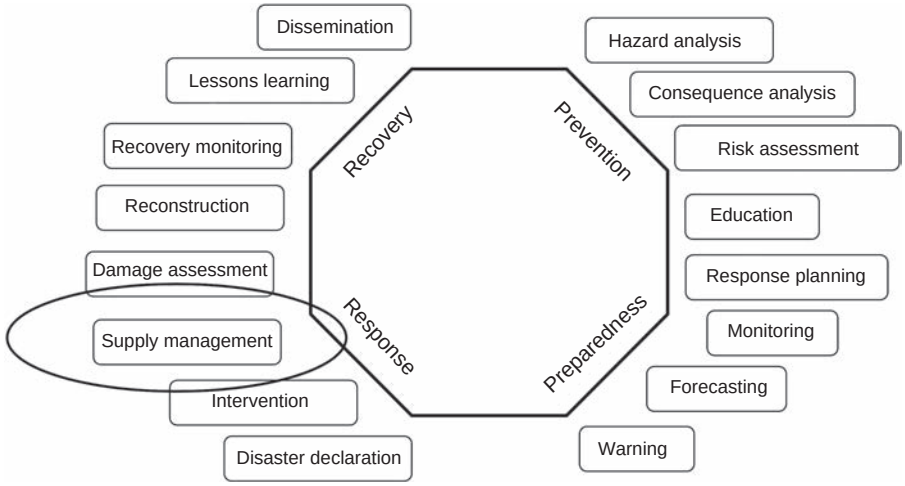

Figure 1.
Phases of disaster management

deployment of people and goods is the key factor to save lives and to mitigate the impact of the crisis. As pointed out in Trunick (2005), logistics efforts account for 80 percent of the overall disaster effort.

A large variety of materials like medicines, food, shelters must be brought to disaster area and the affected people in the shortest possible time.

The role of the logistics and the supply chain has also been highlighted by recent events. In the immediate aftermath of the 2004 Asian Tsunami, relief goods flooded airports and warehouses in the affected regions, aid agencies struggled to sort through, store and distribute the piles of supplies while disposing of those that were inappropriate. In Sri Lanka, the airports were overloaded by the large number of humanitarian cargo flights. At the distribution level, relief agencies struggled to identify warehouses to store excess inventory. Many participants to the relief efforts to the Tsunami disaster, claimed (The Economist Intelligence Unit, 2005) that, logistics and efficient supply chain was more important than a large quantity of goods. Supply chain management for business applications had a long evolution and many companies have well established supply chains around the world but the strategic goal of commercial supply chains and disaster supply chains are different (Cassidy, 2003). Where commercial supply chains are focussed on quality and profitability, humanitarian supply chains must be focussed on minimizing loss of life and suffering.

Supply chain management may be present in all the last four phases of disaster management described above for different reasons and with different roles. In the prevention and the preparedness phase, supply chains are used to stockpile and maintain disaster supplies and equipment, which may be used in disaster management. In these phases, the management of the supply chain is relatively easy as the location of the stockpiling facilities and inventories is well known and the transfer of the materials is planned in advance. In the response phase, supply chains are an essential element in the resolution of the crisis. Depending on the features of the crisis described in Table I, supply chain management can become extremely complex as there are many different players, large quantity of materials to be distributed and degraded infrastructures. Furthermore, there are severe time constraints as people may die if goods (e.g. medicines, food) are not distributed in time. In the recovery phase, relief chains are used to provide support to the rebuilding of destroyed property and the repair of critical infrastructures. This paper will focus on supply chain management in the response phase, without forgetting that to be effective in such phase, some preparation is required.

Kovacs and Spens (2007) presents an excellent overview of the specific characteristics of humanitarian logistics in disaster relief operations. The paper presents a framework, which identifies the actors, phases and logistical processes. The identified actors, which participate to the humanitarian aid supply network are: donors, logistics providers, aid agencies, military, governments and other NGOs. As the paper correctly point out, a significant difference with commercial supply chains is that suppliers have different motivations for participating and customers are not generating a voluntary demand. In relief chains, demand is assessed by the involved government agencies and aid agencies longwood. This is one of the challenges in relief chains.

Figure 2 describes the main participants, which are usually involved in the resolution of a large natural disaster and the related activities: procurement, transportation, local warehousing and local distribution. Military is also usually involved in large natural disasters in most of the activities.

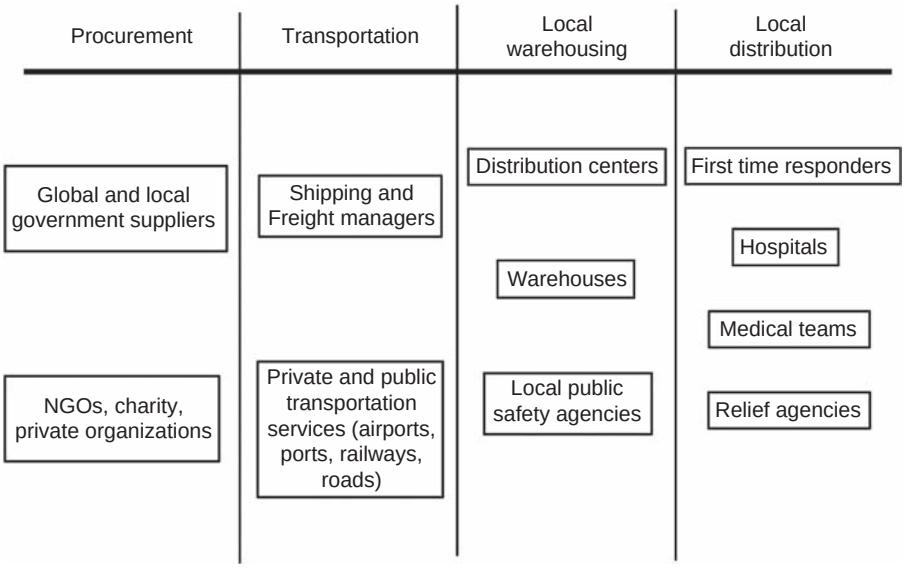

Figure 2.
Participants to the disaster supply chain

Note that some of these actors have different geographical coverage: some agencies are global actors, but there are also regional, national and local aid agencies. Each agency has its own structure and processes. Coordination is one of the major challenges in humanitarian logistics. The next paragraph identifies the main challenges.

