4

Secure RFID for Humanitarian Logistics

Gianmarco Baldini[1], Franco Oliveri[1], Hermann Seuschek[2],
Erwin Hess[2] and Michael Braun[3]
[1]*Joint Research Centre - European Commission*
[2]*Siemens AG*
[3]*University of Applied Sciences, Darmstadt*
[1]*Italy*
[2,3]*Germany*

1. Introduction

Extreme events like hurricanes, flooding and earthquakes cause massive disruption to society, including large death tolls and property damage. In recent years, many events like the Katrina disaster Katrina (2004) have shown the importance of efficient disaster management to alleviate the resulting pain and suffering and to mitigate the consequences of the disaster. Disaster management includes a large set of activities including the care of the survivors needs, protection of assets from any further damage and provision of shelter, water, food, and medicines to dislocated people. The creation of an effective disaster supply chain to deliver necessary goods to disaster relief organizations is an essential function of disaster management. This function is also called humanitarian logistics. Humanitarian logistics is a wide term that covers the operations concerning supply chain strategies, processes, and technologies that will maintain the flow of goods and material needed for the humanitarian.
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, 26th 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 Gardner (2006) and hundreds of thousands of people were displaced from their homes.
In a recent report Fritz (2005), it was highlighted that most of the organizations involved in the 2004 tsunami disaster were lacking in supply chain expertise and technology. Humanitarian logistics is indeed a very challenging task for many organizations for a number or reasons, which will be described in this chapter. For example, natural disasters are usually characterized by a chaotic environment and by a general lack of transportation infrastructures, which are usually degraded or destroyed. Many different organizations may be involved with no a-priori coordination plan defined. All these challenges make the task of humanitarian relief organizations very difficult. Traditional mechanisms and processes implemented in commercial supply chains may not be directly adapted to humanitarian logistics because of these challenges and because of the different operational requirements. Timing constraints are much more severe in disaster supply chain than commercial supply chains because of the potential loss in human lives and assets if essential equipment is not distributed in time.
In other cases, specific processes and technologies can be tailored to humanitarian logistics. Radio-Frequency IDentification (RFID) technology has already been identified 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.
Security is a very important requirement in humanitarian logistics. In the aftermath of a disaster, many goods (e.g., medicine, foods), which are usually available in normal conditions, became extremely valuable and potential target of thieves.
In the commercial domain, theft reduction is considered the main expected benefit as it translates to cost savings, while it will be even more important in crisis situation where replacements for stolen goods, may not be readily available. As a consequence, the distributed goods must be protected and all the components of the supply chain should be made secure: RFID tags 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. As a consequence, security of the RFID tags is an important element in humanitarian logistics.
This chapter will describe the main features and challenges of Humanitarian logistics, the role of RFID technology in disaster supply chains and the implementation and deployment of secure RFID.
The chapter has the following structure: section 2 describes the features of natural disasters and emergency crises, the main phases (mitigation, preparedness, response, recovery), the role of Humanitarian Logistics and the related challenges. Section 3 describes the role of RFID in Humanitarian Logistics. Section 4 describes security aspects in RFID. Section 5 describes the proposed system for secure RFID and the related authentication mechanism. Section 6 describes the system architecture and the deployment of RFID in humanitarian logistics. Section 7 describes the role of telecommunications in the disaster supply chains based on RFID. Finally section 8 provides suggestions for future developments in this area.

2. Disaster management and humanitarian logistics

2.1 Type of disasters and features

In this chapter, we will use the definition of natural disaster from Bankoff (2005):

> "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"

it appears clear that what is relevant is the effect of the disaster on the human lives 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 or the impact on the region. Table 1 provides an overview of the most typical disasters or emergency crises and their features from a qualitative point of view.
Each type of disaster have specific features, which require different responses and recovery actions, but they all produce devastating loss of lives and assets. Disaster management tries to minimize the impact of natural disasters through various activities, which include damage

Disaster Type	Predictability	Severity	Geographical impact
Earthquake	Low	High	National
Tsunami	Low	High	International
Storm/Hurricane	Medium	Medium/High	National
Vulcanic Eruption	Medium	High	National and International (i.e., dust clouds)
Pandemic Disease	Medium	Medium/High	Potentially Global
Terrorist Attack	Medium	Medium	Local/City
Transportation incident	Low	Medium	Local
Armed Conflict	Medium	High	International
Landslide	Medium	Low	Local
Avalanche	Medium	Low	Local
Chemical plant incident	Man-made	Low	Medium
Nuclear incident	Low	High	National and International (i.e., radioactive dust)

Table 1. Features of natural disasters and emergency crisis

assessment, reconstruction, emergency health services and the creation of supply chains to bring needed goods.

2.2 Phases of disaster management

Natural disaster management is usually split in four phases: prevention, preparedness, response and recovery. Such phases may be named in different way by different authors or different organizations, but usually the first two phases are related to activities to avoid the disaster (prevention) or to be prepared for the disaster (preparedness). The third phase (response) includes all the activities to be performed in the aftermath of a disaster, while the last phase (recovery) deals with the endeavor of bringing back a normal life to the people affected by the disaster.
From Altay and Green (2006), a number of activities are defined for each phase of disaster management, which are described in figure 1.