3.1 Challenges for disaster supply chain management

As described, the management of disaster supply chains is a challenging task. We can identify the following main challenges:

(1) Size of the relief chain: in large natural disasters, the amount of goods to be moved and transported could be enormous as a wide geographical area and a large population could be affected by the crisis. Typically, thousands of tons of material must be transported and distributed. Transportation centers (like ports, highways or airports) must sustain a flow of goods, which is much higher than their usual capacity (Balcik *et al.*, 2010). Overloaded transportation centers may not only delay the distribution of goods but they may also increase the risk of material, which is lost or sent to the wrong destination. Another reason for the overload in the transportation centers is the provision by donors of unsolicited supplies, which are not necessary for the specific type of disaster. For example, expired food or clothes, which are not adapt to the climate of the area where the disaster occurred (Cassidy, 2003; Murray, 2005).

Even if the supplied goods are correct, they may be provided in forms, which are not easy to identify and manage as described in Murray (2005) due to a number of reasons including the lack of common standards. This is one of the challenges addressed by the present paper through the introduction of technological solutions to identify and trace the relief goods.

(2) Coordination: there are many different partners participating to the resolution of a crisis. Each of the partners has its own set of capabilities and supply chains. Coordination and interoperability at organizational and procedural

level among the partners is necessary to achieve an overall improvement in the efficiency of supply chain management. Balcik *et al.* (2010) describes the importance of coordination in the supply chain during disaster relief operations. The paper identifies and describes the main challenges to achieve a successful coordination in the main phases of the relief chains including procurement, warehousing, transportation and distribution. Traditional coordination mechanism implemented in commercial supply chains may not be feasible or practical for disaster relief operations because of the different environments and operational requirements. The most significant issues identified in the paper are the number and diversity of the actors involved in the disaster, the unpredictability of the events (i.e. natural disaster) and the costs associated to the coordination itself (Stephenson, 2005). Xu and Beamon (2006) identifies three types of cost: coordination cost, opportunistic risk cost and operational risk cost. Another important aspect is the need to create trust among the many organizations presents in the disaster response situation. As described by Tatham and Kovacs (2009), the response phase to a disaster brings together organizations with their pre-fixed aims and policies, different levels of security (e.g. military, NGOs) and training.

(3) Degradation of critical infrastructure: essential critical infrastructures like transportation, energy and communications may be degraded or destroyed. This aspect is described in Kovacs and Spens (2009). The degradation of the transportation infrastructure has a negative impact on the delivery of the needed goods. In natural disaster, the "last mile" is usually the problem. The degradation of communications infrastructure has a negative impact on the level of coordination and cooperation among the partners participating to the resolution of the crisis. We should also consider the dependencies among critical infrastructures: transportation and telecommunications infrastructure are mostly dependent on the energy infrastructure. Note that the degradation of the infrastructure may also due to an overload of its capacity. In the case of the "London bombing," the communication infrastructure (GSM/UMTS) was inoperable for first time responders because of panic conditions by the population.

(4) Timing: time constraints are very severe. Perishable items like food or medicines must be distributed in time otherwise they are not useful and may increase the risk of casualties and epidemics (Murray, 2005).

(5) Security: criminals like thieves and looters may take advantage of the chaotic environment to steal goods or to disrupt the supply chain to their advantage (Cassidy, 2003; Constable, 2008). In a natural disaster, the goods (medicines, food) brought by aid agencies and relief organizations are even more valuable because of their scarcity. In all disaster situations, there is the potential for loss through theft at all levels of the supply chain, and control systems must be established and supervised at all storage, hand-over and distribution points to minimize this risk. Even more dangerous of simple thieving is tampering: the use of unreliable medicines or rotten food can further endanger the life of the survivors, therefore it is crucial to be able to keep track of the origin of the goods along each step of their delivery. Security of the relief chains is an important requirement in humanitarian logistics.

(6) Demand: as indicated in the previous paragraphs, relief chains represent the links between the supply and the demand. In this type of events, the demand cannot be easily predicted and it is continuously fluctuating based on the incoming reports from the field (Beamon and Benita, 2004).

The secure tracking solution presented in this paper primarily addresses the challenge of ensuring the security of the relief chain to prevent loss/mismanagement of goods through theft and tampering. It also provides the benefits to increase the trust among the organizations involved in the disaster response, improves the efficiency of the supply chain and support the management of large volume of relief goods.

4. RFID in disaster supply chain management

4.1 Role of technology in disaster supply chain management

Technology can be essential in improving disaster supply chain management and in providing more capabilities to the partners involved in the resolution of the crisis. Long (1997) highlights the importance of importance of information technology to improve the resolution of a disaster. A number of technologies have been presented in literature for disaster management. They include decision support systems, fast deployable communications, sensor networks, remote sensing and tools to support warehousing and supply chain management.

One of the basic ingredients of supply chain management is information. Supply chain managers need to know what is the demand of the goods, where they are located at any time, when and where they will be shipped and so on. These tasks are already complex in a generic commercial supply chain, but in disaster supply chain management they become even more difficult because of the challenges described in Section 3.1.

An essential element is the proper identification of the goods and the distribution of this information to all the involved partners. In natural disasters, goods may come from any types of sources, because aid agencies are sometimes not equipped to tag the material in the proper way. Autier *et al.* (1990) discusses the case of drug supplies, after the 1988 Armenian earthquake, when at least 5,000 tons of drugs were sent by international relief operations but only one-third was usable because it is was properly identified, relevant for the emergency situation and distributed in time. One-fifth of the supplies had to be destroyed at the end of 1989.

Security is one important requirement for the technologies used in disaster management. Sensitive data may be distributed among the coordinators of the relief operations. As described in Section 3.1, criminal entities may take advantage of the chaotic conditions to steal or redirect goods to the wrong destination. The information present in the supply chain management systems must be secured and protected so that it cannot be used for criminal purposes. Technology can improve the secure access and distribution of information in a number of ways.

One technology, which has recently gained wide acceptance in supply chain management is RFID. There is already an extensive literature on the use of RFID in commercial supply chains. Sarac *et al.* (2010) provides a recent overview of the application of RFID in commercial supply chains. There is a very limited number of papers, which propose the application of RFID technology for relief chains or support to disaster management. A recent paper is Yang *et al.* (2010), which describes the design of an hybrid RFID sensor network architecture for humanitarian logistics center management. The presented design provides important features for

humanitarian logistics including improved resilience, fast deployment and low power consumption but the paper does not address security issues.