2.3 Supply chains in disaster management

The availability of materials such as medicines, food, shelter for the immediate needs after the disaster is usually not a problem and it is also quite viable to deliver them in the country affected by the disaster; what is a real challenge is to keep track of the shipped crates and ensure that medicines are distributed to the hospitals and the responders working in the disaster sites. Operators deploying the Supply Chain in disaster areas have to face, on top of the heavy disruption of the usual delivery systems as well as of the communication systems, the presence of every sort of looters; in the aftermath of a disaster, the usual physical protection of a sensitive area, such as a warehouse, may be limited. As a consequence, it is of paramount importance that the tools used to keep track of the delivered crates are well designed against tampering. The management of the supply chain is one of the most important activities during a natural disaster or an emergency crisis and an adequate preparation is the key for success in such phase, but it is obviously very difficult to invest large amount of money in the preparation of a response to events that may or may not

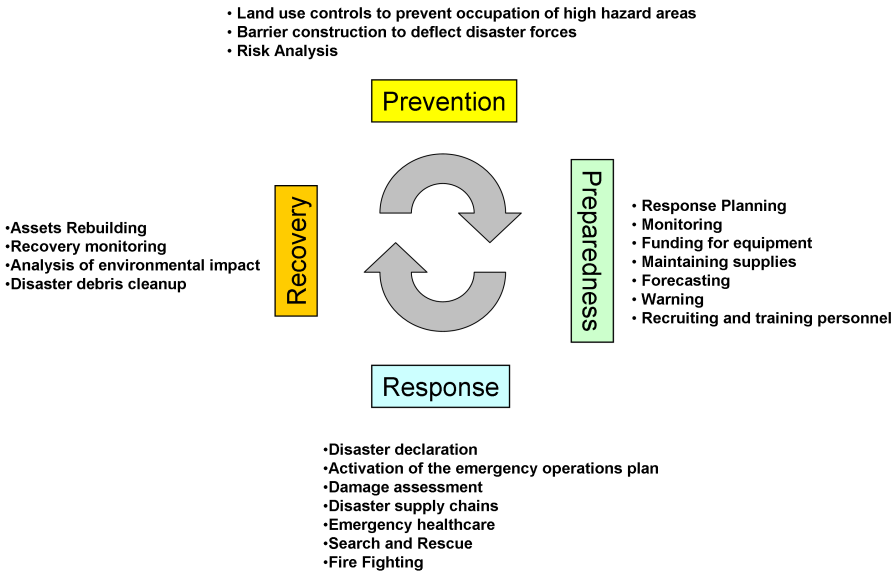


Fig. 1. Phases of Disaster Management

occur, therefore it is crucial to design a solution that is tamper proven, low cost and user friendly. 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. In India, the transportation infrastructure was overloaded and bottlenecks were present at main conjunction points. In Indonesia, the damaged infrastructure combined with the flood of goods from many different agencies created huge logistics problems. Many participants to the relief efforts to the Tsunami disaster, claimed that logistics and efficient supply chain was more important than a large quantity of goods. Figure 1 describes the phases in disaster management and the related functions. Supply chains used in disaster management are usually called disaster supply chains.

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 is different. Commercial supply chains are focused on quality and profitability, humanitarian supply chains must be focused on minimizing loss of life and suffering. Supply chain management may be present in the phases preparedness, response and recovery with different roles. In the preparedness phase, supply chains are used to stockpile and maintain disaster supplies and equipment, which may be used in disaster management. In preparedness phase, 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 as described in Table 1, supply chain management can become very complex with the presence of different stakeholders and large quantity of materials to be distributed. Because transportation infrastructures are degraded or destroyed, the distribution of the materials could be quite difficult. Furthermore, there are severe time constraints as people may die if goods are not distributed in time. In the recovery phase, disaster supply chains are needed to rebuild destroyed property and repair of essential critical infrastructures (e.g., energy, transportation and others). Supply chain management can still be hampered by degraded infrastructure in the area, but the timing constraints are usually more relaxed in comparison to the response phase.

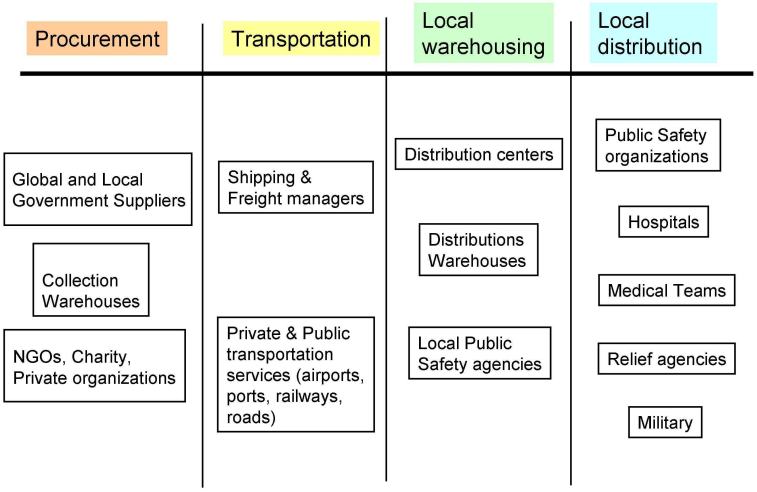


Fig. 2. Participants to Humanitarian Logistics

Another significant challenge for humanitarian logistics is the presence of many different types of organizations: from firefighters, military, relief organizations, non-government organizations (NGO) and others. The coordination among these organizations is essential to support disaster management operations and disaster supply chains in particular. Figure 2 describes the main participants, which are usually involved in the resolution of a large natural disaster or emergency crisis.