4.2 Secure RFID in disaster supply chains

Tags, a reader/writer and a host system compose a typical RFID system. An RFID tag is usually of very small size and low-cost device, so that it can be easily implanted on a physical object like a product, a box or even an animal or a person. An RFID tag is composed by tiny electronic circuits able to store and process a limited amount of data (from several bits to several kilobytes) and by a miniature antenna for short-range wireless communication.

RFID tags are classified as passive or active. Passive tags work by taking the energy received from the reader through the tags antenna and using that energy to transmit stored data back to the reader. Passive tags are less expensive than active tags, which include their own power supply, usually a battery, to transmit information directly to a reader. The battery can also be used to power or improve the interaction with other devices. For example, a company shipping perishable goods may want to use active tags that integrate with thermometers to ensure the goods are kept at an acceptable temperature.

Figure 3 provides a simplified schema of the use of RFID in supply chain. Portable readers or fixed readers are connected to the control center, respectively, through wireless or fixed communications.

RFID provide better data security in comparison to traditional barcode technology and it can be a powerful enabler to improve the operational efficiency of supply chain management (Tajima, 2007; Lin, 2009).

The application of secure RFID to the disaster supply chain is presented in the following sections.

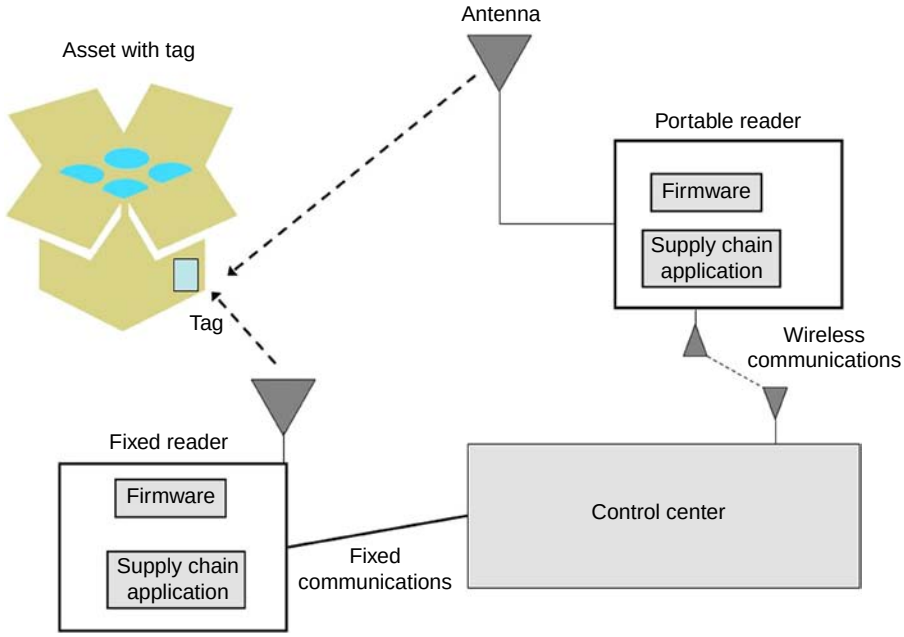

Figure 3.
RFID in the supply chain

4.3 RFID in track and trace

The purpose of this section is to investigate the current RFID approach to obtain a secure identification of objects.

Track and trace systems using RFID allow to track the movement of tagged items from the suppliers to the emergency crisis through distribution. Each item is equipped with an RFID tag that can be read out automatically without any line-of-sight at every point within the supply chain. The read data provides detailed information on the corresponding item and it will then be sent via the internet to the central tracking server which stores the complete history of the RFID tag and checks its plausibility. Providing this electronic pedigree of each transport unit the barrier to disrupt the supply chain can be increased. Figure 4 shows the tracking system. For instance, the Electronic Product Code (= EPC) infrastructure by EPCglobal (2003) enables the exchange of RFID data via the internet and it is currently the most promising approach for a track and trace solution, even if there are issues, which are discussed in the next paragraph.

At first glance such a track and trace only system seems to be a good approach, but there are some major drawbacks of this system, which will be described in the following paragraph.

4.4 Lack of completeness in track and trace only solutions

A major precondition that a solution, which is only based on track and trace techniques, works reliably is that each party involved in the distribution process must take part the track and trace system. On the one hand all participants of the supply chain must be compliant with the chosen track and trace standard at the same time to provide a consistent tracking profile. It requires cooperation between all partners within the multi-party supply chain. On the other hand in emergency crises the RFID infrastructure can be degraded or even destroyed as consequence of the crisis itself. Hence, the item cannot be tracked along the complete supply chain in order to securely identify the object.

4.5 Crime

A major drawback is criminal activity. Since ordinary RFID tags used for track and trace solutions are simple tags, which only store an identification number in plain text the tags themselves are susceptible to faking attacks. It is a misbelief that tags, which carry a unique identifier written during the manufacturing process can be used as

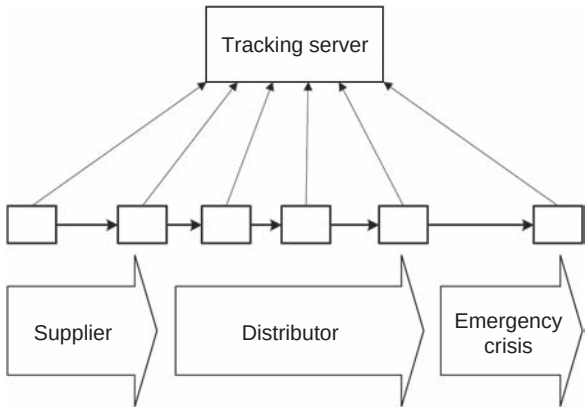

Figure 4.
Tracking system with RFID

security feature for unique identification. Usually RFID systems use standardized radio frequency communication protocols, which are public domain. In addition all necessary information on the functionality of RFID is also available on the internet or in the literature, e.g. the *RFID Handbook* (Finkenzeller, 2003), as well as development tools. Cloning an original tag works as follows. First we need a reader device that supports the tag's communication standard. Then the reader sends a request for the tag's identification number upon which the tag responds with its number in plain text. Afterwards this identification number will be stored to a new tag supporting this standard. Some manufacturers offer tags, which can be personalized by the customer. Using these tags it is rather simple to store the identification numbers of the original tags to these new tags. The following scenario is possible: a criminal party, duplicates tags as described and attaches them to goods. The shipping unit carrying the original RFID may be removed from the supply chain and sold using an illegal distribution channel. The goods carrying the cloned tags move within the supply chain without producing any inconsistence in the tracking history. In the worst case terrorists could replace drugs or food by worthless or even harmful units to sabotage disaster relief.

5. Cryptographic authentication

The above mentioned problems show that track and trace only solution may not be sufficient for a secure identification of items. To obtain an appropriate security level that ensures authentication on item level, the RFID tags themselves must implement authentication mechanisms (Staake *et al.*, 2005). This authentication mechanism must withstand the cloning attack as described in the previous section. The approach is the commonly used challenge-response-protocol. The RFID tag contains its identification number, a secret key and a cryptographic unit. The reader transmits a randomly selected number, the so-called challenge and the tag calculates the corresponding response with the cryptographic algorithm using the secret key and the challenge. Afterwards the tag sends this response back to the reader. Finally the reader, and consequently the back end system, checks whether the response is correct or not. The crucial point in this protocol is the fact, that the secret key itself will never be transmitted over the radio channel and the correct response can only be generated with the aid of the secret key. Guessing the correct secret key or analyzing several pairs consisting of challenge and response to retrieve the secret key is computationally infeasible.

5.1 Public key authentication

Most RFID systems as the recently broken Mifare tag uses authentication mechanisms based on symmetric cryptography. It that case the tag and the reader share a common key to run the authentication protocol – the tag uses this secret key for response generation and the reader for the verification. But this approach has some drawbacks in decentralized environments concerning the key management. Either the readers must store the secret keys of the RFID tags belonging to the application domain or an online connection from the reader to a server must be established since the secret keys of the RFID tags are stored in a secure and reliable back end system.

A different approach can be based on public-key cryptography. In this case the response generation will still be performed using a secret key, the so-called private key $priv_{id}$, but the response verification on the reader side can be performed without any secret key only with a public key pub_{id}, which need not be protected against misuse. In order to avoid that each reader has to store the individual public keys pub_{id} of all tags

belonging to the application, a certification authority (CA) issues a certificate $cert_{id}$ for every public key pub_{id} and only the CA knows the secret signature key (= PrivSigKey) necessary for the generation of the certificate. The corresponding public signature key (= PubSigKey) for verifying the certificates must be downloaded exactly one time to each reader within the system.

First the tag transmits its certificate $cert_{id}$ containing its public key pub_{id}. Then the reader verifies the authenticity of the sent public key pub_{id} with the public signature key. Afterwards a challenge-response-protocol will be initialized. The reader generates a challenge C, transmits C to the tag upon which the tag computes the corresponding response R with its private key $priv_{id}$ using the public key operation. The tag sends R back to the reader and finally the reader checks the response with the tag's public key pub_{id} using the verification algorithm.

The major benefit of this approach is that no secret key is needed for the authentication on the reader side, neither in the back end nor in the reader itself which saves expenses. Furthermore the authentication process can be performed without any online connection which simplifies the system.

5.2 Related work in RFID security

One major drawback of public key approach is the higher complexity in comparison to the symmetric key approach, which means a higher implementation effort in chip size and finally a lower performance and higher power consumption. Besides these evident disadvantages of the realization of public key cryptography on smart but low-cost devices as RFID tags the interest of the cryptographic research community has been concentrated to investigate the requirements of public key operations under which it is possible to implement them on RFID tags. Many publications have appeared on this interesting topic. We now give a brief summary of the most important ones.

Gaubatz *et al.* (2004) showed that the well-known RSA public key scheme is not a feasible approach while the NTRU crypto system (NTRU, 2008) can be implemented with $<3{,}000$ gate equivalents[1]. But NTRU has some weaknesses and it is still under investigation by the crypto community. Recent publications investigated the applicability of public key cryptography on RFID tags and the authors proposed approaches toward a low-cost RFID tag based on elliptic curve cryptography (= ECC). Wolkerstorfer (2005) implemented a compact ECC engine that meets the constraints imposed by the EPC standard. He used a signature-based protocol. Batina *et al.* (2006) gave a further area optimization using a protocol based on zero knowledge. A milestone toward a first implementation of ECC on RFID tags was published in Braun *et al.* (2008) and Bock *et al.* (2008)). The authors presented product like prototype of an ISO 15693 RFID tag realizing a challenge response protocol based on ECC. In the following subsection we give a short description of the protocol including the cryptographic primitives. Zhang *et al.* (2008) describes a secure RFID-based track and trace solution in supply chains, by leveraging on the EPCglobal standard. The proposed solution is valid for commercial supply chains but not for supply disaster chains like the one described in this paper, where the supply chain flow is much more decentralized. To our knowledge, this is a first time that a secure RFID is proposed for disaster supply chain management.

5.3 ECC and the protocol

Our RFID tags use elliptic curves over binary finite fields GF(2^n). An elliptic curve E is a set of points $P = (x_P, y_P)$ satisfying the Weierstraß equation $y^2 + xy = x^3 + ax^2 + b$

where $a, b \in \mathrm{GF}(2^n)$. On an elliptic curve E we can define an addition $R = (x_R, y_R) = P + Q$ of elliptic curve points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ by the following formulae for the case of $P \neq Q$ and the case of $P = Q$:

$$P \neq Q$$

$$x_R = \lambda^2 + \lambda + x_P + x_Q + a$$
$$y_R = \lambda(x_P + x_R) + x_R + y_P$$
$$\lambda = \frac{y_P + y_Q}{x_P + x_Q}$$

$$P \neq Q$$
$$x_R = \lambda^2 + \lambda + a$$
$$y_R = x_P^2 + (\lambda + 1)x_R$$
$$\lambda = x_P + \frac{y_P}{x_P}$$

The structure determined by the set of points and this addition operation allows public key operation which is the scalar multiplication $s \times P$ of a scalar value s in binary representation $s = (s_l, \ldots, s_1)_2$ with a point $P = (x_P, y_P)$ on the curve E. An in deep introduction to this field of cryptography may be found in Hankerson *et al.* (2004). The so-called elliptic curve point multiplication is the basis for our protocol. We implemented Montgomery's method for scalar multiplication (Bock *et al.*, 2008; Hankerson *et al.*, 2004). This method has special characteristics preventing so-called side channel attacks and it is well suited for hardware efficient implementations since expensive inversions of finite fields elements can be avoided as projective coordinates of the x-coordinates are used (Hankerson *et al.*, 2004).

The applied authentication protocol is based on a challenge-response-protocol, where the security is based on the Elliptic-Curve-Diffie-Hellman problem.