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.

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 generic commercial supply chains, but in humanitarian logistics they become even more difficult because many different partners are involved, which must share information among themselves in the severe time constraints imposed by the operational context. Interoperability issues may especially appear in unplanned situations.

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 type of sources, because aid-agencies are sometimes not equipped to tag the material in the proper

way. Autier (1990) discusses the case of drug supplies, after the 1988 Armenian earthquake, when at least 5000 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.
One important aspect is security. As described in the challenges above, 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 access, distribution and security of the information in a number of ways.

3. Application of RFID to disaster supply chains

3.1 RFID technology

Radio Frequency Identification (RFID) is said to be the future technology to improve and optimize supply chain management systems. In comparison to traditional bar codes, RFID technology provides better data security, does not need line of sight because it is based on radio propagation, provide computational capability, improve automation and thus enhances the operational efficiency of supply chains Lin (2009). Figure 3 shows the differences with barcode technology: RFID allows to write information on the tag without line of sight as they are based on radio propagation and they provide computational capability, which can be used to implement security features. Typical components of RFID systems are RFID tags attached to the assets, reading/writing devices, and back-end systems.
RFID tags are usually very small sized low cost devices which can be easily fixed on physical objects like asset boxes or even implanted in animals or persons. The interface to control RFID tags is a short range wireless link. The simplest tags just send a unique identification number (UID) on request. More sophisticated tags offer several bits to severals bytes of read and write memory. High end RFID tags are equipped with a computing device to execute tasks like cryptographic algorithms for authentication or encryption. Beside the classification concerning the feature set of RFID tags there are basically two possibilities for the power supply of RFID tags: passive and active. Passive tags harvest the energy received from the reader through the antenna and using that energy to power the device. Passive tags are less expensive than active tags, which include their own power supply like a battery. The battery powered tags offer the possibility to execute tasks while not connected to a reader. For example perishable goods may be monitored by active tags that integrate with thermometers to ensure the goods are kept at an acceptable temperature.
Devices for accessing RFID tags are called RFID readers. RFID readers can either be fixed devices with antennas mounted at points where assets pass by (e.g., reader gates) or readers can be handheld devices available for several operational environments. Some handheld devices are even equipped with a wireless communication link to access the back-end system. In the back-end system all the RFID data is aggregated, stored, and provided to the supply chain management. The main component of the back-end system is the RFID middleware which connects the reader infrastructure to databases and supply chain management tools.

3.2 Track and trace based on RFID

Systems based on RFID technology provide the track and trace capability to monitor the movement of tagged items from the suppliers to the emergency crisis through distribution channels. figure 4 shows the typical supply chain based on RFID technology. The crates carrying the necessary assets are equipped with RFID tags, which are read at every point

RFID tags are like barcodes but offer more functionality:

- Writing status information in the field
- Reading/writing without line of sight
- More Capacity (several kilobytes)
- Enhanced reading distance depending on RFID standard
- Sensors to monitor environmental conditions
- The chip provides computation capability, which can be used to implement security features