Now let P denote the base point on the elliptic curve E with order q. For each RFID tag an individual private key $priv_{id}$ is given, which is a random number d with $0 < d < q$. The corresponding public key pub_{id} is then the point Q given by the scalar multiplication of d and the base point P:

$$Q := d \times P$$

As already pointed out in the previous section the RFID reader generates a challenge C. This will be done by choosing a random scalar k and multiplying it with P:

$$C := k \times P$$

The corresponding response R is then calculated by the tag using its private key d:

$$R := d \times C$$

The reader itself calculates $V := k \times Q$ and compares $R = V$. The verification works since the following chain of equations holds:

$$R = d \times C = d \times (k \times P) = (dk) \times P = k \times (d \times P) = k \times Q = V$$

The complete authentication protocol is depicted in Figure 5.

6. System architecture

In this section we propose a system architecture for managing secure supply chains suitable for distribution of relief items from suppliers to disaster areas. Figure 6 gives a brief overview of the architecture.

In the first step of the supply chain there are blank RFID tags (i.e. these tags are not personalized and do not hold cryptographic key material) and relief items, which are not labeled with RFID tags. In this early stage the security mechanisms are not activated. The activation has to be done in a trustworthy environment as explained in the following. The trustworthy environment may be installed at the supplier of relief items or at a logistic center of the humanitarian organization. It is also possible to distribute the trustworthy environment to different locations where at one location the tags are personalized and at another location the RFID tags are mounted to the relief items. Delivering personalized RFID from the personalization site to the mounting site requires a secure channel for delivery.

The most important part of the trustworthy environment is the CA. In general the CA is a server system, which stores the private signature key PrivSigKey, which has to be kept secret by the CA because this key is the cryptographic security anchor of the whole system. The associated public signature key PubSigKey may be publicly known and part of the CA certificate. The CA certificate has to be installed on all readers in the distribution chain. It is also possible to install certificates of different CAs on reader devices. But it is important to note that only trusted certificates are allowed to be installed on the readers.

Figure 7 describes the deployment workflow of the proposed solution among the participants of the disaster supply chain.

Additionally the CA generates the key pairs to be stored on the RFID tags. The key pairs may be individual for each RFID tag or alternatively for a bunch of tags. The tag private key $priv_{id}$ is only stored on the RFID tag and is discarded by the CA after

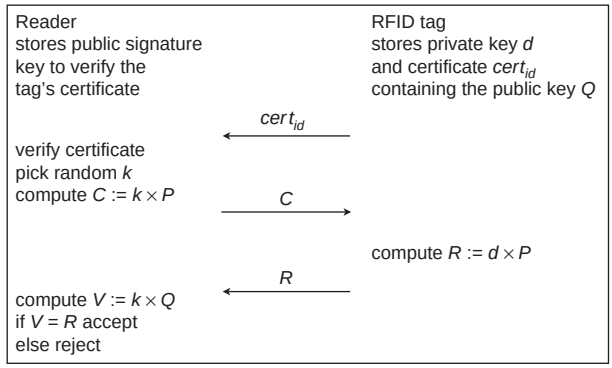

Figure 5.
The authentication protocol

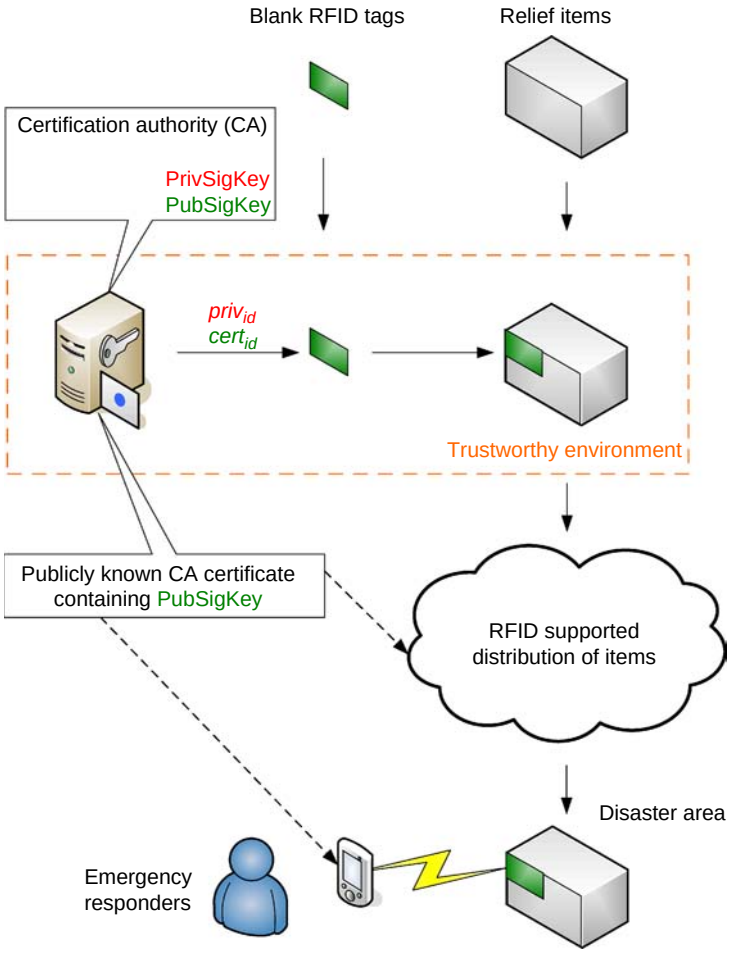

Figure 6.
Proposed system architecture for distribution of RFID to relief items

writing it on the RFID tag. There is even no possibility to read the private key from the RFID tag. The corresponding tag public key pub_{id} is embedded in the certificate $cert_{id}$ and signed with the PrivSigKey which only known to the CA. This certificate is also stored on the RFID and may be publicity known. There is no possibility to alter the certificate by another party then the CA because the certificate cannot be signed without knowing the PrivSigKey. After storing the private key $priv_{id}$ and the certificate $cert_{id}$ the RFID will be locked to prevent further personalization.

The personalized RFID tags are attached to the relief items and delivered to the disaster area using the distribution infrastructure. In this distribution network it is possible to read the RFID tag at all times and if the CA certificate is available to the reader it is also possible to verify the authenticity of the items using the authentication protocol depicted in Figure 5. At the disaster area the emergency responders may use handheld devices equipped with RFID readers to read the attached RFID tags and verify their authenticity. On the whole way from the supplier to the disaster area

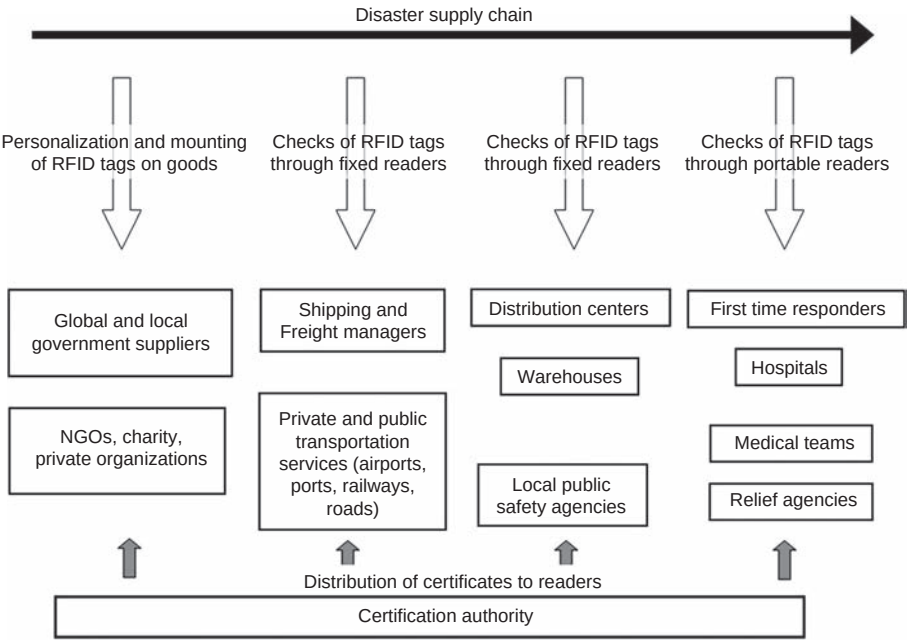

Figure 7.
Deployment workflow

there is no need to have an online connection to a backend system. So it is possible to verify the authenticity of relief items in an environment with highly degenerated infrastructure.

The proposed solution can be used to augment existing supply chains and it has a minimal impact on the organization structure and procedures of the relief organizations. The personalized RFID tags and secure readers can be distributed to the relief personnel in the planning phase. Certificates can also be distributed in the planning phase using Internet or existing communication links. The CA can be managed by a public safety or international government organization, which has already links with the major participants of the disaster supply chain. The proposed solution can be deployed through a gradual approach: in a first phase only the most critical goods like medicines are tracked through the secure RFID tags, in the second phase the solution is extended to all types of goods.

The proposed solution addresses most of the challenges described in Section 3.1:

- Size of the relief chain: RFID can be used to improve the tracking and tracing of goods from the supplier to the local distribution. This is benefit provided by the RFID technology itself and not specifically by the security framework.
- Coordination: the proposed solution does not directly support the coordination among the participants of the disaster supply chain; in fact it actually requires an additional activity for the setup of the security framework. The benefit of the proposed solution is to increase the level of trust among the participants in the management of the disaster supply chain as relief goods provided by one partner (e.g. donors, suppliers) can be trusted by the partners responsible for the distribution (e.g. local relief agencies, first time responders).

- Security: the proposed solution address directly the security aspects of the relief chains by ensuring a secure tracking and tracing of the relief good.

To the authors' knowledge, this is the first paper, which contributes to the definition of secure disaster supply chains by applying secure RFID technology.

7. Conclusion and future developments

Emergency crises presents big challenges for disaster relief teams especially on the management of the supply chain. An important function is secure tracking and tracing of the relief goods, which is an essential part of disaster supply chain management. Security is an important requirement, as emergency crises are often chaotic environments with degraded and overloaded infrastructure where criminals can exploit the situation to steal or redirect relief goods. These facts combined with a highly decentralized organization require flexible, reliable and secure supply chains. The passive RFID tag, presented in this paper, is a robust and cost effective solution for this application domain. It is based on leading edge public-key cryptography and offers security mechanisms, which do not need an intact communication infrastructure. We discussed the technical facts and presented the prototypic implementation of our new cryptographic RFID tag.

The next step would be to investigate the integration of the proposed solution with relief agencies and their information technology infrastructures to assess the impact both from an organizational and technological point of view.

Note

1. The complexity of an RFID chip can be described by the number of transistors or the so-called gate equivalent, which is about a fourth of the number of transistors. The number of gate equivalents scales the cost of an RFID tag, i.e. 1,000 gates cost approximately 1 cent Wei:03.

References

Autier, P., Ferir, M.C., Hairapetien, A., Alexanian, A., Agoudjian, V., Schmets, G., Dallemagne, G., Leva, M.N. and Pinel, J. (1990), "Drug supply in the aftermath of the 1988 Armenian earthquake", *Lancet*, Vol. 335 No. 8702, pp. 1388-90.

Balcik, B., Beamon, B.M., Krejci, C.C., Muramatsu, K.M. and Ramirez, M. (2010), "Coordination in humanitarian relief chains: practices, challenges and opportunities", *International Journal of Production Economics*, Vol. 126 No. 1, pp. 22-34.

Baldini, G., Seuschek, H., Oliveri, F., Braun, M. and Hess, E. (2009), "The use of secure RFID to support the resolution of emergency crisis", in IEEE (Ed.), *ICCST 2009, 43rd Annual International Carnahan Conference on Security Technology*, IEEE, Zurich, pp. 321-8.

Bankoff, G., Frerks, G. and Hilhorst, D. (2003), *Mapping Vulnerability: Disasters, Development and People*, Earthscan Publications Ltd, London.

Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P. and Verbauwhede, I. (2006), "Public key cryptography for RFID tags", RFIDSec 2006, Proceedings of the 2th Workshop on RFID Security, July, Graz.

Beamon, B.M. and Benita, M. (2004), "Humanitarian relief chains: issues and challenges", The 34th International Conference on Computers and Industrial Engineering, November 14-16, San Francisco, CA.

Bock, H., Braun, M., Dichtl, M., Heyszl, J., Hess, E., Kargl, W., Koroschetz, H., Meyer, B. and Seuschek, H. (2008), "A milestone towards RFID products offering asymmetric

authentication based on elliptic curve cryptography", RFIDSec 2008, Proceedings of the 4th Workshop on RFID Security, July 9-11, Budapest.