Fig. 3. Barcode and RFID

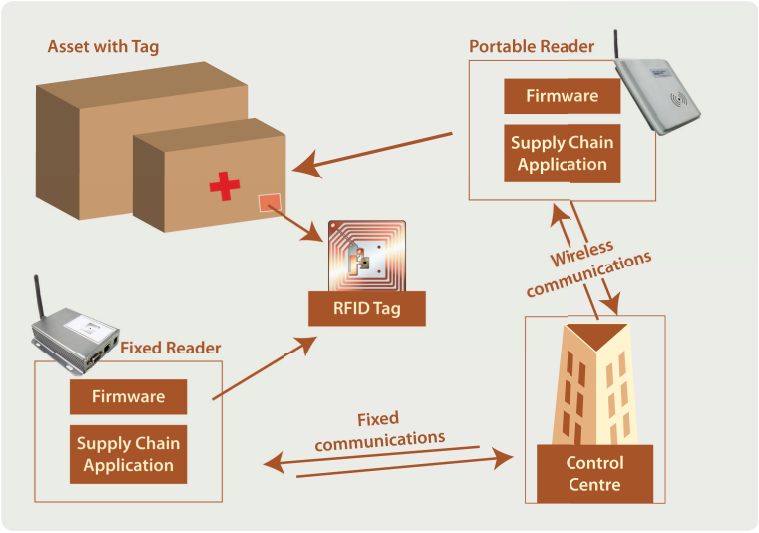


Fig. 4. Supply chains based on RFID technology

within the supply chain through automated systems equipped with RFID readers. The identification number provided by the RFID tag has to be unique for each item. The reading device aggregates the tag ID with its own ID and sent the data set to a central tracking server in a control center. Both fixed readers and mobile readers can be used to track the assets with RFID tags. Fixed readers are usually installed at main goverment and transportation centers (e.g., ports, airports). Mobile readers can be used by the government and relief agencies in the field or if the transportation centers themselves are destroyed by the disasters. Mobile readers may also provide their location through Global Navigation Satellite Systems (GNSS) like GPS. Control centers can use the position provided by the mobile readers to organize the distributions of goods in a more efficient way. There is the need to have a central tracking server, which stores the complete history of the RFID tags across all the disaster supply chain.

Various relief organizations and their own ICT systems can connect with the central tracking server to retrieve the information on the distributed goods as shown in figure 5. Currently the most promising approach for a track and trace solution is the Electronic Product Code (EPC) infrastructure. Designed and standardized by EPCglobal EPCGlobal (2003) it enables the exchange of RFID data using Internet protocols.

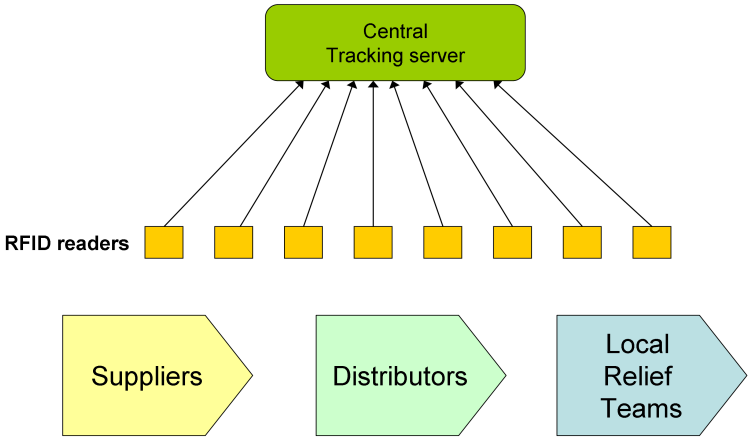


Fig. 5. Tracking system

At a first glance such a track and trace system seems to be a good approach, but there are some drawbacks. A precondition for track and trace techniques to work reliably is that each party involved in the distribution process must take part to 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 and they must also provide a consistent tracking data. This requires cooperation among all partners within the multi party supply chain. On the other hand in emergency crises the communication 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.
As written in the previous sections, security is an essential requirement. Ordinary RFID tags, with no security features, which are commonly used in commercial supply chains are simple tags, which only store an identification number in plain text. As a consequence the tags themselves can be susceptible to faking attacks. 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. More information on the need for secure RFID in disaster supply chains in provided in section 5.1.

4. RFID security

Like other wireless technologies, RFID is vulnerable to a wide range of security threats, which have been identified in literature.
In Tanenbaum et al (2006), the authors identify the following threats to RFID technology:

1. *Sniffing or eavesdropping*, where RFID tags are read without the knowledge of the tag bearer. Even if RFID is a short-range wireless technology, RFID tag reading my happen

also at large distances using RFID readers equipped with directional antennas and power amplifiers.

2. *Spoofing*. Spoofing attacks supply false information that looks valid and that the system accepts. Attackers can create *authentic* RFID tags by writing properly formatted tag data on blank or rewritable RFID transponders.
3. *Tracking*. RFID readers in strategic locations can record sightings of unique tag identifiers.
4. *Denial of service*. Denial of Service (DoS) is when RFID systems are prevented from functioning properly. Tag reading can be hindered by Faraday cages or *Signal jamming*, both of which prevent radio waves from reaching RFID-tagged objects
5. *Replay attack* where a valid RFID signal is intercepted and its data is recorded; this data is later transmitted to a reader where it is played back. Because the data appears valid, the system accepts it.
6. *Cloning* where a RFID tag is duplicated with the same information.

Some of these RFID security threats are relevant to disaster supply chains. For example sniffing can be used to extract the information on the contents of the crates to understand if they contain valuables goods. By using long distance sniffers, malicious parties can collect the information on the distributed goods, without being detected by authorities, and plan a subsequent phyisical attack to steal valuable material. By using RFID replay attacks, thieves can make the theft more efficient. In a first phase, thieves intercept a valid RFID signal. Then they replace the crates and they use the replayed signal to mislead the RFID reader owned by the authorities. In another example, malicious parties can track the flow of goods of specific types to improve the planning for a subsequent theft.
While sniffing is relatively easy to implement, other RFID threats are more complex to implement and malicious parties may use them only for very valuable goods. For example Tanenbaum et al (2006) introduces a new type of RFID threat called RFID malware, where malicious software carried by an infected RFID tag can "'infect"' the backend of a RFID IT infrastructure during the reading phase. This type of attack is more complex to implement and may be limited to the commercial domain.
Security issues in the context of supply chain management has been investigated in Li and Ding (2007), which identifies the specific security requirements in supply chains and propose a practical design of RFID communication protocols that satisfy the security requirements.