Braun, M., Hess, E. and Meyer, B. (2008), "Using elliptic curves on RFID tags", *International Journal of Computer Science and Network Security*, Vol. 8 No. 2, pp. 1-9.

Cassidy, W.B. (2003), "A logistics lifeline", *Traffic World*, October, p. 1.

Constable, M. (2008), "Disaster mythology: looting in New Orleans", *Disaster Prevention and Management*, Vol. 17 No. 4, pp. 519-25.

EPCglobal (2003), "EPC global web site", available at: www.epcglobalinc.org/home (accessed July 12, 2010).

Finkenzeller, K. (2003), *RFID-Handbook*, 3rd ed., Wiley & Son Ltd, Chichester.

Fritz Institute (2005), "Logistics and the effective delivery of humanitarian relief", available at: www.fritzinstitute.org (accessed July 12, 2010).

Gaubatz, G., Kaps, J.-P. and Sunar, B. (2004), "Public key cryptography in sensor networks – revisted", ESAS 2004, 1st European Workshop on Security in Ad-Hoc and Sensor Networks, August 6, Heidelberg.

Hankerson, D., Menezes, A. and Vanstone, S. (2004), *Guide to Elliptic Curve Cryptography*, Springer, New York, NY.

Jungbae Roh, J., Kunnathur, A. and Tarafdar, M. (2009), "Classification of RFID adoption: an expected benefits approach", *Information and Management*, Vol. 46 No. 6, pp. 357-63.

Kovacs, G. and Spens, K.M. (2007), "Humanitarian logistics in disaster relief operations", *International Journal of Physical Distribution & Logistics Management*, Vol. 37 No. 2, pp. 99-114.

Kovacs, G. and Spens, K.M. (2009), "Identifying challenges in humanitarian logistics", *International Journal of Physical Distribution & Logistics Management*, Vol. 39 No. 6, pp. 506-28.

Lin, L.C. (2009), "An integrated framework for the development of radio frequency identification technology in the logistics and supply chain management", *Computers and Industrial Engineering*, Vol. 57 No. 3, pp. 832-42.

Long, D. (1997), "Logistics for disaster relief: engineering on the run", *IIE Solutions*, Vol. 29 No. 6, pp. 19-26.

Miller, H.E., Engemann, K.J. and Yager, R.R. (2006), "Disaster planning and management", *Communications of the International Information Management Association*, Vol. 6 No. 2, pp. 25-36.

Murray, S. (2005), "How to deliver on the promises: supply chain logistics: humanitarian agencies are learning lessons from business in bringing essential supplies to regions hit by the tsunami", *Financial Times*, January 7, p. 9.

NTRU (2008), "An asymmetric cryptosystem", available at: www.ntru.com (accessed July 12, 2010).

Richardson, V. (2006), "An entrepreneur tackles the logistics of disaster", available at: www.globalenvision.org/library (accessed July 12, 2010).

Rosenthal, U., Charles, M.T. and Hart, P. (Eds) (1989), *Coping with Crises: The Management of Disasters, Riots and Terrorism*, Charles C. Thomas Publishers, Springfield, IL.

Sarac, A., Absi, N. and Dauzere-Peres, S. (2010), "A literature review on the impact of RFID technologies on supply chain management", *International Journal of Production Economics*, Vol. 128 No. 1, pp. 77-95.

Staake, T., Thiesse, F. and Fleisch, E. (2005), "Extending the EPC network the potential of RFID in anti-counterfeiting", 20th ACM symposium on Applied computing, ACM, March, pp. 1607-12.

Stephenson, M. (2005), "Making humanitarian relief networks more effective: operational coordination, trust and sense making", *Disasters*, Vol. 29 No. 4, pp. 337-50.

Tajima, M. (2007), "Strategic value of RFID in supply chain management", *Journal of Purchasing and Supply Management*, Vol. 13 No. 4, pp. 261-73.

Tatham, P. and Kovacs, G. (2009), "The application of 'swift trust' to humanitarian logistics", *International Journal of Production Economics*, Vol. 126 No. 1, pp. 35-45.

The Economist Intelligence Unit (2005), "Disaster-response management – going the last mile", *The Economist*.

Trunick, P.A. (2005), "Special report: delivering relief to tsunami victims", *Logistics Today*, Vol. 46 No. 2, pp. 1-3.

US House of Representatives (2006), "A failure of initiative – final report of the select bipartisan committee to investigate the preparation for and response to Hurricane Katrina", Congressional reports, H. Rpt, pp. 109-377.

Wolkerstorfer, J. (2005), "Is elliptic curve cryptography suitable to secure RFID tags?", Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, Graz, July.

Xu, L. and Beamon, B.M. (2006), "Supply chain coordination and cooperation mechanisms", *The Journal of Supply Chain Management*, Vol. 42 No. 1, pp. 4-12.

Yang, H., Yang, L. and Yang, S. (2010), "Hybrid Zigbee RFID sensor network for humanitarian logistics centre management", *Journal of Network and Computer Applications*, Vol. 34 No. 3, pp. 938-48

Zhang, N., He, W., Tan, P.S., Lee, E.W., Li, T.Y. and Lim, T.L. (2008), "A secure RFID-based track and trace solution in supply chains", INDIN 2008, 6th IEEE International Conference on Industrial Informatics, Daejeon, July 13-16, pp. 1364-69.

Further reading

Akbulut, A. and Kelle, P. (2005), "The role of ERP tools in supply chain information sharing, cooperation, and cost optimization", *International Journal of Production Economics, Proceedings of the Twelfth International Symposium on Inventories, January 8, Vol. 93-4*, Elsevier, Amsterdam, pp. 41-52.

Balcik, B., Beamon, B.M. and Smilowitz, K. (2008), "Last mile distribution in humanitarian relief", *Journal of Intelligent Transportation Systems*, Vol. 12 No. 2, pp. 51-63.

Beamon, B.M. (2004), "Humanitarian relief chains: issues and challenges", Proceedings of 34th International Conference on Computers and Industrial Engineering, November 14-16, San Francisco, CA.

Beamon, B.M. and Balcik, B. (2008), "Performance measurement in humanitarian relief chains", *International Journal of Public Sector Management*, Vol. 21 No. 1, pp. 4-25.

Feldhofer, M., Dominikus, S. and Wolkerstorfer, J. (2004), "Strong authentication for RFID systems using the AES algorithm", *CHES 2004, Workshop on Cryptographic Hardware and Embedded Systems, Vol. 3156 of Lecture Notes in Computer Science*, Springer, Berlin, pp. 357-70.