5. Secure RFID in humanitarian logistics

5.1 Need for secure RFID

As described in the previous sections, a major issue in natural disasters and emergency crises is 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). 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. 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.
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 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 (see Finkenzeller (2003)), as well as development tools. Cloning an original tag is not difficult with the proper tools.
Is the RFID is not secure, 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.
This chapter will analyze practical utilization of this type of device in the resolution of emergency crises to guarantee the reliability of sealing of the goods and their identification.
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.
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 5 shows the tracking system. For instance, the Electronic Product Code (=EPC) infrastructure by EPCglobal (see 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.

5.2 Cryptographic authentication

A 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 (see also Staake (2005)). This authentication mechanism must withstand the cloning attack as described in the previous sections. 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. Then the tag sends this response back to the reader. Finally the reader, respectively the back end system, checks whether the response is correct or not. Note that the secret key itself is not transmitted over the radio channel and the correct response can only be generated with the aid of the secret key.

5.3 Public key authentication

A weakness of symmetric cryptography used in most of RFID system is that 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. This approach requires that the readers must store the secret keys of the RFID tags belonging to the application domain or an on-line connection from the reader to a server must be established to store the secret keys of the RFID tags in a secure and reliable back end system.

In public-key cryptography, the response generation is 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 needn't 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.

The authentication flow is following:

- the tag transmits its certificate $cert_{id}$ containing its public key pub_{id}.
- the reader verifies the authenticity of the sent public key pub_{id} with the public signature key.
- 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 benefits of this approach are that:

- no secret key is needed for the authentication on the reader side, neither in the back end nor in the reader itself.
- the authentication process can be performed without any online connection which simplifies the system.

The disadvantage of the 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. Low-cost RFID tag based on elliptic curve cryptography (=ECC) are proposed in Wolkerstorfer (2005). Batina (2006) gave a further area optimization using a protocol based on zero knowledge.

5.4 Authentication protocol

An efficient authentication protocol for RFID tags is based on 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 one 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:

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

The structure determined by the set of points and this addition operation allows public key operation which is the scalar multiplication $s * P$ of a scalar value s in binary representation $s = (s_\ell, \ldots, s_1)_2$ 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 (2004). The so-called elliptic curve point multiplication is the basis for our protocol. We implemented Montgomery's method for scalar multiplication Bock (2008); Hankerson (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 (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:

$$Q := d * P$$

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:

$$C := k * P$$

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

$$R := d * C$$

The reader itself calculates $V := k * Q$ and checks if $R = V$. The verification works since the following chain of equations holds:

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

The complete authentication protocol is depicted in Figure 6.

6. System architecture

The application of secure RFID to Humanitarian logistics is depicted in figure 7.
The deployment of this system is based on the following steps:

1. In the first step of the disaster supply chain, the Certification Authority (CA) generates the key pars and store them in the RFID tags. This step has to be executed in a trustworthy environment; for example a logistic center of an humanitarian organization or a government agency. The CA is a server system which stores the private signature key

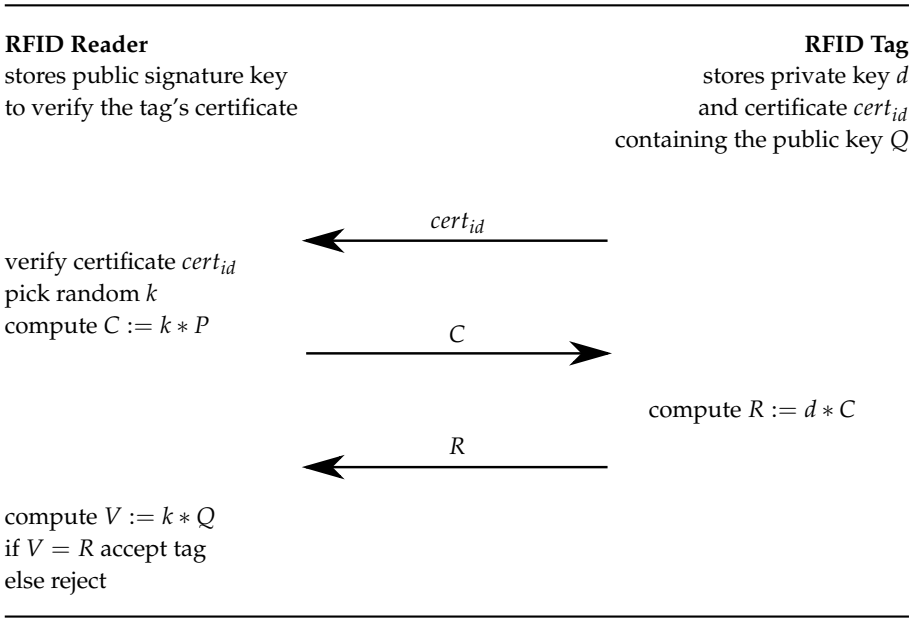


Fig. 6. The RFID Authentication Protocol based on Elliptic Curve Cryptography

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.

2. Certificates must be distributed to the main stakeholders as described in figure 8 to be installed on RFID readers (both fixed and mobile). Certificates can also be distributed in the mitigation phase using secure links over Internet or through secure communication links (e.g., VPN).
3. Then the RFID tags are applied to the relief goods, which are then transported to the disaster areas.
4. Relief agencies and other organizations can use the fixed and mobile RFID readers to track and trace the relief goods through all the nodes of the disaster supply chain. It is important that only trusted certificates are allowed to be installed on the readers.
5. At the disaster area the emergency responders may use handheld devices equipped with RFID readers to read the attached RFID tags, verify their authenticity and finally distribute the goods.

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.
Figure 8 describes the deployment workflow of the proposed solution among the participants of the disaster supply chain.

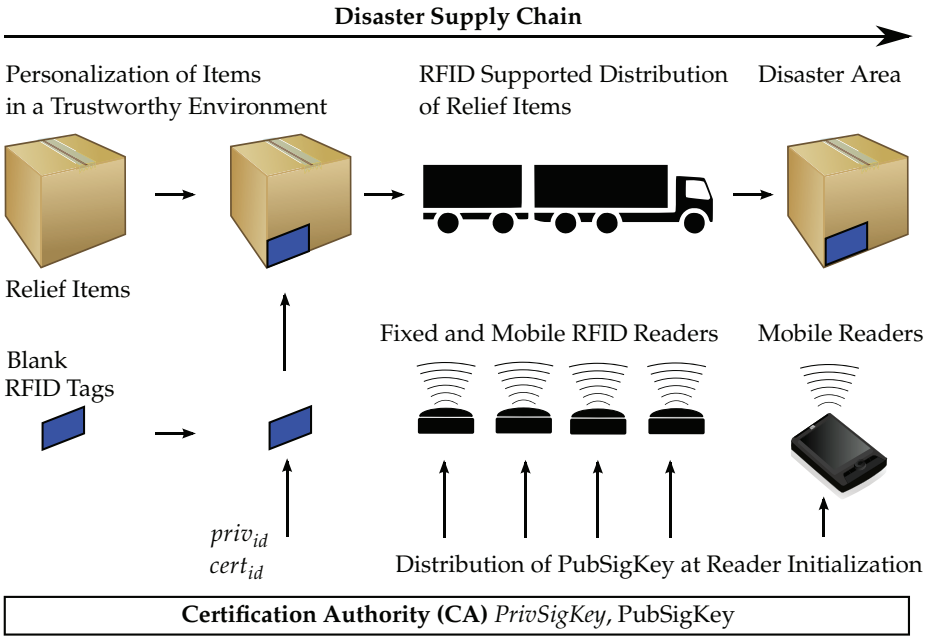


Fig. 7. Proposed system architecture for RFID secured relief item distribution

7. Communication infrastructure for humanitarian logistics

In order to fully exploit the capabilities of the RFID based Supply Chain Management, such system must be supported by an efficient and secure communication system as well as by a distributed data base management system. In a disaster area, most communications will be wireless because first responders need high mobility and because the fixed line infrastructure can be unavailable, e.g. destroyed, damaged or overloaded. The security of the communication link between the RFID tag and the reader/writer is described in another part of this paper, but it is very important to consider that any system is as secure as its weakest component; therefore the communication link between the reader/writer and its local or remote controller has to be considered and made secure. In order to make the system usable, it is very important to consider that the remote stations should be allowed to work without an *always-on connection* because it is unthinkable to have such connection available all the time. In the following we will provide a broad description of communication systems that could be implemented in a disaster situation to support the Supply Chain exploiting the security features described in the previous chapters. From the logical point of view, the logistic of the disaster supply chains is very similar to the Logistic of any Commercial Supply Chain, therefore we can assume that the basic concepts and the basic infrastructure remain the same, but few key features must be redesigned in order to cope with the peculiar operational environment of the Disaster Relief Operations. The first aspect to address is the lack of standard communication infrastructures (GSM/UMTS/PSTN) where crates of goods and people have to be dispatched, therefore the ideal situation is that any RFID reader used to acquire the information on the crates present in any intermediate station (e.g, warehouse)