Gardner, T. (2006), *Former FEMA Director Shoulders Greater Share of Blame for Katrina Failures*, Associate Press, New York, NY.

Garshnek, V. and Burkle, F. Jr (1999), "Telecommunications systems in support of disaster medicine: applications of basic information pathways", *Annals of Emergency Medicine*, Vol. 34 No. 2, pp. 213-8.

Haddow, G., Bullock, J. and Coppola, D. (2008), *Introduction to Emergency Management*, 3rd ed., Butterworth-Heinemann, Oxford.

Hamzeh, F. (2007), "Logistics centres to support project-based production in the construction industry", *Proceedings of the IGLC-15, Michigan*, International Group for Lean Construction (IGLC), San Diego, CA, pp. 181-91.

Harald, J., Chansue, N. and Monticelli, F. (2006), "Implantation of radio frequency identification device (RFID) microchip in disaster victim identification (DVI)", *Forensic Science International*, Vol. 157 Nos 2-3, pp. 168-71.

Kömmerling, O. and Kuhn, M. (1999), "Design principles for tamper-resistant smartcard processors", *Smartcard*, USENIX Association, Berkeley, CA, pp. 9-20.

Long, D.C. and Wood, D.F. (1997), "The logistics of famine relief", *Journal of Business Logistics*, Vol. 16 No. 1, pp. 213-29.

McClintock, A. (2009), "The logistics of humanitarian emergencies: notes from the field", *Journal of Contingencies and Crisis Management*, Vol. 17 No. 4, pp. 295-302.

Sheu, J. (2010), "Dynamic relief-demand management for emergency logistics operations under large-scale disasters", *Transportation Research Part E: Logistics and Transportation Review*, Vol. 46 No. 1, pp. 1-17.

Walker, P. and Feinstein International Famine Center (2005), "Is corruption an issue in the tsunami response?", *Humanitarian Exchange Magazine*, No. 30, June.

Weis, S. (2003), "Security and privacy in radio-frequency identification devices", master thesis, Massachusetts, Institute of Technology (MIT), Boston, MA.

Whybark, C. (2007), "Issues in managing disaster relief inventories", *International Journal of Production Economics*, Vol. 108 No. 1, pp. 228-35.

Zhenling, L. (2009), "Integrated supply chains of the natural disaster relief substances. Management and service science", *Management and Service Science, 2009, MASS '09. International Conference on, Beijing, China*, IEEE Wuhan Section, Wuhan, pp. 1-4.

About the authors

Gianmarco Baldini completed his Master's degree (Laurea) in 1993 in Electronic Engineering from the University of Rome "La Sapienza", with specialisation in Wireless Communications. He has worked for more than 14 years in the design, development and testing of wireless communication systems in the R&D departments of multinational companies such as Ericsson, Lucent Technologies, Hughes Network Systems and Selex Communications before joining the Joint Research Centre in 2007. Gianmarco Baldini is the corresponding author and can be contacted at: gianmarco.baldini@jrc.ec.europa.eu

Franco Oliveri received the Master's degree (Laurea) in Electronic Engineering (System design and control system design) in 1983 from the University of Genoa. He was Manager of the C3I R&D Laboratory in Marconi Italy, dealing with HW & SW design of military computers and communication systems. He joined the Joint Research Centre of the European Commission in 2006.

Michael Braun worked at Siemens AG, Corporate Technology until 2008, when he joined the University of Applied Sciences of Darmstadt as Assistant Professor.

Hermann Seuschek, at the time of writing this paper, was working for Siemens AG, Corporate Technology in the field of cryptography and secure RFID. He is now based at the Institute for Security in Information Technology, Technische Universität München.

Erwin Hess is working at Siemens AG, Corporate Technology in the field of cryptography and secure communications.

This article has been cited by:

1. Ahmed Musa, Al-Amin Abba Dabo. 2016. A Review of RFID in Supply Chain Management: 2000–2015. *Global Journal of Flexible Systems Management* **17**:2, 189-228. [CrossRef]
2. Ana Laura R. Santos Design for Sustainability, Faculty of Industrial Design Engineering, Delft University of Technology, Delft, The Netherlands Linda S.G.L. Wauben Department of BioMechanical Engineering, Faculty of Mechanical, Maritime and Materials Engineering, Delft University of Technology, Delft, The Netherlands Richard Goossens Industrial Design Faculty, Delft University of Technology, Delft, The Netherlands Han Brezet Design for Sustainability, Faculty of Industrial Design Engineering, Delft University of Technology, Delft, The Netherlands . 2016. Systemic barriers and enablers in humanitarian technology transfer. *Journal of Humanitarian Logistics and Supply Chain Management* **6**:1, 46-71. [Abstract] [Full Text] [PDF]
3. Alain Vaillancourt, Ira Haavisto. 2016. Country logistics performance and disaster impact. *Disasters* **40**:2, 262-283. [CrossRef]
4. Rameshwar Dubey, Angappa Gunasekaran. 2016. The sustainable humanitarian supply chain design: agility, adaptability and alignment. *International Journal of Logistics Research and Applications* **19**:1, 62-82. [CrossRef]
5. Dr Burcu Balcik Marianne Jahre Department of Industrial Management and Logistics, Lund University, Lund, Sweden AND Department of Accounting, Auditing, and Business Analytics, BI Norwegian Business School, Oslo, Norway Nathalie Fabbe-Costes CRET-LOG Research Centre, Aix-Marseille Université, Aix-en-Provence, France . 2015. How standards and modularity can improve humanitarian supply chain responsiveness. *Journal of Humanitarian Logistics and Supply Chain Management* **5**:3, 348-386. [Abstract] [Full Text] [PDF]
6. Sarah Schiffling Logistics Research Centre, Heriot-Watt University, Edinburgh, UK Maja Piecyk Logistics Research Centre, Heriot-Watt University, Edinburgh, UK . 2014. Performance measurement in humanitarian logistics: a customer-oriented approach. *Journal of Humanitarian Logistics and Supply Chain Management* **4**:2, 198-221. [Abstract] [Full Text] [PDF]
7. Naveeta Panwar, Dikshit Uniyal, Krishna Singh RautelaMapping Sustainable Tourism into Emergency Management Structure to Enhance Humanitarian Networks and Disaster Risk Reduction using Public-Private Partnerships (PPP) Initiatives in Himalayan States 129-151. [CrossRef]
8. Faye TaylorTourism and Crisis: 163-189. [CrossRef]