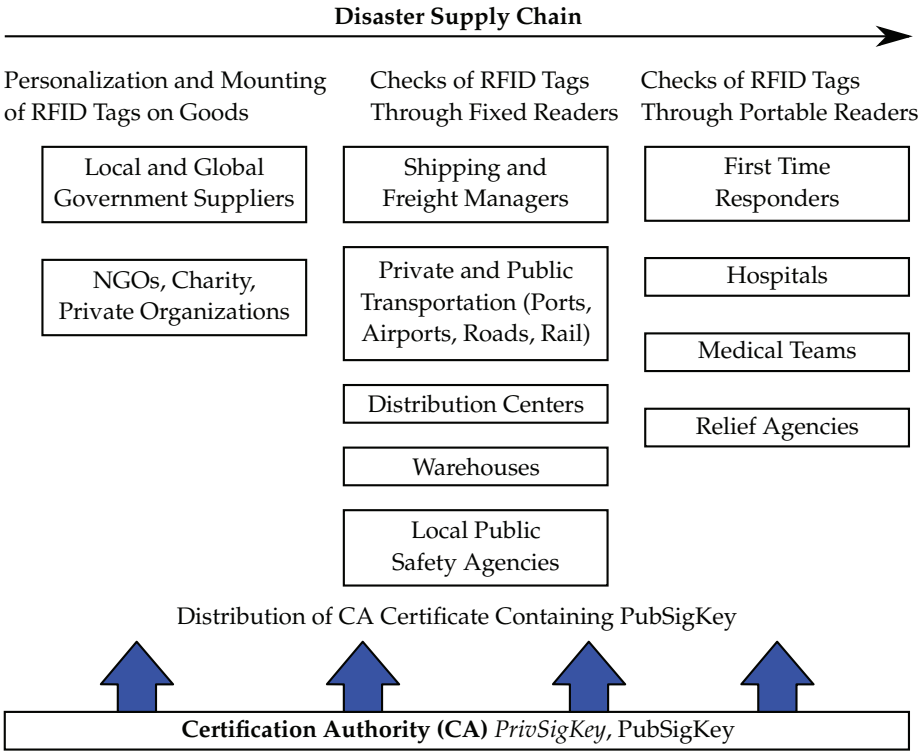


Fig. 8. Deployment workflow

in the disaster area is provided with a satellite link to transmit the data to the Logistic Control Centre as described in Figure 9.

An alternative solution (depicted in Figure 10) could be the establishment of a Wireless Local Area Network, to collect and manage data locally, connecting with the Central Logistic Control Center only when required. This solution presents some important pros, namely the possibility to operate without a permanent link with the logistic centre and a significant reduction in term of the cost of the communication equipment. The cons are the need to set up a local logistic control centre and the implementation of a secure client-server mechanism, between the control centres capable of surviving an unstable connection: usual commercial software, designed for a reliable "always on" environment may run into troubles facing frequent loss of connection. Furthermore the WiFi connection must be implemented with a reasonable level of security to avoid jeopardizing the secure RFIDs. An example of RFID sensor network for humanitarian logistics based on Zigbee communication technology is presented in Yang (2010).

In summary, the communication structure needed for such system should take into account some key issues:

- Distributed databases connected through potentially unreliable communication links

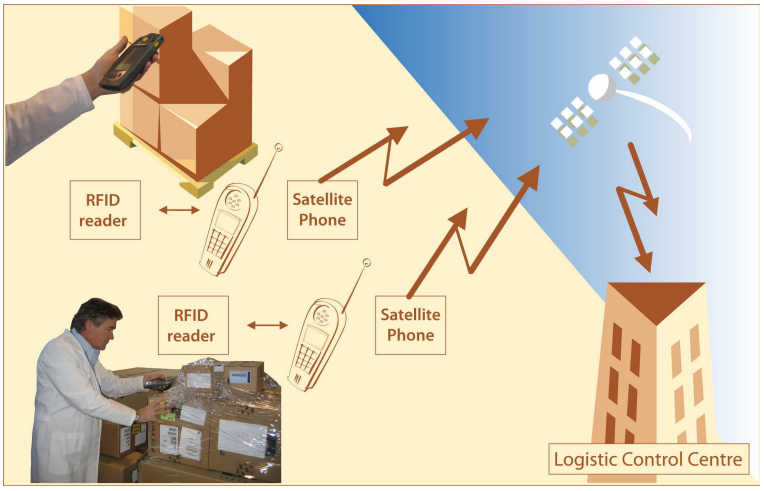


Fig. 9. RFID readers directly connected to the Logistic control center through Satellite Communications

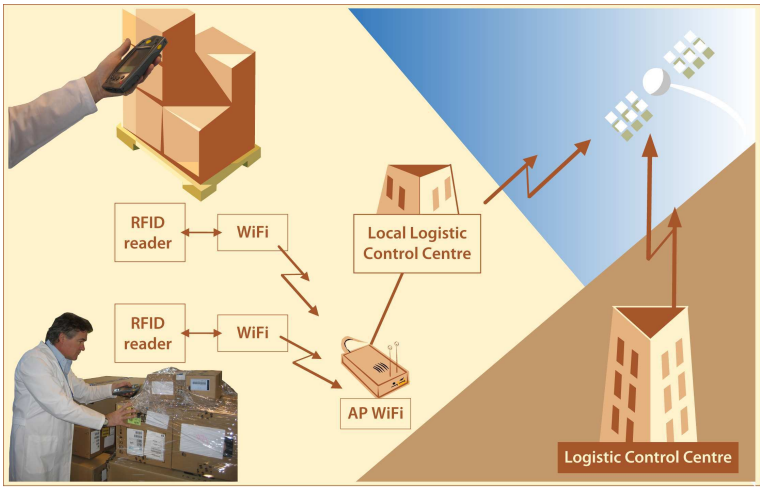


Fig. 10. RFID readers connected to a wireless Local Area Networks for local management

- Integrated and redundant communication systems using: a) Direct satellite links; b) Local wireless coverage (GSM and/or WiMAX and/or WiFi) plus satellite link
- Secure wireless links
- Store and forward protocols

8. Conclusions

The chapter has presented the application of secure RFID technology to the specific domain of humanitarian logistics. Because security is a important requirements in disaster management,

we believe that relief organizations can benefit from this technology to ensure that goods are not stolen or tampered. A potential system architecture has been presented and described. Because, infrastructures are usually degraded or destroyed in a natural disaster or emergency crisis, mobile readers and fast deployable communication systems is an important component in the overall system architecture.
Future developments in this research area would be the integration of these technologies in the organizational and procedural frameworks of relief and government agencies. As described in this chapter, a central Certification Authority (CA) must be defined to provide the certificates, which must be installed in the fixed and mobile portable readers. Furthermore, an efficient disaster supply chain requires the set-up of a coordinated track and trace system in the prevention phase of disaster management.

9. References

Tom Gardner, Former FEMA director shoulders greater share of blame for Katrina failures, *ASSOC. PRESS*, Jan. 19, 2006

Melanie R. Rieback, Patrick N.D. Simpson, Bruno Crispo, Andrew S. Tanenbaum, RFID malware: Design principles and examples, *Pervasive and Mobile Computing*, Volume 2, Issue 4, Special Issue on PerCom 2006, November 2006, Pages 405-426, ISSN 1574-1192

Li, Y. and X. Ding, Protecting RFID communications in supply chains, in: *Proceedings of the 2nd ACM symposium on Information, computer and communications security, ASIACCS '07*, 2007, pp. 234Ű241

"An Entrepreneur Tackles the Logistics of Disaster". Available at URL: *http://www.globalenvision.org/library/*

Fritz Institute. "Logistics and the effective delivery of humanitarian relief". May 2005. Available at URL: *http://www.fritzinstitute.org/*.

A Failure of initiative - Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina

Autier P, Ferir MC, et al. "Drug supply in the aftermath of the 1988 Armenian earthquake", Lancet 1990;

Cassidy W. A logistics lifeline. *Traffic World*, October 2003.1. 335(8702):1388-1390.

L.C. Lin, "An integrated framework for the development of radio frequency identification technology in the logistics and supply chain management". *Computers and Industrial Engineering* (2009).

EPCglobal. available at URL: *http://www.epcglobalinc.org/home/*.

Infineon. available at URL: *http://www.infineon.com/*.

An asymmetric cryptosystem. available at URL: *http://www.ntru.com/*.

NXP. available at URL: *http://www.nxp.com/*

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

H. Bock, M. Braun, M. Dichtl, J. Heyszl, E. Hess, W. Kargl, H. Koroschetz, B. Meyer, and H. Seuschek. A milestone towards RFID products offering asymmetric authentication based on elliptic curve cryptography. In *RFIDSec 2008, Proceedings of the 4th Workshop on RFID Security*, July 9-11 2008, Budapest, Hungary, July 2008.

Altay N., W. G. Green III W. G., OR/MS research in disaster operations management, European Journal of Operational Research, Volume 175, Issue 1, 16 November 2006, Pages 475-493, ISSN 0377-2217,

K. Finkenzeller. RFID-Handbook. Wiley & Son LTD, third edition,

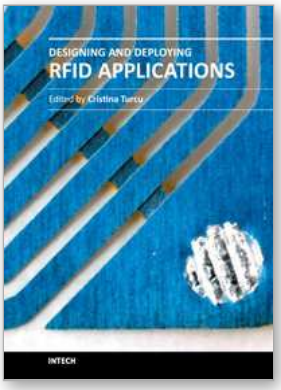
Yang H,et al. Hybrid Zigbee RFID sensor network for humanitarian logistics centre management. *Journal of Network Computer Applications* (2010)

D. Hankerson, A. Menezes, and S. Vanstone. *Guide to elliptic curve Cryptography*. Springer, 2004.

T. Staake, F. Thiesse, and E. Fleisch. Extending the EPC Network — the potential of RFID in anti-counterfeiting. In *20th ACM symposium on Applied computing*, pages 1607–1612. ACM, March 2005.

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

G. Bankoff, G. Frerks, D. Hilhorst (eds.) (2003). Mapping Vulnerability: Disasters, Development and People. ISBN ISBN 1-85383-964-7



Designing and Deploying RFID Applications

Edited by Dr. Cristina Turcu

ISBN 978-953-307-265-4
Hard cover, 384 pages
Publisher InTech
Published online 15, June, 2011
Published in print edition June, 2011

Radio Frequency Identification (RFID), a method of remotely storing and receiving data using devices called RFID tags, brings many real business benefits to today world's organizations. Over the years, RFID research has resulted in many concrete achievements and also contributed to the creation of communities that bring scientists and engineers together with users. This book includes valuable research studies of the experienced scientists in the field of RFID, including most recent developments. The book offers new insights, solutions and ideas for the design of efficient RFID architectures and applications. While not pretending to be comprehensive, its wide coverage may be appropriate not only for RFID novices, but also for engineers, researchers, industry personnel, and all possible candidates to produce new and valuable results in RFID domain.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821